Manual de Usuario

UKC Desktop para macOS

Contenido

1. Introducción

El presente manual recoge una guía de usuario para el uso de los certificados digitales remotos almacenados en SignCloud (nube de Uanataca) en macOS.
En el capítulo 2 se explica cómo utilizar el certificado digital remoto.

2. Certificado digital remoto con UKC Desktop en macOS.

El presente documento tiene el objetivo de guiar al usuario a través del software **UKC Desktop** para el uso de certificados digitales custodiados en el sistema SignCloud de Uanataca.
En él se detalla el proceso de instalación del UKC Desktop, así como su uso.
A través de la aplicación middleware UKC Desktop, el usuario podrá de manera muy sencilla firmar electrónicamente y autenticarse en páginas web.
Para ello se requieren las credenciales utilizadas en el proceso de generación del certificado (Usuario, Contraseña y código PIN)

2.1 Instalar el programa UKC Desktop en macOS

A continuación, se detalla el procedimiento para llevar a cabo la instalación del software UKC Desktop en macOS.

1. Descargar el programa UKC Desktop.
2. Ejecutar el archivo y seguir el proceso de instalación.

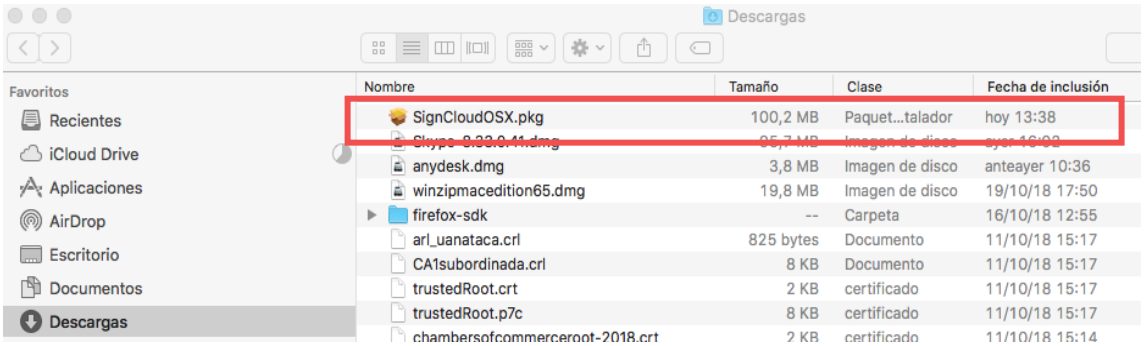

Figura 1. Descarga en macOS de SignCloud

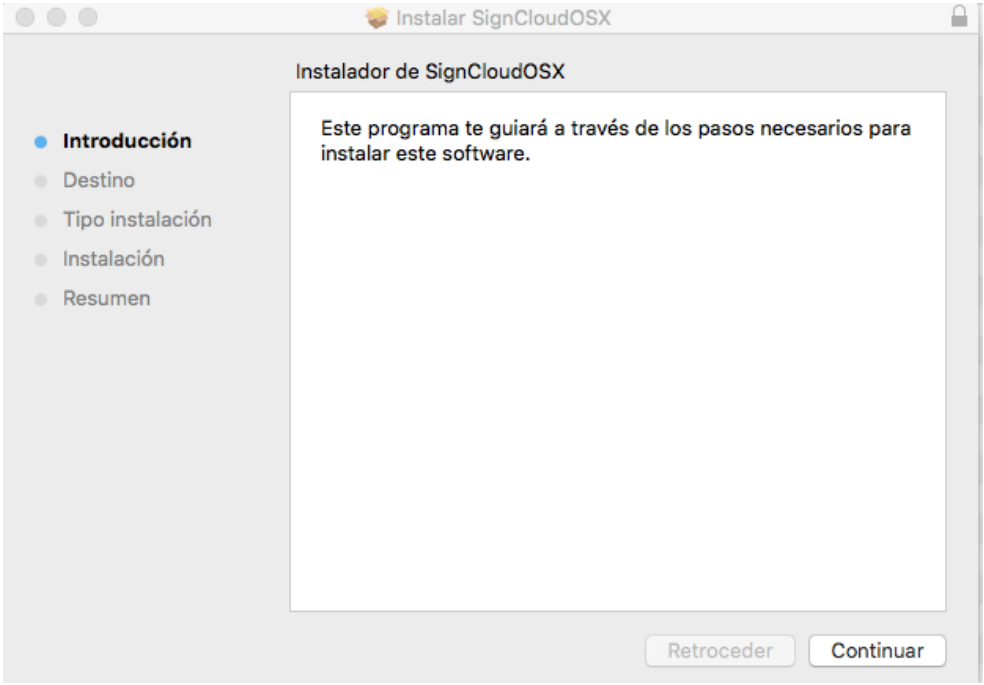

Figura 2. Asistente instalación de UKC Desktop macOS de SignCloud

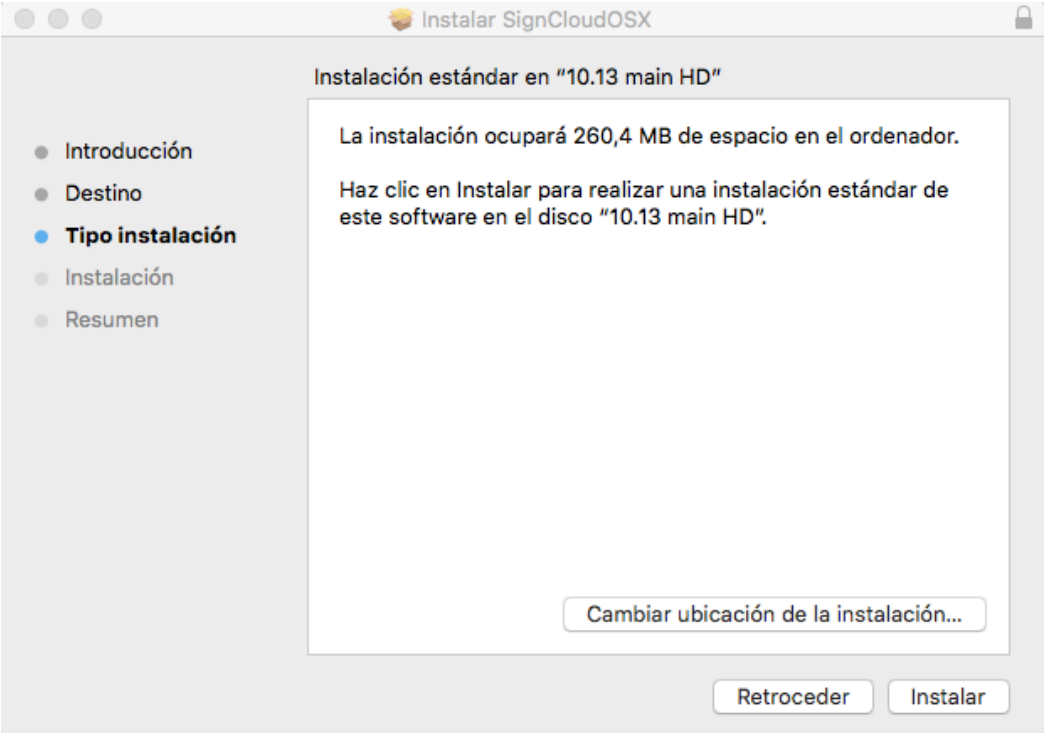

Figura 3. Asistente ubicación instalación de UKC Desktop macOS de SignCloud

4. Instalar software
5. Cerrar el instalador una vez completada la instalación.

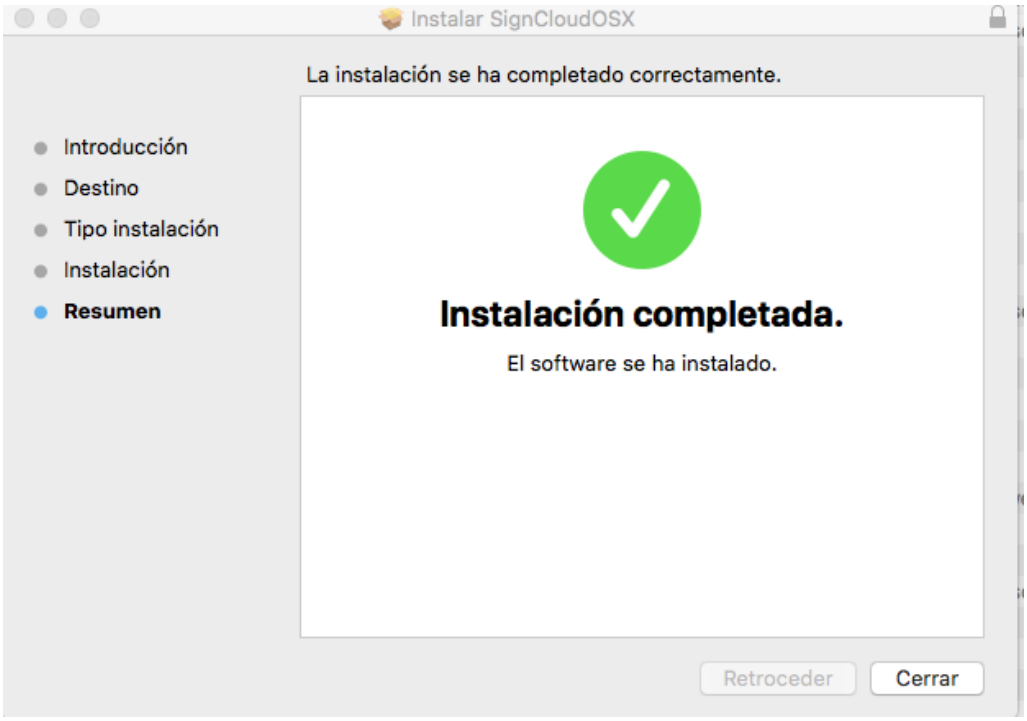

Figura 4. Instalación completada de UKC Desktop macOS de SignCloud

2.2. Configuración del programa UKC Desktop en macOS.

Para poder utilizar las funcionalidades de UKC Desktop con certificados remotos es necesario disponer de un certificado digital emitido en el sistema SignCloud de Uanataca. Esta identidad o certificado remoto tiene asociadas las siguientes credenciales, que permiten utilizar los servicios de firma electrónica:

- Usuario (entregado en mano en el documento “Carta de Credenciales”, cuando el usuario se identificó en la autoridad de registro.
- Contraseña (contenida en el email que le fue enviado al usuario, cuando éste se identificó en la autoridad de registro)
- Código PIN (elegido e introducido por el usuario cuando se generó el certificado digital)

El programa UKC Desktop se ejecuta automáticamente cuando se arranca el Mac. Para acceder a la aplicación, debemos presionar el icono que aparece en la barra de tareas.

Figura 5. UKC Desktop en la barra de herramientas superior

2.2.1. Contenido y configuración en macOS

Una vez abierto UKC Desktop, nos muestra la ventana principal.

Figura 6. Ventana principal de UKC Desktop

Esta vista principal está compuesta por un menú superior con diferentes opciones. Cada una de estas opciones permite llevar a cabo tareas diversas. A continuación, se definen en detalle cada una de ellas:

Archivo:

- **Salir**. Esta opción cierra la aplicación UKC Desktop.
-

Configuración:

- **Red**: En caso de ser necesario, permite configurar un servidor Proxy.
- **Tarjeta/Token**: Desde esta opción podremos gestionar las credenciales PIN (cambiar y desbloquear) y PUK (cambiar) de las tarjetas y tokens criptográficos del fabricante Bit4id que eventualmente estén conectados al Mac.
- **SignCloud:** Esta opción permite gestionar los certificados digitales custodiados en el sistema SignCloud de Uanataca.
  - Iniciar sesión en el sistema SignCloud a través de la opción **"Conectar"**. La aplicación solicitará las credenciales necesarias.
  - Para cerrar sesión en el sistema SignCloud debemos utilizar la opción "**Desconectar"**.
  - Durante el inicio de sesión, el sistema permite memorizar (**"Memorizar esta acción**") las credenciales **"Usuario"** y **"Contraseña"** para evitar introducirlas cada vez que ejecutemos la aplicación.
  - Marcando la opción "**Descartar Credenciales**" borraremos la información memorizada.
  - Se puede cambiar la contraseña asociada a nuestro certificado digital remoto a través de la opción "**Cambiar contraseña**". Cualquier tipo de cambio en las credenciales (PIN, PUK y contraseña) del certificado digital remoto requiere contar con las credenciales en vigor.

Acerca…:

Muestra información acerca de la versión de UKC Desktop instalada.

Figura 7. Cambiar contraseña

2.2.2. Inicio de sesión en SignCloud macOS

El inicio de sesión permite acceder al certificado digital custodiado en el sistema SignCloud de Uanataca, cargándola en el Mac y constituye la fase de identificación del usuario. No obstante, para poder utilizar dicho certificado digital en los servicios de firma y/o autenticación, necesitaremos el código PIN (sea estático o dinámico), completando así el proceso de autenticación para el desbloqueo de la firma.

Para poder iniciar sesión en el sistema SignCloud, seleccionamos dentro de "Configuración" la opción **"SignCloud"** y seguidamente **"Conectar…"**:

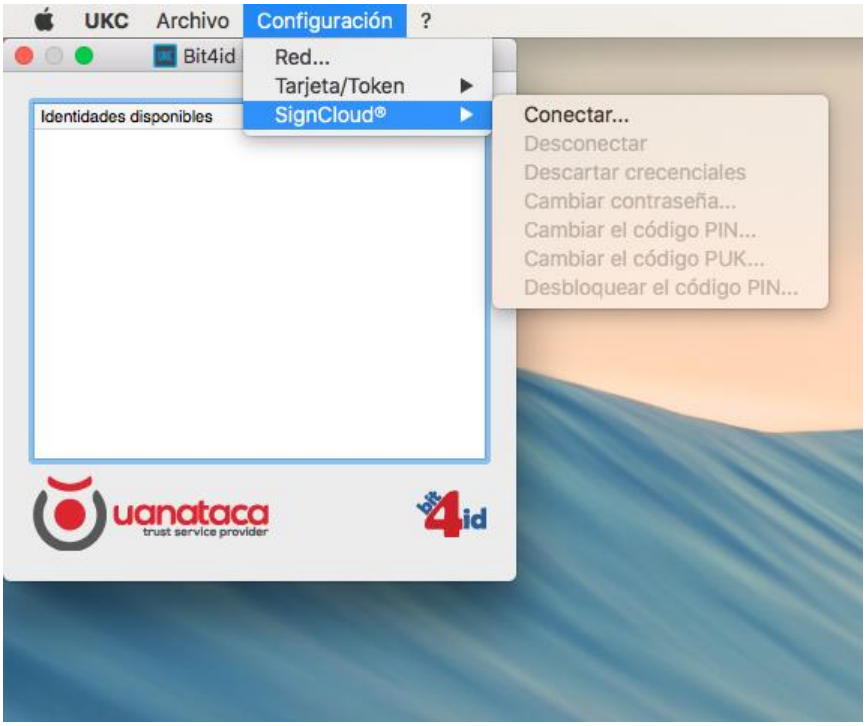

Figura 8. Conectarse al sistema SignCloud

La aplicación muestra una ventana donde debemos introducir las credenciales identificativas "Usuario" y "Contraseña" asociados a nuestro certificado digital remoto.

Figura 9. Iniciar sesión en SignCloud

A partir de este momento, el certificado digital remoto se encuentra cargado en el sistema y listo para ser utilizado.

Figura 10. Vista de certificados digitales disponibles

2.3 Cómo utilizar el programa UKC Desktop

UKC Desktop actúa como un proveedor de identidades digitales remotas en el sistema. Esto quiere decir que no es un motor de firma electrónica en sí mismo, ya que no genera firmas PAdES, XAdES o CAdES por sí solo.

