GOBIERNO DE ESPAÑA

MINISTERIO DE INCLUSIÓN, SEGURIDAD SOCIAL Y MIGRACIONES

SECRETARÍA DE ESTADO DE LA SEGURIDAD SOCIAL Y PENSIONES

Gerencia de Informática de la Seguridad Social

FIRMA NO NORMALIZADA TIPO 2

Configuración de entorno para la Firma No Normalizada Tipo 2. Solución mediante *Cryptobrowser*

Centro de Seguridad de la Información

15/09/2022

Versión: 2.2

Clasificación: Público

Gerencia de Informática de la Seguridad Social

CONTROL DE VERSIONES			
Título		FIRMA NO NORMALIZADA TIPO 2 (Solución mediante *Cryptobrowser*)	
Autor		CSI	
Fecha versión 1.0		22/08/2017	
Versión	Fecha	Responsable	Cambios introducidos
1.1	30/10/2017	Dirección de Seguridad, Innovación y Proyectos	Primer Documento
2.0	17/07/2020	Centro de Seguridad de la Información	Actualización de contenidos
2.1	12/04/2021	Centro de Seguridad de la Información	Actualización de contenidos
2.2	15/09/2022	Centro de Seguridad de la información	Actualización de contenidos

INDICE

1. OBJETIVO

El sistema de Firma No Normalizado Tipo 2, es un sistema de *firma en cliente* que utiliza un componente criptográfico incluido como una extensión del navegador bajo el nombre *CryptoBrowser*. Este sistema de firma sólo requiere la instalación de una pequeña aplicación en el *PC* del usuario y la activación de la mencionada extensión en el navegador de internet. En este manual se describe la configuración necesaria para este tipo de firma en los navegadores compatibles *Chrome y Firefox* en sistemas *Windows.*

1.1. SERVICIOS DE LA SEDE QUE UTILIZAN C*RYPTOBROWSER*

La práctica totalidad de los servicios web de nuestra Sede están adaptados al sistema de firma Normalizado mediando *JNLP,* siendo muy pocos los que realizan el proceso de firma mediante *Cryptobrowser*.

Consulte el listado de servicios y tipo de firma asociado en el apartado de Requisitos de Firma Electrónica:

https://sede.seg-social.gob.es/binarios/es/Listados_tipo_firma

2. COMPATIBILIDAD DE SISTEMAS OPERATIVOS Y NAVEGADORES EN EL SISTEMA DE FIRMA NO NORMALIZADO TIPO 2

Cuadro de compatibilidad de Sistemas Operativos y navegadores para la firma mediante certificado digital:

Actualmente los siguientes sistemas operativos y navegadores son los únicos compatibles con este tipo de firma:

- **Sistemas Windows**: navegadores Edge, Chrome y Firefox

Los servicios habilitados para este tipo de firma pueden ejecutarse en otros navegadores, como Internet Explorer o Safari, sin embargo, en estos casos el proceso de firma se realizará de manera automática mediante *Applets*. Si va a utilizar alguno de estos navegadores, consulte antes los requisitos técnicos de configuración incluidos en el manual correspondiente *Firma No Normalizada Tipo 1*.

