MANUAL DE RESOLUCIÓN DE INCIDENCIAS EN LA PLATAFORMA APPLE OS X

CÓDIGO: ADEL-Apple OS X VERSIÓN: 1.3

FECHA: 19/03/2025

PARA DISTRIBUCIÓN: PÚBLICA

ELABORADO POR:		REVISADO POR:		APROBADO POR:	
NOMBRE:	ADEL-SSII	NOMBRE:		NOMBRE:	
FECHA:	19/03/2025	FECHA:		FECHA:	
FIRMA:		FIRMA:		FIRMA:	

HISTÓRICO EVOLUCIÓN

VERSIÓN	FECHA	MOTIVO DE LA EVOLUCIÓN
0.1	20/02/2023	Primera versión.
0.2	13/09/2023	Actualización de la aplicación AutoFirma a la versión 1.8.2
0.3	22/01/2024	Actualización de medidas
1.0	03/04/2024	Actualización para la instalación de certificados de la FNMT en Apple OS X
1.1	12/06/2024	Actualización de la aplicación AutoFirma a la versión 1.8.3
1.2	09/09/2024	Actualización de la aplicación AutoFirma a la versión 1.8.4
1.3	19/03/2025	Solución de problemas en la actualización de AutoFirma a la versión 1.8.4

ÍNDICE

1. OBJETO 4

2. DOCUMENTACIÓN DE REFERENCIA 4

3. DESCRIPCIÓN DEL PROCEDIMIENTO 4

3.1. INSTALACIÓN DE LA APLICACIÓN 5

3.2. ACTUALIZACIÓN DE LA APLICACIÓN 8

3.2.1. Problemas en la actualización del programa 'autofirma' 8

3.3. INSTALACIÓN DEL PLUGIN DE HUELLAS DIGITALES V1.0 10

3.3.1. Problemas en la instalación del plugin de huellas digitales v1.0 14

4. PROCEDIMIENTO ADICCIONAL SI EXISTEN PROBLEMAS PARA REALIZAR LA FIRMA ELECTRÓNICA DEBIDO A LA CONFIGURACIÓN DE LOS CERTIFICADOS DE AUTOFIRMA 15

4.1. ACCEDER AL LLAVERO DE MAC. 15

4.2. ACCEDER AL LLAVERO 'SISTEMA' Y A LA OPCIÓN DE 'CERTIFICADOS'. 15

4.3. ACCEDER AL LLAVERO DE 'INICIO DE SESIÓN' Y A LA OPCIÓN 'MIS CERTIFICADOS'..... 17

4.4. ACCEDER A LA SEDE ELECTRÓNICA. 18

5. OTROS..... 19

5.1. RECOMENDACIÓN DE LA UTILIZACIÓN DE DISTINTOS NAVEGADORES. 19

5.2. PROBLEMAS EN LA VALIDACIÓN DEL CERTIFICADO DIGITAL EN LA PLATAFORMA VALIDE. .. 19

6. INSTALACIÓN DEL CERTIFICADO 'AC RAÍZ FNMT-RCM SERVIDORES SEGUROS' EN EQUIPOS APPLE OS X 19

7. INSTALACIÓN DEL CERTIFICADO 'AC RAÍZ FNMT-RCM SERVIDORES SEGUROS' EN DISPOSITIVOS MÓVILES CON APPLE IOS 23

1. OBJETO

El propósito de este documento es dar respuesta a la resolución de problemas asociados al uso del programa 'AutoFirma' en los ordenadores MAC con sistema operativo OSX.

Las pruebas han sido realizadas en '*macOS Sequoia 15.3.2'.*

2. DOCUMENTACIÓN DE REFERENCIA

- Requisitos para el uso de la Sede Electrónica de la UCM:

  https://sede.ucm.es/opencms/system/modules/sede/contents/pages/Requisitos

- Requisitos para el uso de 'AutoFirma', página de descarga:

  https://firmaelectronica.gob.es/Home/Descargas.html

3. DESCRIPCIÓN DEL PROCEDIMIENTO

En primer lugar, es necesario respetar los requisitos para usar la Sede Electrónica de la UCM que están recogidos en la siguiente página:

https://sede.ucm.es/opencms/system/modules/sede/contents/pages/Requisitos

IMPORTANTE: Para poder firmar documentos electrónicamente en la Sede de la UCM deberá tener instalada la última versión de la aplicación Autofirma, para descargarla pulse aquí.

Puede verificar el funcionamiento de Autofirma, además de en la Sede de la UCM, en la plataforma Valide.

3.1. INSTALACIÓN DE LA APLICACIÓN

Para configurar Autofirma deben realizarse los siguientes pasos:

1. Descargar el programa AutoFirma, para la versión de su sistema operativo y arquitectura de su equipo, desde:

   https://firmaelectronica.gob.es/Home/Descargas.html

2. Una vez descargado en la carpeta de descargas aparecerá un archivo .zip el cual debemos descomprimir haciendo doble clic sobre él. Obtendremos de esta forma el archivo de instalación del programa (Imagen 1).

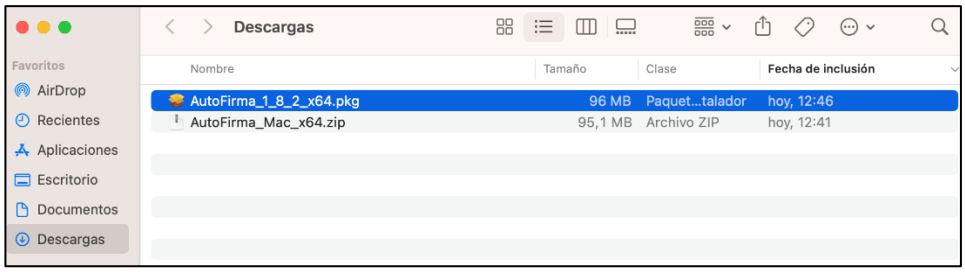

Imagen 1. Instalador comprimido '.zip' y paquete de instalación.

3. Seguidamente pulsaremos sobre el archivo de instalación para instalar el programa. El usuario con el que estemos identificados en nuestro equipo debe tener permisos de administrador de lo contrario no podremos realizar la instalación.

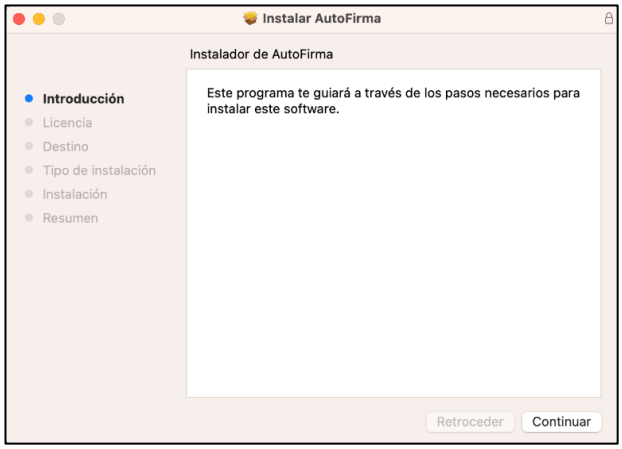

Imagen 2. Inicio del proceso de instalación.

4. Posteriormente se lanzará el proceso de instalación, en el cual debemos aceptar la licencia del programa (Imagen 3), y se informará del espacio que se va a consumir en el disco (Imagen 4). Para continuar tendremos que indicarle la contraseña de nuestro usuario. Además, se pedirá permiso sobre una serie

de cuestiones como es la instalación del certificado SSL (Imagen 5) o la configuración de Firefox (Imagen 6).