En otras palabras, las aplicaciones instaladas en el sistema que sean motores de firma (Ej. PDF Adobe Acrobat Reader, Microsoft Word, 4identity, AutoFirma, etc.) harán uso de los certificados digitales ofrecidos por UKC Desktop para llevar a cabo las firmas electrónicas.

2.4 Firma electrónica de un documento en macOS.

Para firmar un documento utilizando PDF Adobe Acrobat Reader con un certificado digital en macOS por primera vez, se tiene que configurar primero.

Los pasos a seguir son:

1. Ir a “preferencias”

Figura 11. Configuración Adobe Acrobat Reader con certificado digital en macOS

2. Seleccionar “Firmas.
3. Ir a “Crear y administrar identidades para firmar”

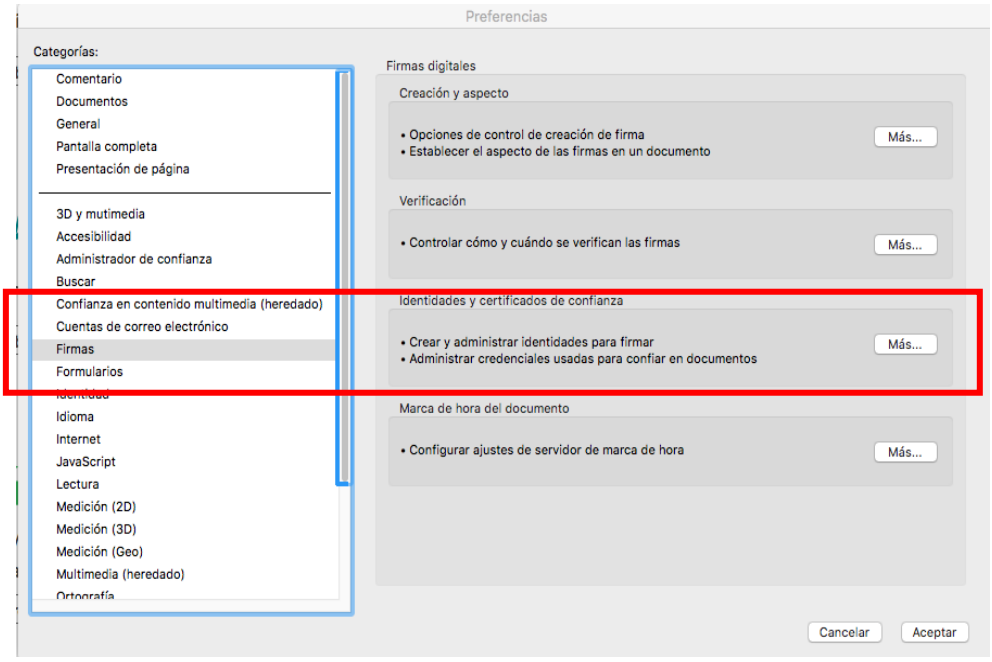

Figura 12. Configuración Adobe Acrobat Reader con certificado digital en macOS

4. Seleccionar “Módulos y distintivos PKCS#11”
5. Adjuntar módulo

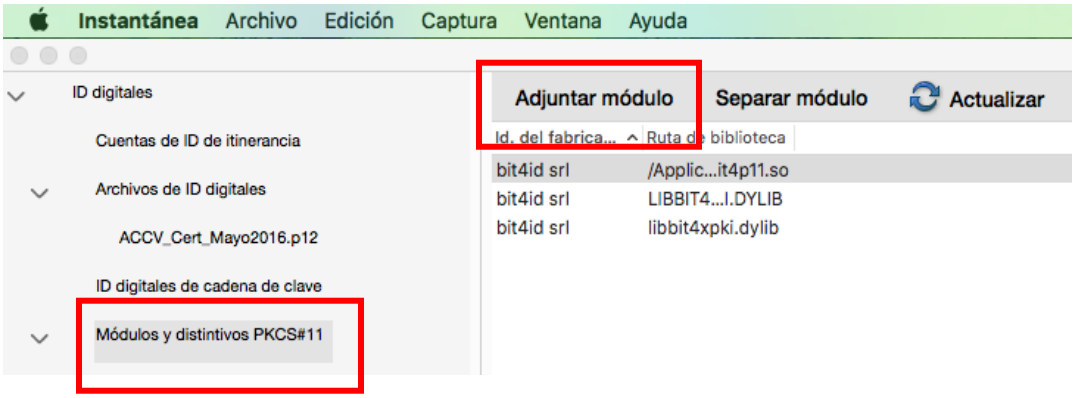