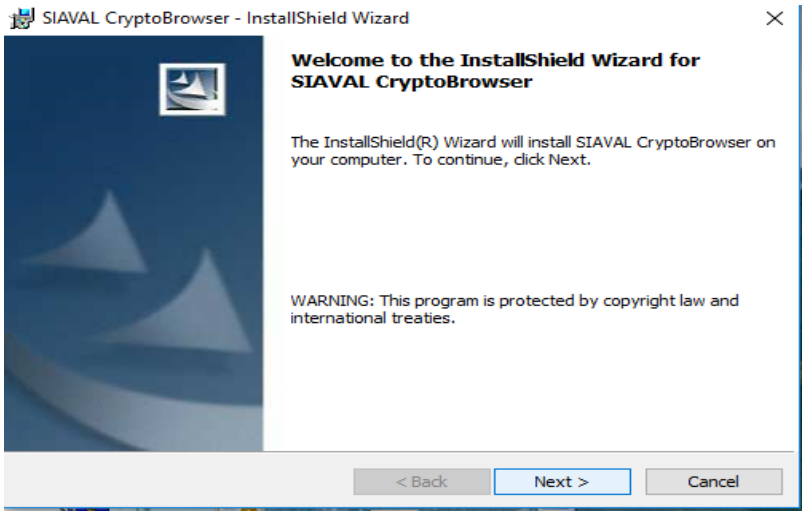
3. INSTALACIÓN DE LA APLICACIÓN *SIAVAL CRYPTOBROWSER*

3.1. DESCARGA

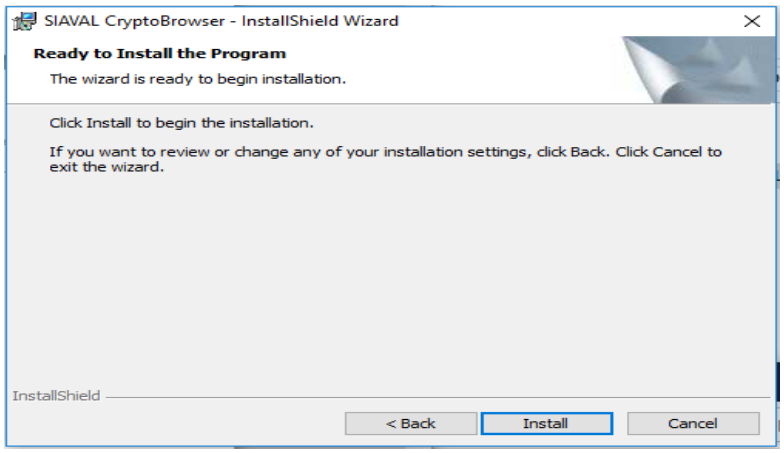
La aplicación *Siaval CryptoBrowser* está disponible para su descarga en la página de *Requisitos Técnicos* de la Sede de la Seguridad Social, *Requisitos de firma electrónica*, en el apartado relativo a *Firma No Normalizada Tipo 2,* junto a este manual. El fichero tiene por nombre: *CryptoBrowser.msi*

3.2. INSTALACIÓN DE LA APLICACIÓN CLIENTE *SIAVAL CRYPTOBROWSER*

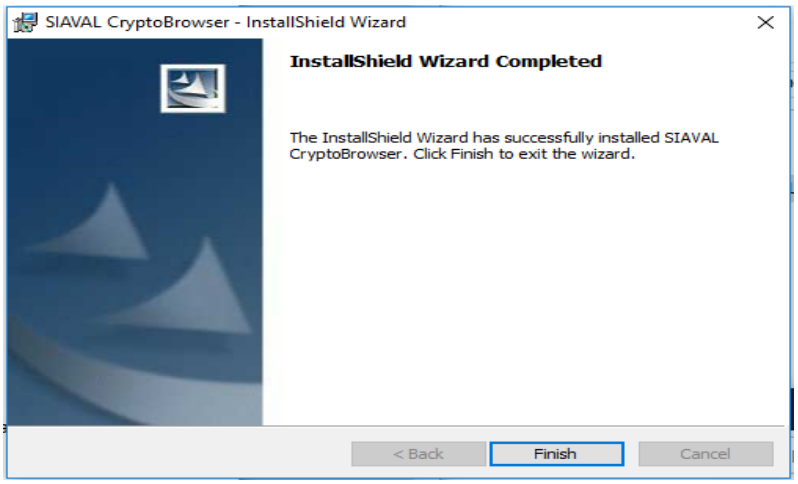
Una vez descargada la aplicación, localizar la misma en el directorio de descargas habitual o en el directorio que se indicó en su momento. Ejecutar el fichero haciendo doble clic sobre el mismo, se abrirá el asistente de instalación. A continuación, pulsar el botón "*Next*"



Pulsar el botón "*Install*"