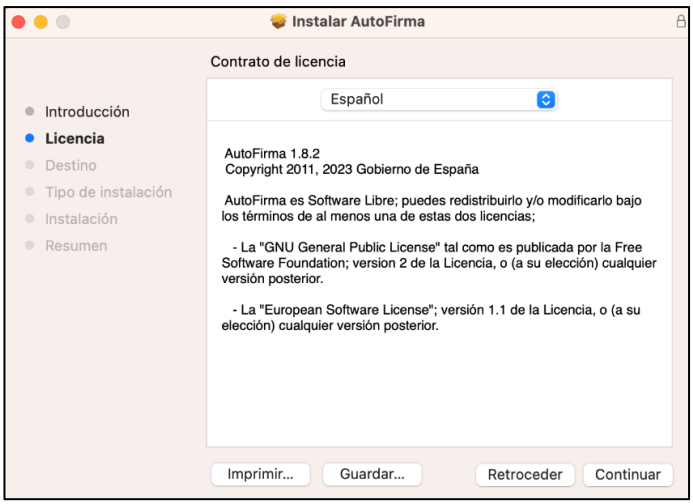

Imagen 3. Licencia de Autofirma

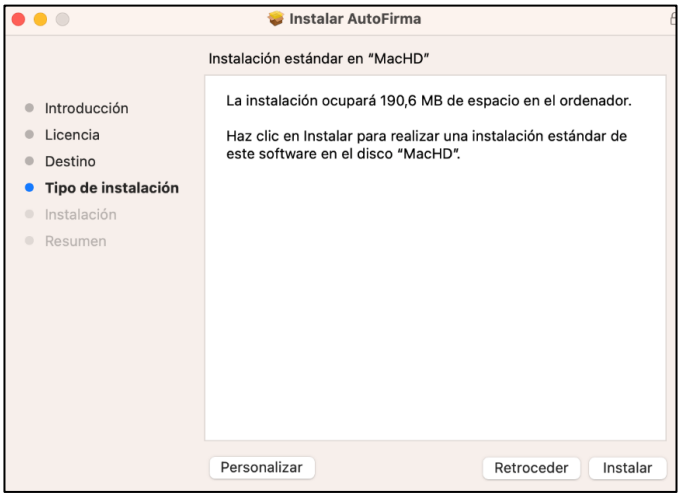

Imagen 4. Espacio utilizado en disco.

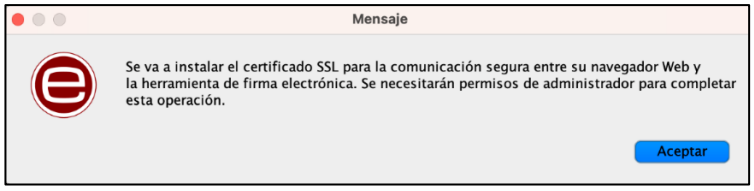

Imagen 5. Mensaje certificado SSL.

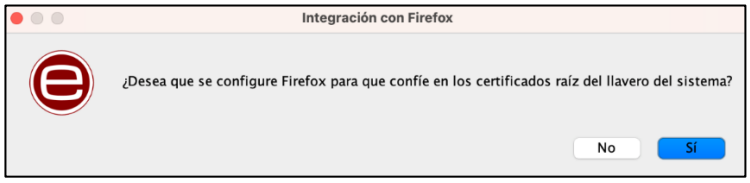

Imagen 6. Mensaje configuración certificados de Firefox.

5. Una vez finalizada la instalación tenemos la opción de conservar el instalador o trasladarlo a la papelera.
6. Llegados a este punto ya tenemos instalada la aplicación que se podrá utilizar de forma autónoma para la firma de documentos o como complemento del navegador en el momento de identificarse o firmar (Imagen 7).

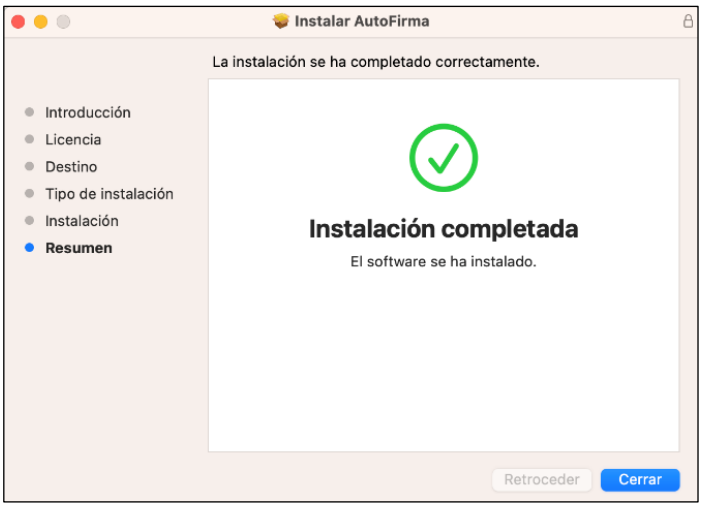

Imagen 7. Instalación completada.

3.2. ACTUALIZACIÓN DE LA APLICACIÓN

Para comprobar que versión tenemos instalada en el equipo bastará con abrir el programa y fijarnos en la barra superior de la ventana donde aparece el número de la versión (versión v1.8.2 en la imagen 8, la versión actual es la v1.8.4).

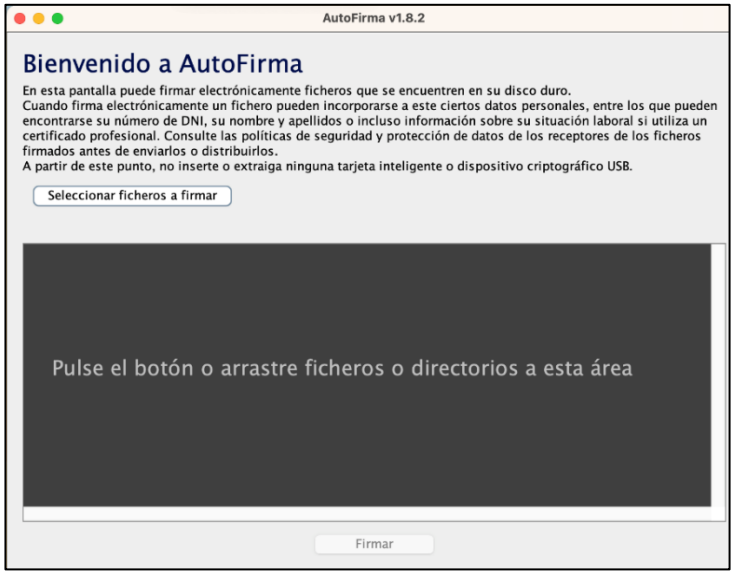

Imagen 8. Página de principal del programa Autofirma.

En el caso de tener una versión antigua del programa deberemos actualizarla a la última versión disponible en:

https://firmaelectronica.gob.es/Home/Descargas.html

Para actualizar la aplicación debemos seguir los mismos pasos de la instalación, con la salvedad de que la secuencia de actualización nos informará de que para realizar la misma el programa no puede estar en ejecución.

3.2.1. PROBLEMAS EN LA ACTUALIZACIÓN DEL PROGRAMA 'AUTOFIRMA'

Puede ocurrir que durante el proceso de actualización se elimine el certificado 'AutoFirma ROOT' del Sistema y debamos instalar el certificado de nuevo. Para ello accederemos a la carpeta:

'/Users/nombredelusuario/Library/Application Support/AutoFirma'

Procederemos a la instalación del certificado haciendo doble clic sobre 'AutoFirma_ROOT' (Imagen 9).

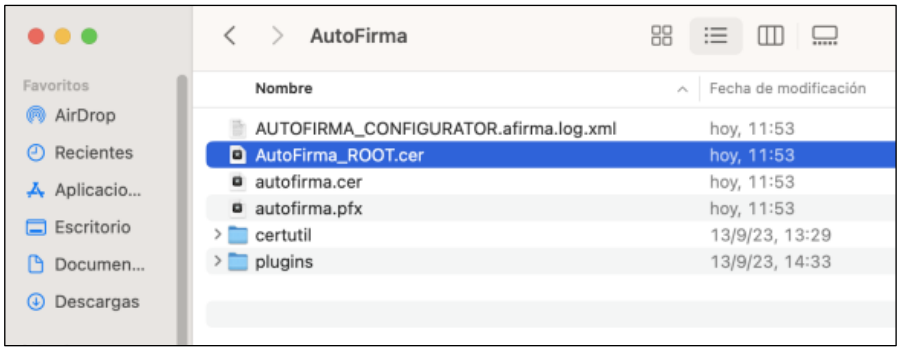

Imagen 9. Contenido de la carpeta 'Autofirma'.

Una vez instalado el certificado debemos confiar en él para poder utilizarlo. Esto lo haremos desde el 'Acceso a Llaveros' accediendo al certificado y seleccionando la opción de 'confiar siempre' (Imágenes 10 y 11).

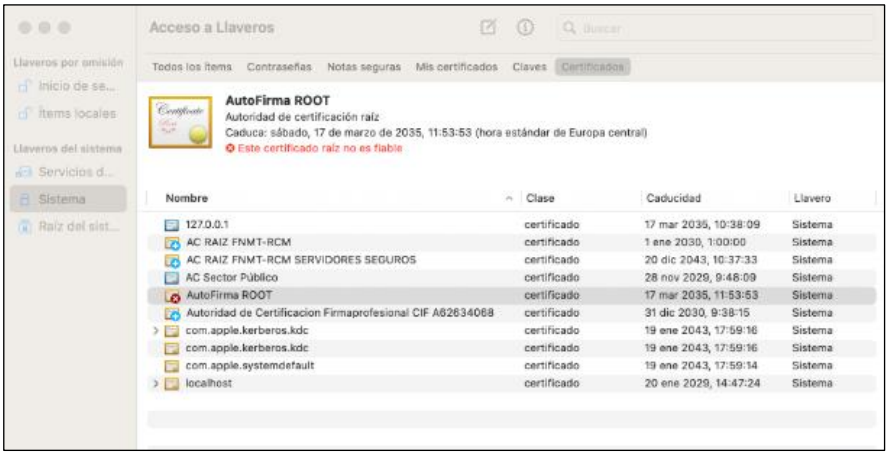

Imagen 10. Acceder a los certificados de Sistema del Llavero.

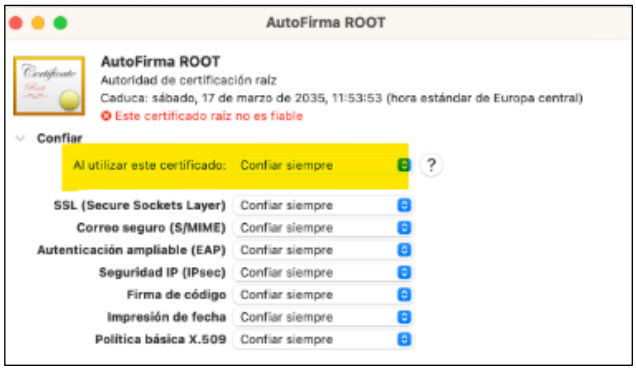

Imagen 11. Configurar el certificado 'Autofirma ROOT' en modo 'Confiar Siempre'.

3.3. INSTALACIÓN DEL PLUGIN DE HUELLAS DIGITALES V1.0

El Plugin para el cálculo y la comprobación de hashes versión v1.0 es un componente que permite generar ficheros de hashes con el hash de un fichero o de todos los ficheros de un directorio. También permite comprobar que un fichero de hashes es válido seleccionado el fichero o el directorio a partir del cual se generó.

IMPORTANTE: El plugin requiere de Autofirma v1.8 o superior (no es compatible con la versión 1.7.2 y anteriores). En versiones de Autofirma anteriores a la v1.8 la funcionalidad del plugin estaba integrada en la aplicación. Su paso a plugin se ha realizado para facilitar su gestión y evolución.

Los pasos para instalar el plugin de Huellas Digitales v1.0 son los siguientes:

1. Descargar el instalador en desde: https://firmaelectronica.gob.es/Home/Descargas.html

2. Abrir el programa de Autofirma y acceder desde el menú a la opción ‘Herramientas’ y después a la opción ‘Gestionar Plugins’ (Imagen 12).

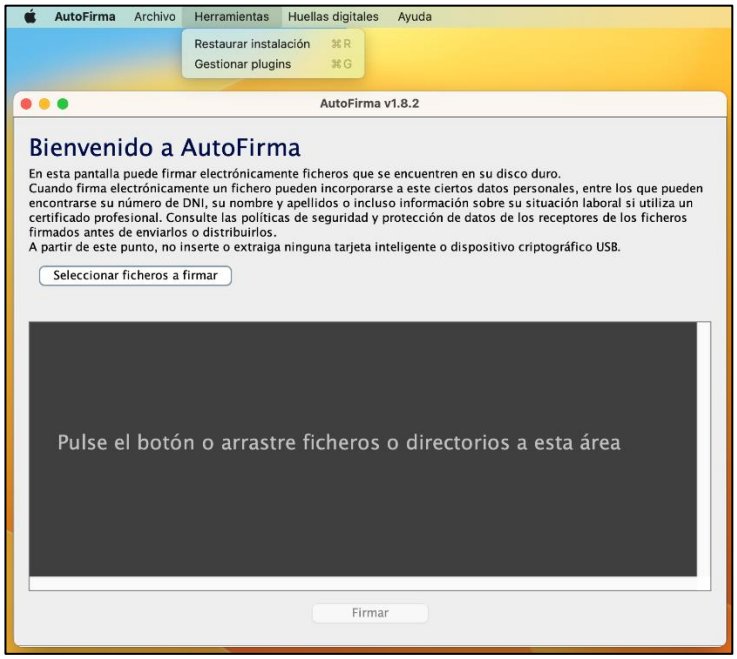

Imagen 12. Menú de herramientas.

3. Seleccionar la opción de ‘Agregar’ en el Gestor de plugins (Imagen 13).

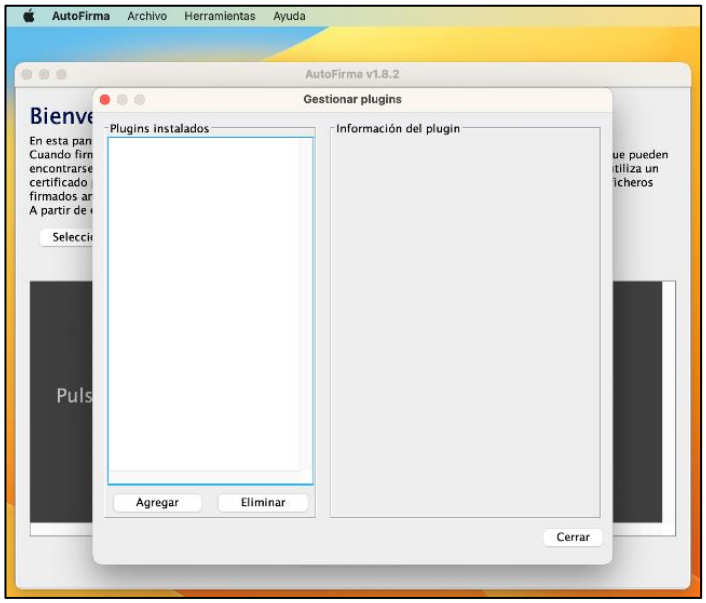

Imagen 13. Gestor de plugins.