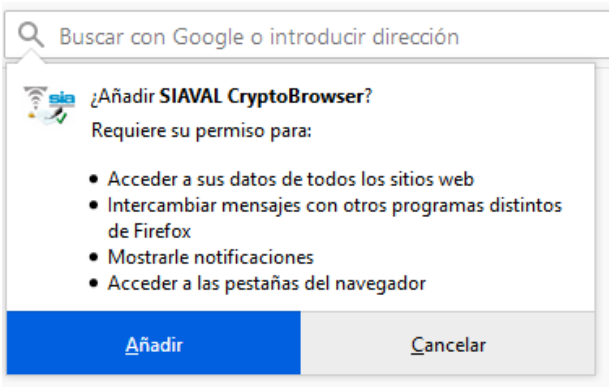
Finalizar la instalación presionando el botón "*Finish*"



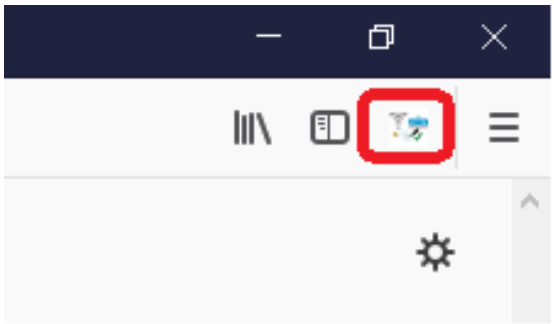
Al terminar la instalación, se abrirá una ventana solicitando reiniciar el equipo para finalizar la instalación, presione el botón "*Yes*".

3.3. INSTALACIÓN DE LA EXTENSIÓN *CRYPTOBROWSER* EN *FIREFOX*

Instalada la aplicación *Siaval CryptoBrowser*, tras reiniciar el equipo y abrir *Firefox*, podrá aparecer un aviso para añadir la extensión correspondiente *CryptoBrowser.* Pulsar "Añadir".



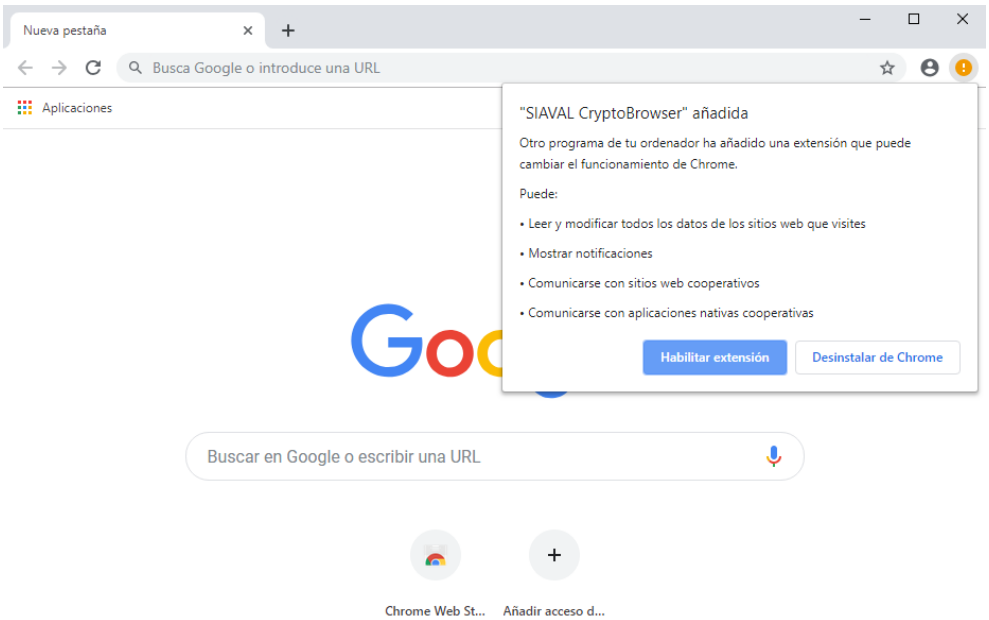
Finalizada la instalación aparecerá un icono de la extensión en la parte superior derecha del navegador:



Del mismo modo en el apartado de extensiones del navegador puede comprobar que aparece la extensión instalada e información de esta:

3.4. INSTALACIÓN DE LA EXTENSIÓN *CRYPTOBROWSER* EN *CHROME*

Instalada la aplicación *Siaval CryptoBrowser*, tras reiniciar el equipo y abrir *Chrome*, podrá aparecer un aviso para habilitar la extensión de *Siaval CryptoBrowser.* Pulsar "Habilitar extensión". Tras su activación se mostrará mensaje de confirmación.