4. Seleccionar el paquete instalador descargado previamente (Imagen 14).

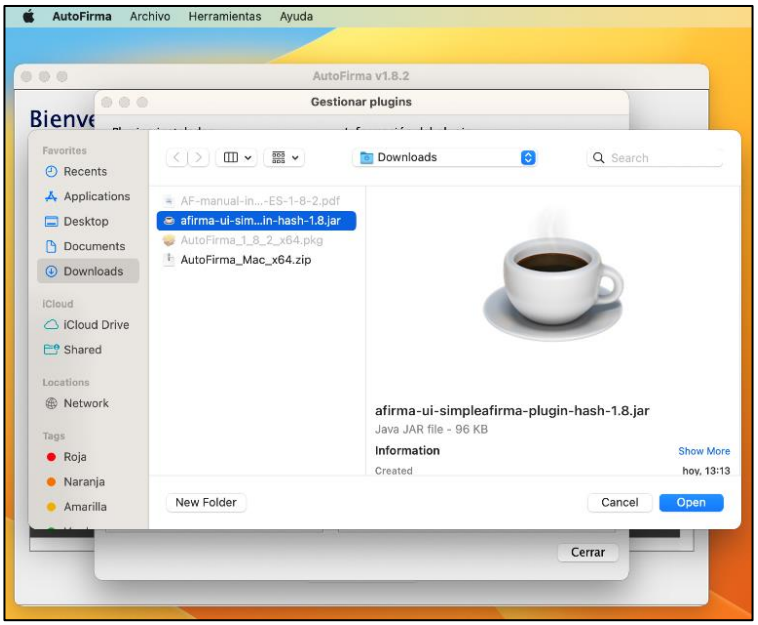

Imagen 14. Seleccionar el paquete instalador.

5. La instalación le informará que el plugin se encuentra firmado por 'Firma de código Java Secretaría General de Administración Digital' (Imagen 15).

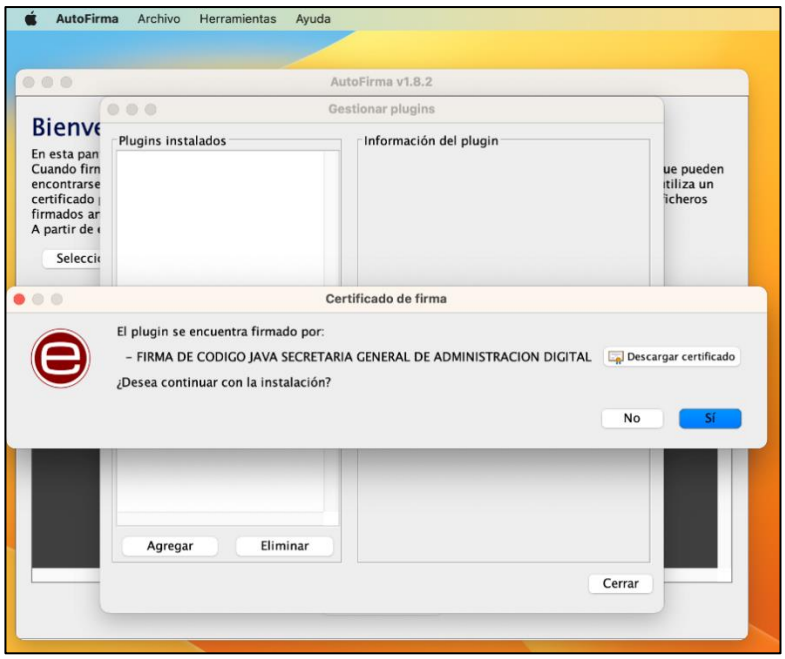

Imagen 15. Mensaje del certificado de firma.

6. La instalación pedirá permisos para la instalación, reinicio, permiso para agregar la funcionalidad al menú y permisos para los nuevos comandos (Imagen 16).

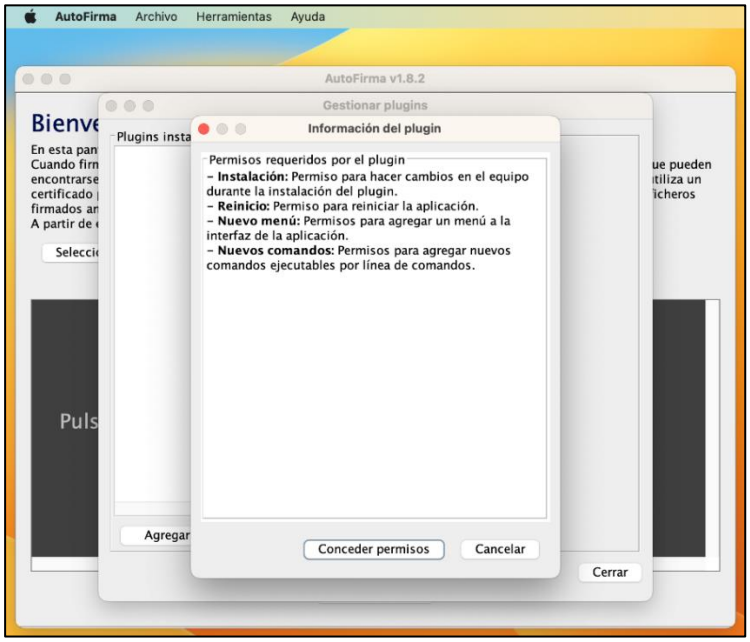

Imagen 16. Permisos de instalación.

7. Finalmente se reiniciará la aplicación (Imagen 17).

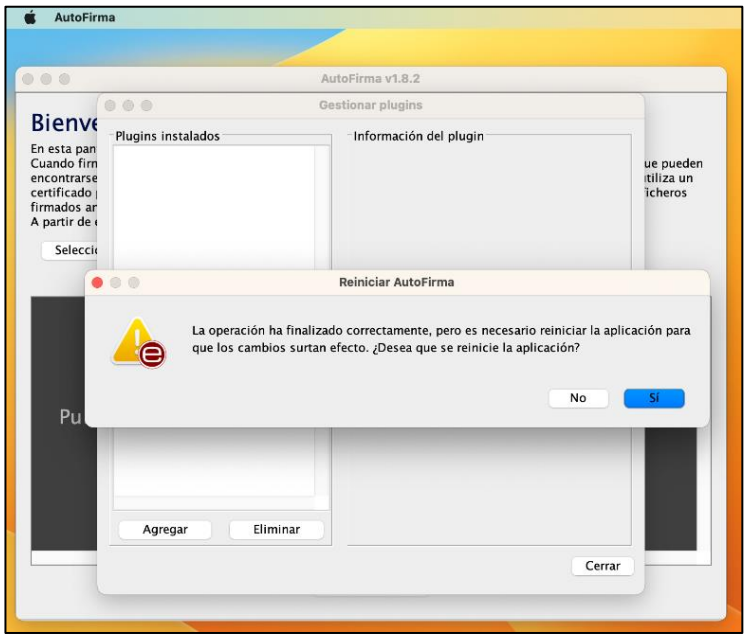

Imagen 17. Reinicio.

8. Puede comprobar que el plugin está correctamente instalado abriendo la aplicación y observando que el menú incluye la opción de 'Huellas digitales', y además dentro del gestor de plugins aparece dentro de los plugins instalados (Imagen 18).

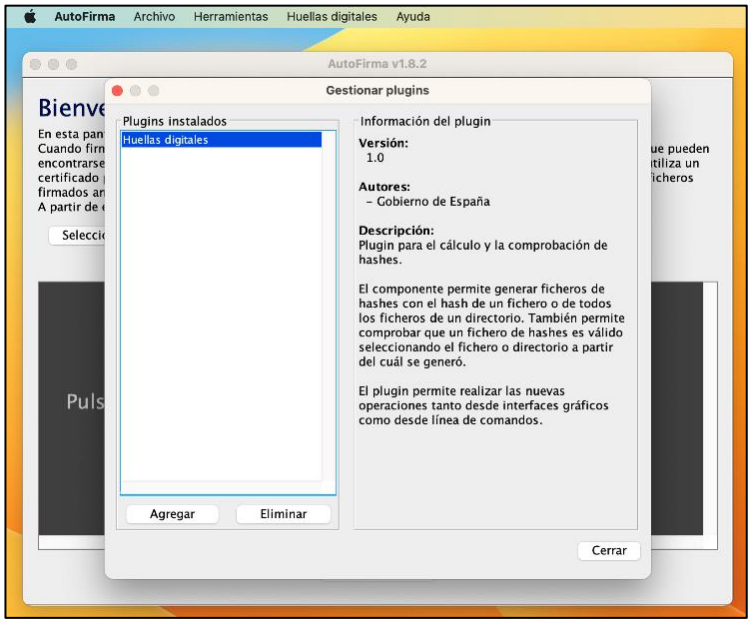

Imagen 18. Instalación completada.

3.3.1. PROBLEMAS EN LA INSTALACIÓN DEL PLUGIN DE HUELLAS DIGITALES V1.0

Ocasionalmente se han observado problemas en la instalación del plugin cuando la carpeta de instalación no tiene los permisos de usuario adecuados. En ese caso será necesario dotar a la carpeta de instalación con los permisos pertinentes:

'/`Users/nombredelusuario/Library/Application Support/AutoFirma`'

El usuario debe tener permiso en la carpeta `'Autofirma'`.

4. PROCEDIMIENTO ADICCIONAL SI EXISTEN PROBLEMAS PARA REALIZAR LA FIRMA ELECTRÓNICA DEBIDO A LA CONFIGURACIÓN DE LOS CERTIFICADOS DE AUTOFIRMA

Si tiene problemas para acceder a la plataforma de tramitación o realizar la firma electrónica con su certificado electrónico debe realizar los siguientes pasos:

4.1. ACCEDER AL LLAVERO DE MAC.

El almacén de certificados para un ordenador Mac es el que se conoce como Llaveros.

4.2. ACCEDER AL LLAVERO 'SISTEMA' Y A LA OPCIÓN DE 'CERTIFICADOS'.

Dentro del 'Acceso a Llaveros' de su ordenador seleccione el Llavero de 'Sistema' y haga clic en la opción 'Certificados' (Imagen 19).

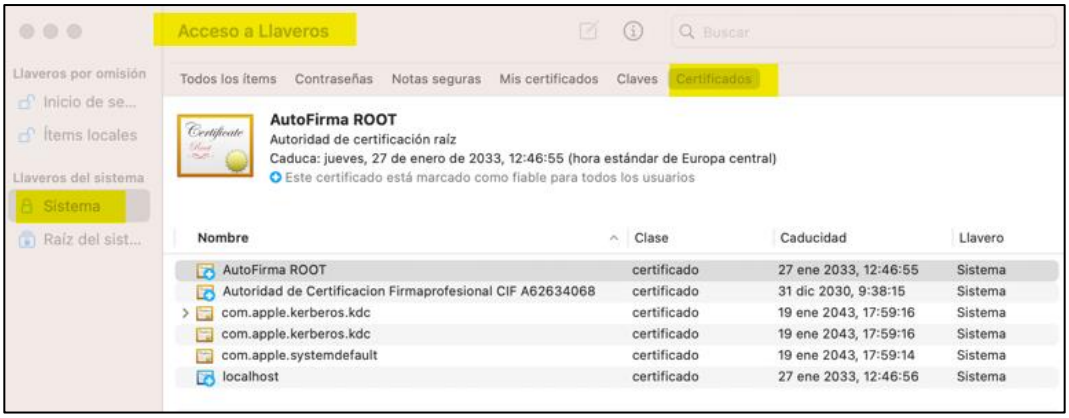

Imagen 19. Llavero de Mac

Los certificados '**Autofirma ROOT**' y '**127.0.0.1**' o '**localhost**' se deben configurar ambos con la opción de 'Confiar Siempre' (Imágenes 20, 21 y 22).

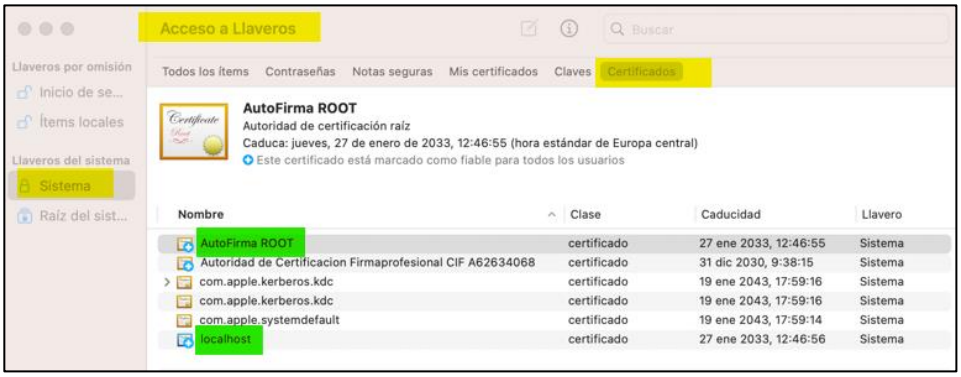

Imagen 20. Acceder a los certificados de Sistema del Llavero.

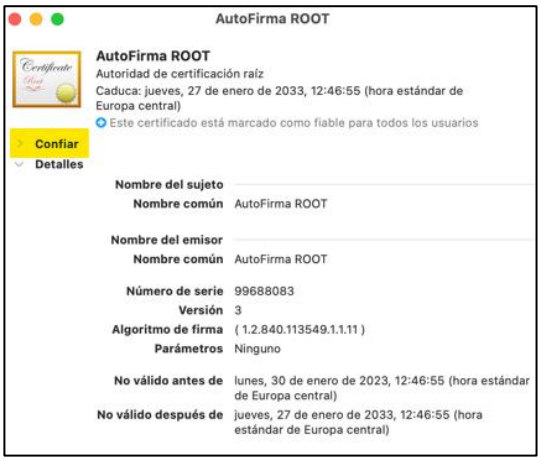

Imagen 21. Acceder al certificado 'Autofirma ROOT'.

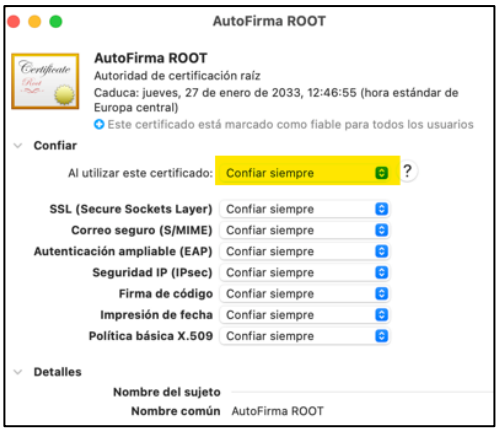

Imagen 22. Configurar el certificado 'Autofirma ROOT' en modo 'Confiar Siempre'.