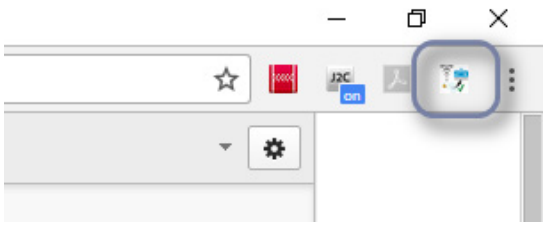


Si el aviso de detección no aparece, se puede añadir la extensión manualmente desde el siguiente enlace (*copiar y pegar en la línea de direcciones del navegador Chrome*):

https://Chrome.google.com/webstore/detail/siavalcryptobrowser/fmgobkioeenfdomplekgcgiafllkohfl

Hacer clic sobre "*Añadir a CHROME*" para instalar la extensión ***CryptoBrowser*** en el navegador

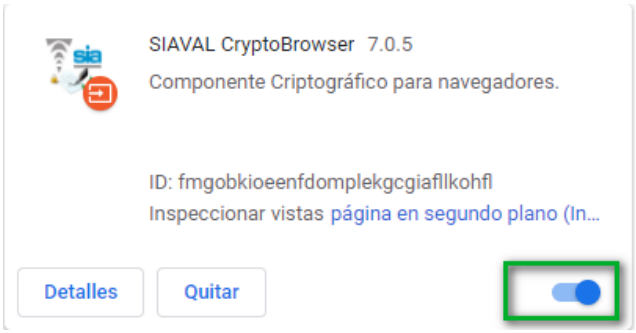
Añadida la extensión debe mostrarse un icono en la parte superior derecha del navegador que indica que la extensión está instalada.



3.4.1. Habilitar de forma manual la extensión de CryptoBrowser en Chrome

En Chrome, pulsar en el icono *"personaliza y controla Google Chrome"* - ajustes – en el menú desplegado: "*Más herramientas*" y después "*Extensiones*".

Habilitar la extensión activando el deslizador a la derecha:

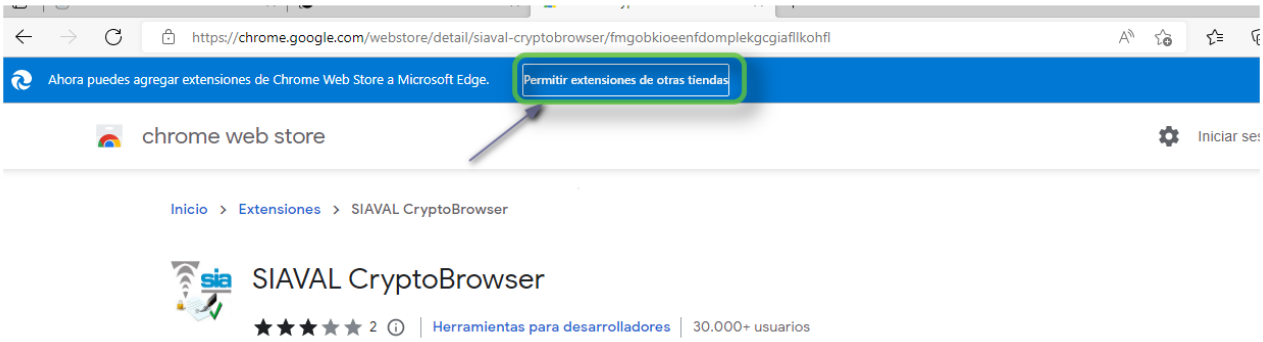


3.5. INSTALACIÓN DE LA EXTENSIÓN *CRYPTOBROWSER* EN *EDGE*

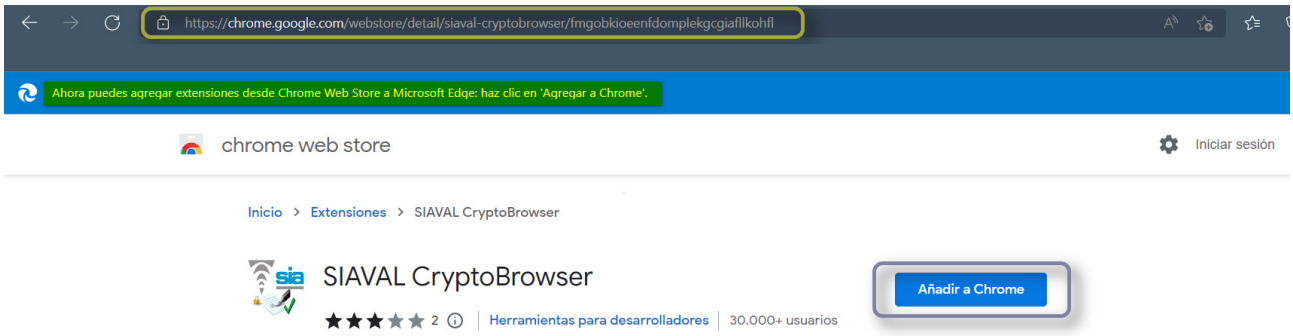
Instalada la aplicación *Siaval CryptoBrowser*, tras reiniciar el equipo abrir *EDGE;* copie y pegue la siguiente *url* en la línea de direcciones del navegador:

https://Chrome.google.com/webstore/detail/siavalcryptobrowser/fmgobkioeenfdomplekgcgiafllkohfl

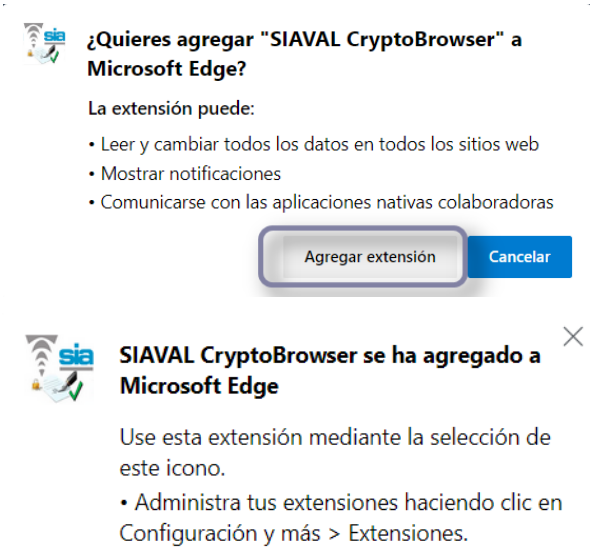
Si aparece la opción, pulse el botón *Permitir extensiones de otras tiendas.*



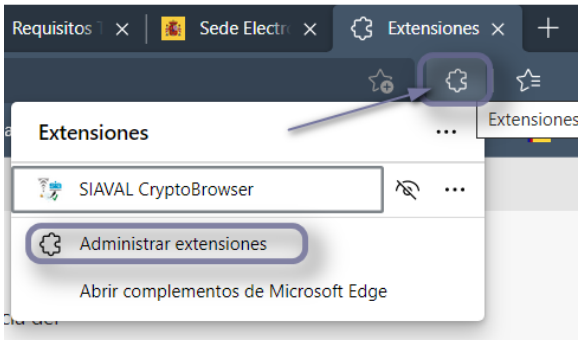
Pulse en el botón "*Añadir a Chrome",*



Se mostrará una advertencia para añadir la extensión a EDGE:



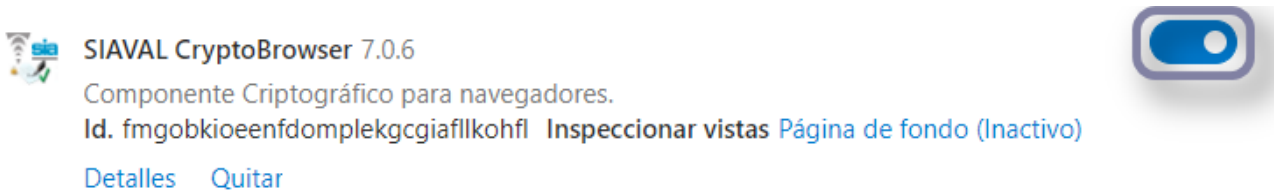
Puede comprobar en el icono de *extensiones* que se ha instalado y activado correctamente:



3.5.1. Habilitar de forma manual la extensión de CryptoBrowser en EDGE

En EDGE, pulsar en el icono de extensiones o por menú: *Configuración -> Extensiones -> Pulse Administrar extensiones.*

En su caso, habilitar la extensión activando el deslizador a la derecha:



4. CONFIGURACIÓN DE LOS NAVEGADORES

4.1. CERTIFICADOS DE CONFIANZA

Los certificados de confianza firmantes actuales, tanto el de los servidores de la Seguridad Social como el que certifica el software involucrado en los procesos de firma, por lo general ya vienen incluidos en los navegadores de internet más habituales. No obstante, se aconseja verificarlo y en caso de que dé algún error el proceso de firma por falta de confianza en la entidad firmante deberá instalar los siguientes certificados raíz e intermedio de la FNMT-RCM (Fábrica Nacional de la Moneda – Real Casa de la Moneda).

4.1.1. Descarga de los certificados Raíz e intermedios de FNMT-RCM

La página de descarga de certificados de la Autoridad de Certificación de la FNMT-RCM es:

Certificados raíz de la FNMT - Sede

Descargar los siguientes certificados a una unidad local del equipo.

Certificado Raíz:

Descarga certificado AC Raíz FNMT-RCM

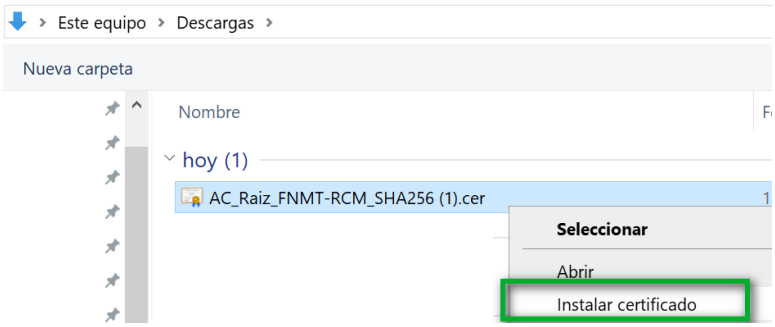
Certificados Intermedios:

Descarga certificado AC FNMT Usuarios

Descarga certificado AC Componentes Informáticos

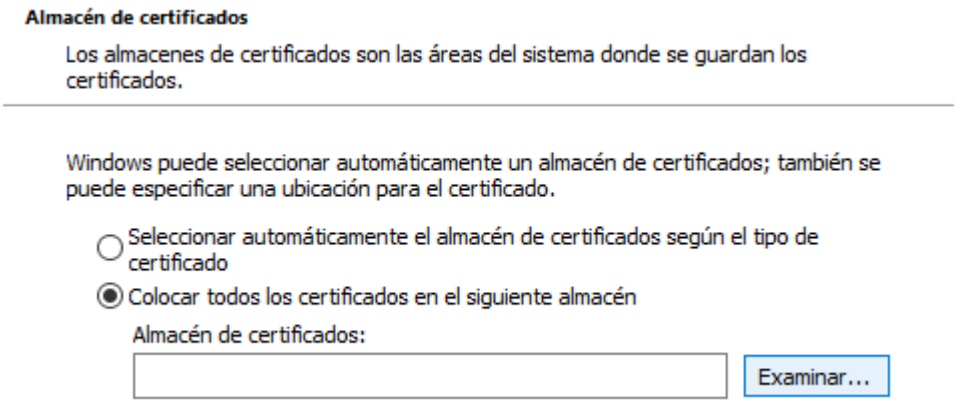
4.1.2. Instalación de los certificados Raíz e intermedios de FNMT-RCM en Chrome