Se deben realizar las mismas acciones para “localhost” o “127.0.0.1”.

Una vez cerremos esta ventana haciendo clic en el círculo rojo de la esquina superior izquierda el sistema nos pedirá confirmar los cambios introduciendo la contraseña de nuestro ordenador.

4.3. ACCEDER AL LLAVERO DE ‘INICIO DE SESIÓN’ Y A LA OPCIÓN ‘MIS CERTIFICADOS’.

A continuación, seleccione el Llavero de ‘Inicio de Sesión’ y haga clic en la opción de ‘Mis Certificados’ (Imagen 23).

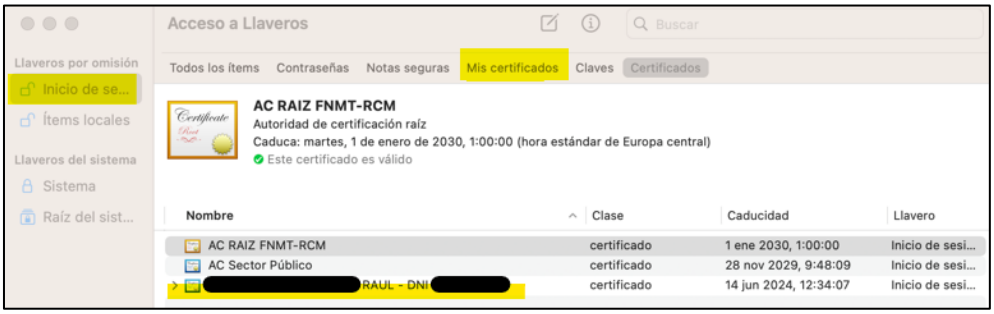

Imagen 23. Seleccionar su certificado digital en ‘Inicio de sesión’ en ‘Mis certificados’.

Allí deberá configurar su certificado digital con la configuración de “Confiar siempre” (Imagen 24).

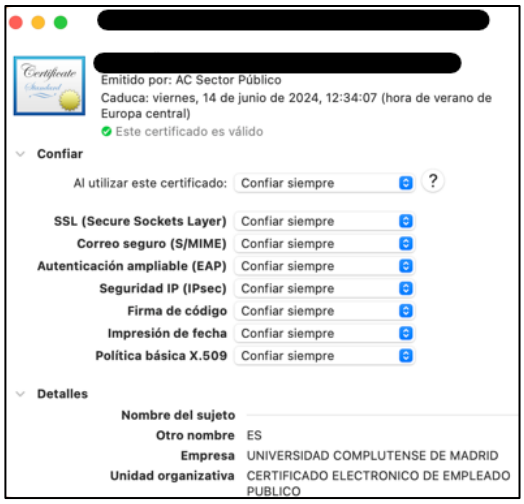

Imagen 24. Configurar el certificado digital en modo “Confiar Siempre”.

Para confirmar los cambios se le pedirá nuevamente la contraseña de su ordenador.

4.4. ACCEDER A LA SEDE ELECTRÓNICA.

Finalmente, vuelva a intentar conectarse a la Sede Electrónica de la UCM para comprobar si se conecta adecuadamente.

https://sede.ucm.es/

5. OTROS.

5.1. RECOMENDACIÓN DE LA UTILIZACIÓN DE DISTINTOS NAVEGADORES.

Cuando existen problemas en el uso de la plataforma recomendamos que se realicen las acciones requeridas en distintos navegadores (Chrome, Firefox, Safari, …)

Además, en el caso de Firefox y para el certificado electrónico es necesario que el certificado esté instalado en el almacén de certificados de este navegador; o conceder permiso al navegador para acceder a los certificados del sistema, de tal modo que, cuando se seleccione 'Seleccione un certificado' → 'Cambiar almacén de claves' → 'Almacén de claves del sistema', el navegador tenga acceso al certificado.

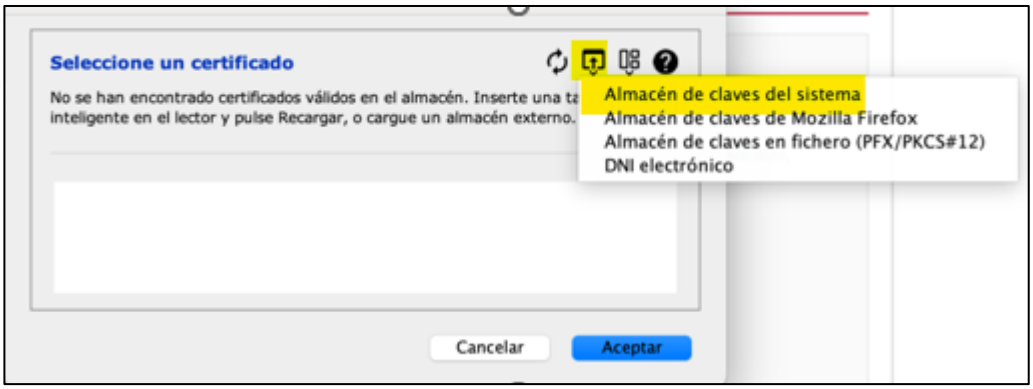

Imagen 25. Selección de certificado en Firefox.

Si se quiere utilizar el certificado en otros navegadores (Safari o Google Chrome) deberán estar instalados en el "Llavero" de Mac.

5.2. PROBLEMAS EN LA VALIDACIÓN DEL CERTIFICADO DIGITAL EN LA PLATAFORMA VALIDE.

La plataforma VALIDe permite, entre sus servicios, determinar la validez de firmas y certificados digitales.

Problemas en el uso de los servicios de la plataforma, en determinadas ocasiones, se han solventado realizando la reinstalación del programa Autofirma.

6. INSTALACIÓN DEL CERTIFICADO 'AC RAÍZ FNMT-RCM SERVIDORES SEGUROS' EN EQUIPOS APPLE OS X

En ocasiones se presenta el problema de acceso a la sede electrónica de la UCM (https://sede.ucm.es) a través del navegador nativo de MacOS (Safari).

Imagen 26. Advertencia del navegador Safari sobre el certificado de la sede.

Tenemos dos opciones para conseguir la conexión con la sede a través del navegador Safari:

1. Aceptar la conexión a pesar de la advertencia del navegador de que: "El certificado 'AC RAIZ FNMT-RCM SERVIDORES SEGUROS' no es fiable".
2. Instalar el 'Certificado AC Raíz FNMT-RCM Servidores Seguros' https://www.sede.fnmt.gob.es/descargas/certificados-raiz-de-la-fnmt

Pasos que seguir en la **instalación del certificado 'AC Raíz FNMT-RCM Servidores Seguros'**:

1. Descargar el certificado 'AC Raíz FNMT-RCM Servidores Seguros'.

Imagen 27. Página de descarga del certificado
https://www.sede.fnmt.gob.es/descargas/certificados-raiz-de-la-fnmt

2. Acceder a la carpeta de descargas.

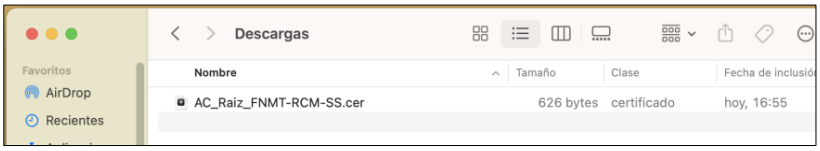

Imagen 28. Carpeta de descargas con el certificado descargado.

3. Hacer doble clic en el archivo para instalar el certificado en el llavero de certificados.

4. Acceder al llavero de certificados para conceder permisos de confianza sobre el mismo.

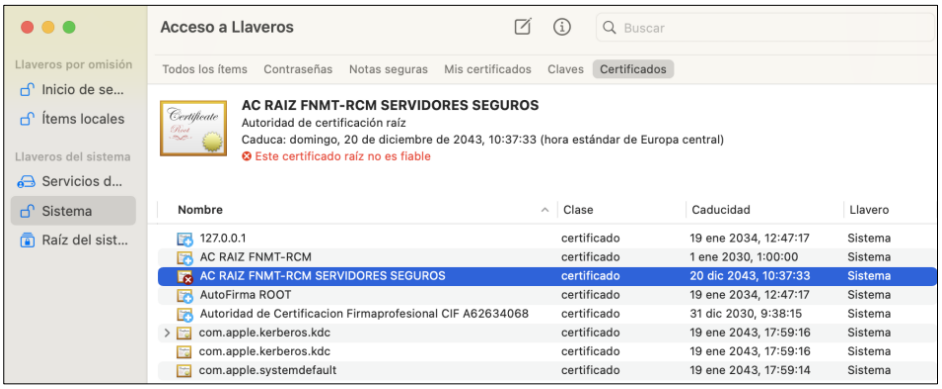

Imagen 29. Llavero de certificados, vista de los certificados instalados.

Imagen 30. Conceder permisos de confianza al certificado 'Confiar siempre'.

5. Acceder a la sede electrónica (https://sede.ucm.es), y comprobar que el certificado está correctamente instalado (pinchando sobre el candado de la url de navegación).

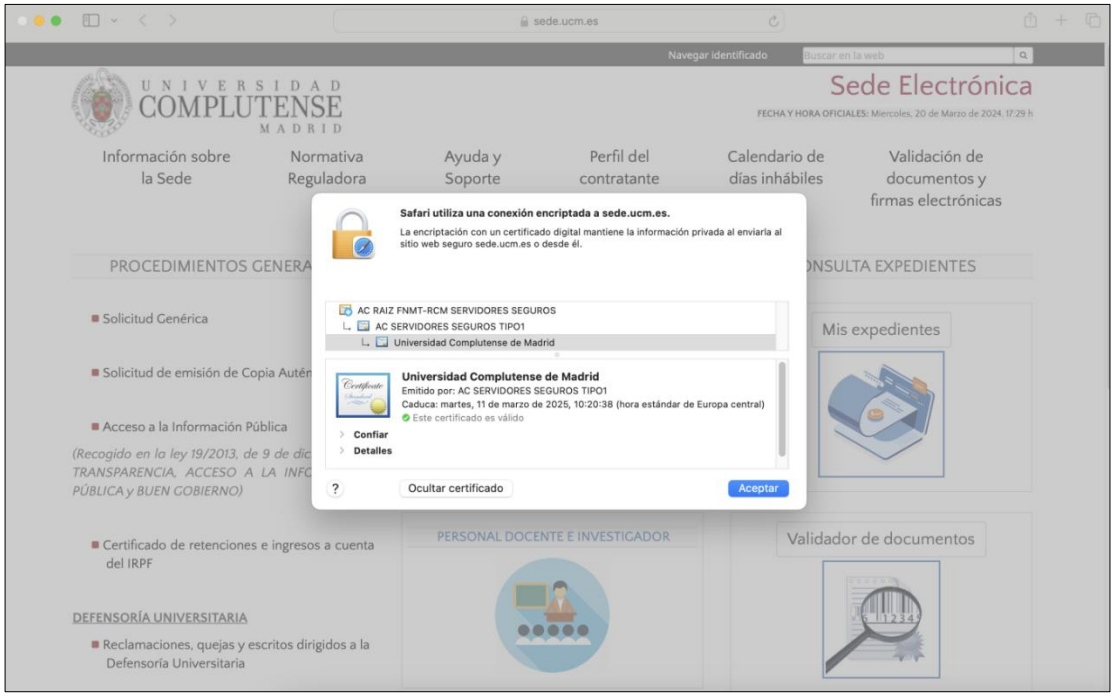

Imagen 31. El certificado está correctamente instalado y tiene permisos de confianza.

7. INSTALACIÓN DEL CERTIFICADO 'AC RAÍZ FNMT-RCM SERVIDORES SEGUROS' EN DISPOSITIVOS MÓVILES CON APPLE IOS

En los dispositivos móviles de Apple con sistema operativo iOS se debe realizar la **instalación del certificado 'AC Raíz FNMT-RCM Servidores Seguros'**:

1. Descargar el certificado 'AC Raíz FNMT-RCM Servidores Seguros' en: *https://www.sede.fnmt.gob.es/descargas/certificados-raiz-de-la-fnmt*

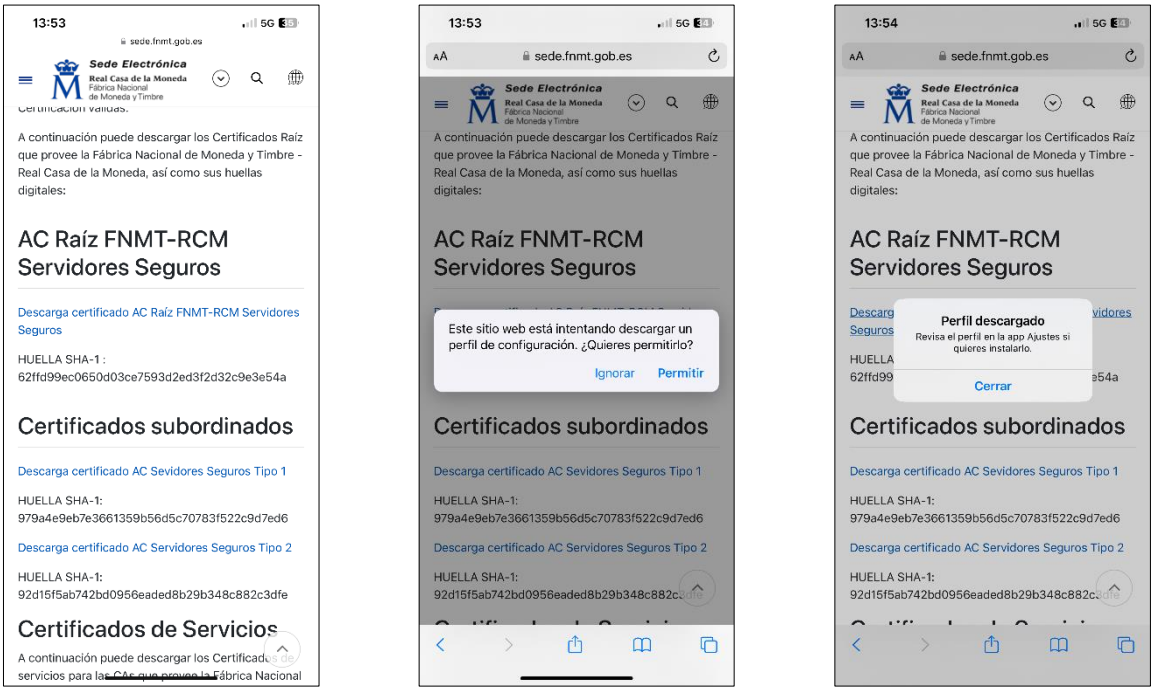

Imagen 32. Página de descarga del certificado
https://www.sede.fnmt.gob.es/descargas/certificados-raiz-de-la-fnmt