Localizar la carpeta donde se han descargado los certificados y con cada uno pulsar con el botón derecho del ratón y seleccionar: "I*nstalar certificado".*

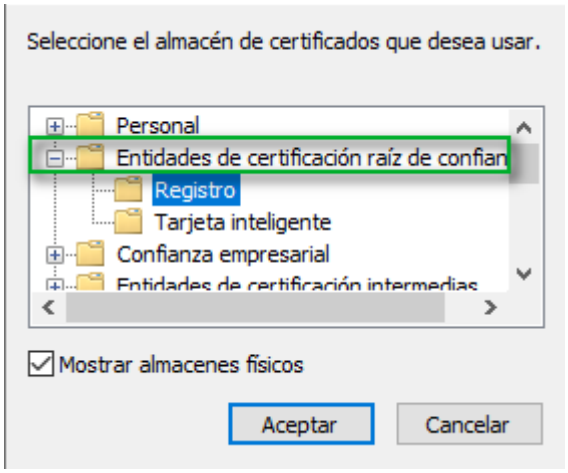


Se iniciará el proceso de importación. Pulse *Siguiente*.

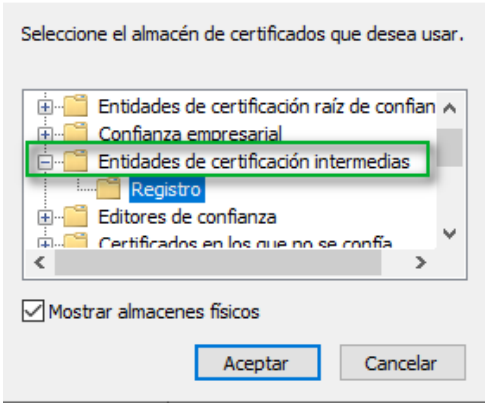
Marque "*Colocar todos los certificados en el siguiente almacén*" y pulse "*Examinar*"



Para el certificado Raíz: Marque la opción "*Mostrar almacenes físicos*" y seleccione la carpeta "***Entidades de certificación Raíz de Confianza***" -> Carpeta "*Registro*". Pulse "*Aceptar*".

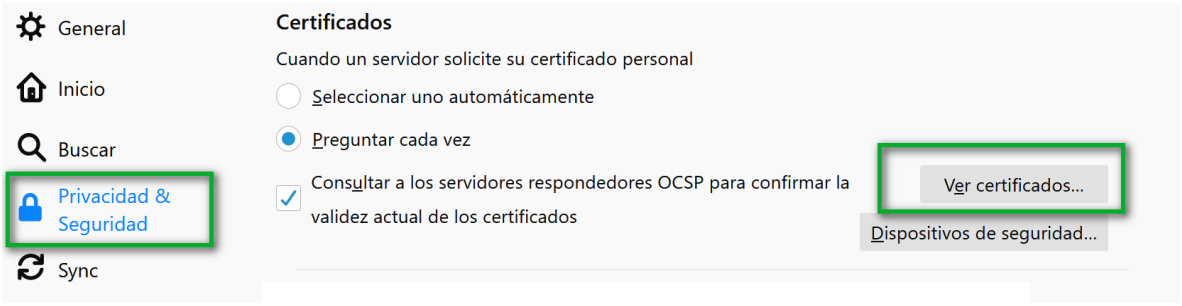


Para los certificados intermedios: Marque la opción "*Mostrar almacenes físicos*" y seleccione la carpeta "***Entidades de certificación Raíz de Confianza***" -> Carpeta "*Registro*". Pulse "*Aceptar*" y "*finalizar*".