2. Acceder a la configuración del dispositivo para acceder al nuevo 'perfil descargado'.

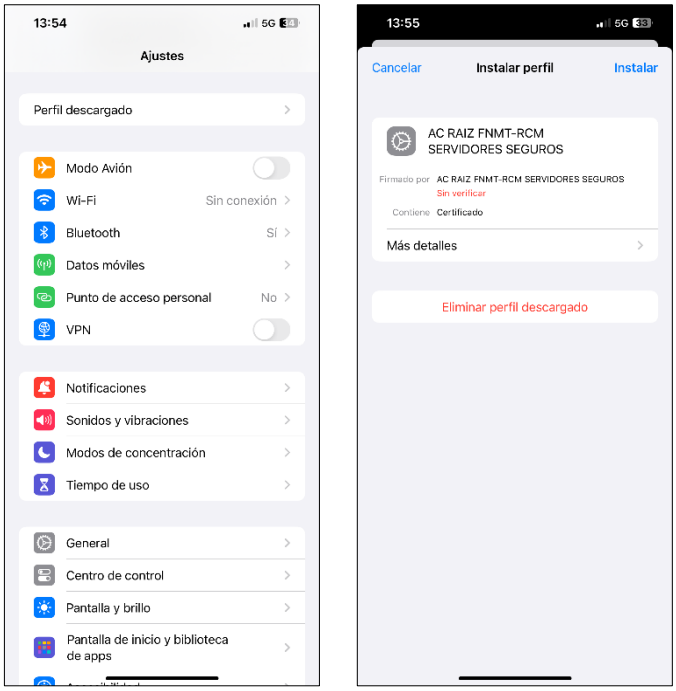

Imagen 33. Acceder al 'perfil descargado'

3. Instalar el nuevo perfil.

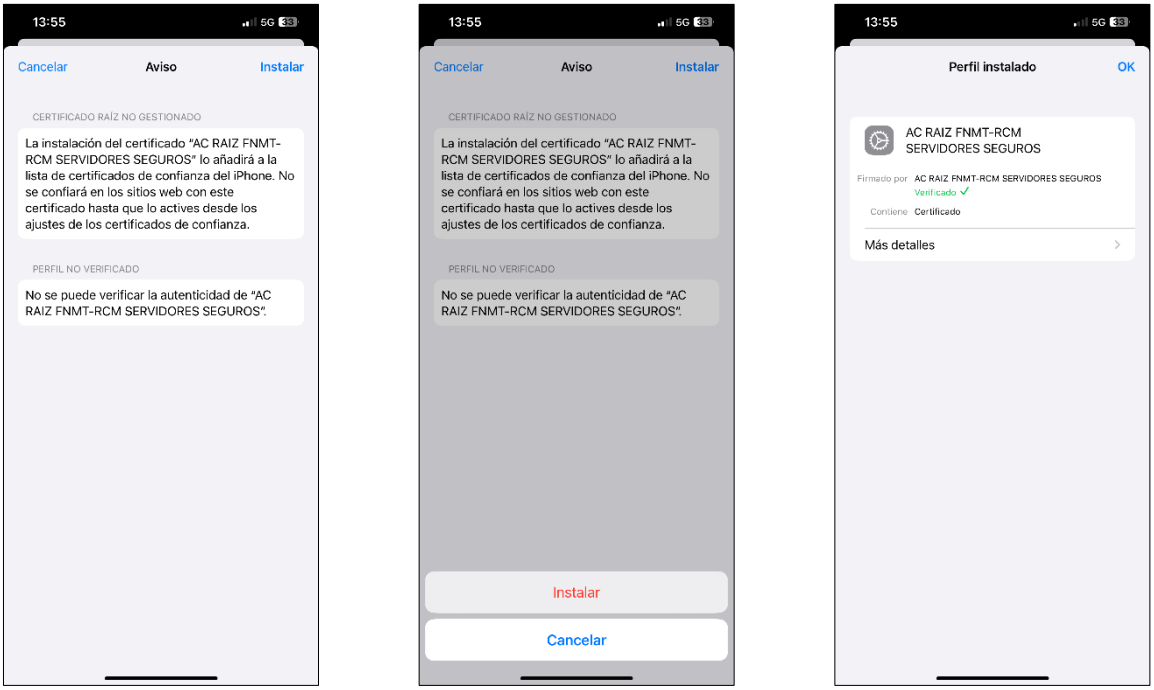

Imagen 34. Instalar el nuevo perfil

4. Acceder a ‘VPN y Gestión de dispositivos’ para conceder permisos de confianza sobre el certificado raíz **‘AC Raíz FNMT-RCM Servidores Seguros’.**

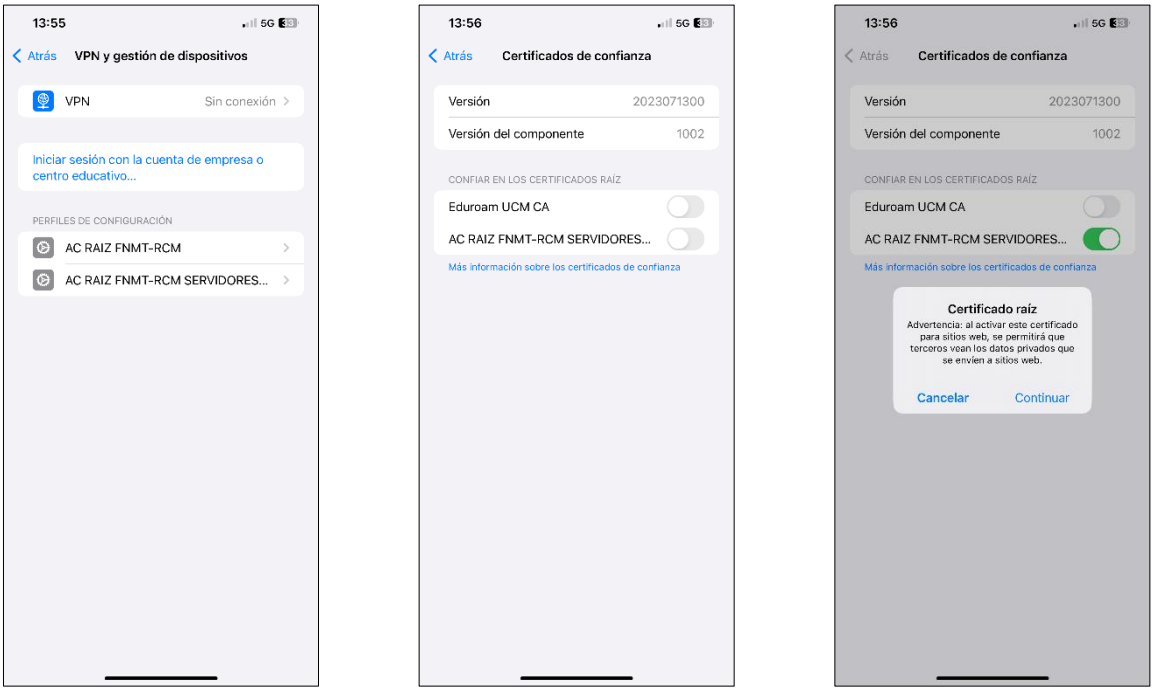

Imagen 35. Conceder permisos de confianza sobre el certificado raíz ‘AC Raíz FNMT-RCM Servidores Seguros’

5. Acceder a la sede electrónica (https://sede.ucm.es), y comprobar que el certificado está correctamente instalado.