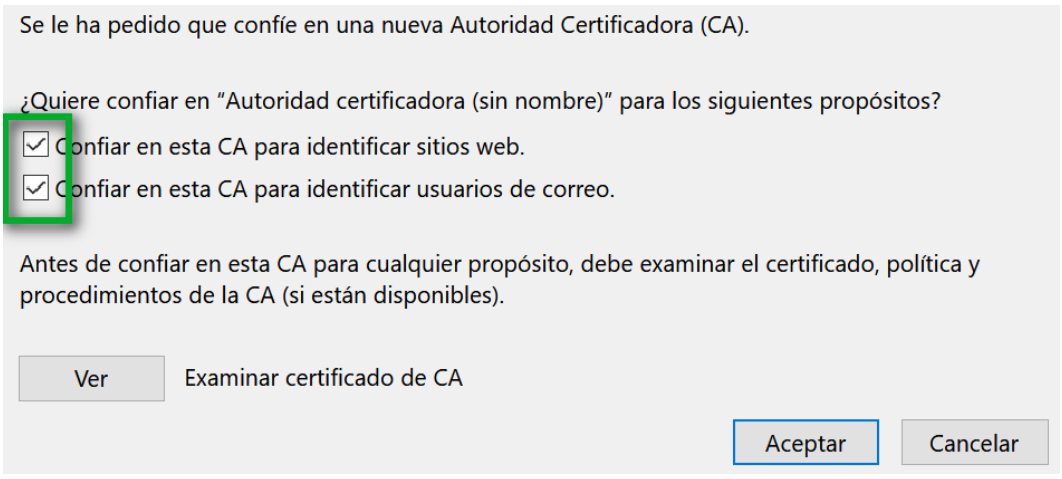


4.1.3. Instalación de los certificados Raíz e intermedios de FNMT-RCM en Firefox

Abrir *Firefox* y seleccionar *Herramientas -> Opciones -> Privacidad y Seguridad -> Ver Certificados*



Seleccionar la pestaña ***Autoridades*** y pulsar ***Importar.*** Localizar y seleccionar el certificado raíz de la FNMT descargado. Habilitar "***Confiar en esta CA"*** y aceptar.

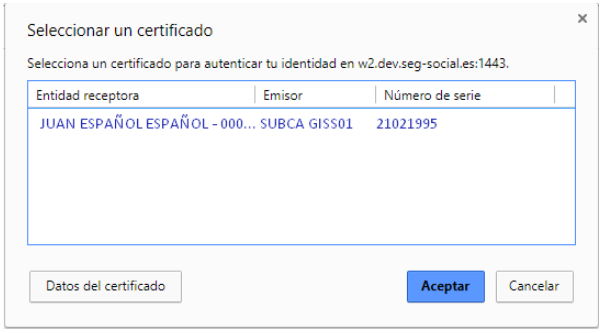


Repetir este mismo procedimiento con el resto de los certificados intermedios descargados.

5. DESCRIPCIÓN DEL PROCESO DE FIRMA NO NORMALIZADO TIPO 2 (*CRYPTOBROWSER*)

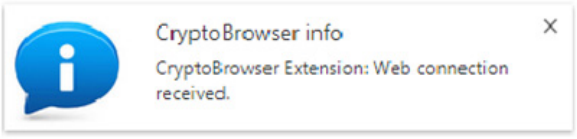
El siguiente ejemplo simula un proceso de firma realizado con *Cryptobrowser* en Chrome.

Autenticado en el servicio electrónico, al pulsar "*Firmar y enviar*", se solicitará seleccionar el certificado a utilizar:



Una vez pulse "*Aceptar*", la extensión de *CryptoBrowser* tomará el control del proceso de firma, informando de que el proceso está en marcha.

Al término del proceso de firma, se indicará si éste ha finalizado con éxito. La apariencia de este mensaje depende del servicio web ejecutado.



6. COMUNICACIÓN DE INCIDENCIAS

Si tiene problemas relacionados con el acceso a las aplicaciones, errores en el procesamiento de los datos, incidencias en el proceso de firma, tiene a su disposición el formulario del **Buzón de Consultas** en la página de la Seguridad Social:

http://www.seg-social.es/wps/portal/wss/internet/FAQ

Si su incidencia es técnica, en el apartado *"Formule aquí su propia pregunta",* incluya en el texto de la consulta la siguiente información de su entorno de trabajo: Sistema Operativo, navegador utilizado, tipo de certificado utilizado, Autoridad de Certificación emisora, nombre del servicio o trámite que intenta realizar y código de la incidencia si se muestra en el mensaje de error.