Figura 13. Configuración Adobe Acrobat Reader con certificado digital en macOS

6. Insertar la siguiente ruta en la “Ruta de biblioteca”:

/Applications/UniversalKeychain/UniversalKeychain.app/Contents/Resources/pkcs11/libbit4p11.so

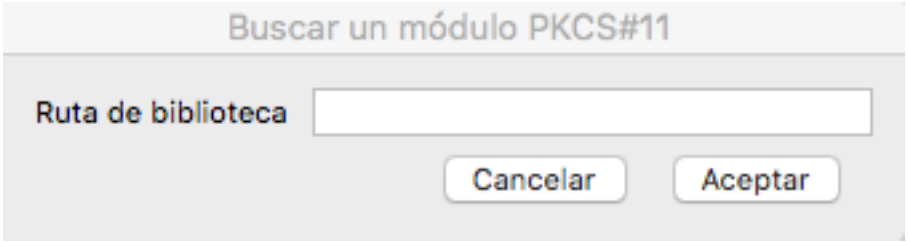

Figura14.Configuración Ruta de biblioteca Adobe Acrobat Reader con certificado digital en macOS

La configuración estará realizada.

Ya podrá firmar documentos con el programa PDF Adobe Reader.

2.5 Ejemplo de firma electrónica de un documento en macOS.

Una vez configurado nuestro certificado digital en **PDF Adobe Acrobat Reader,** a continuación, se muestra un ejemplo de cómo firmar un documento.

Abrir el documento PDF que se desea firmar desde la aplicación Adobe Acrobat Reader.

1. Acceder al menú “Herramientas” y seleccione “Certificados”.
2. En la barra “Certificados” abrir la opción “Firmar Digitalmente”.

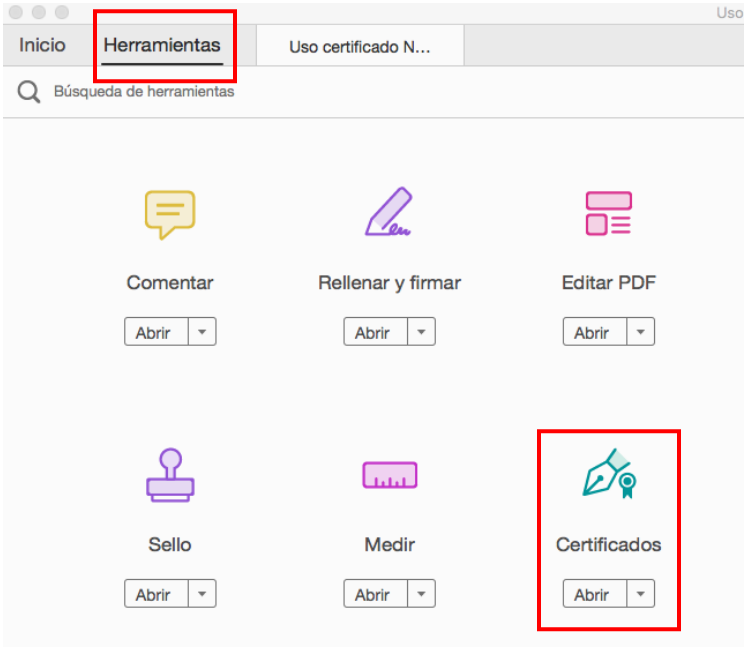

Figura 15. Herramientas en el sistema (PDF Adobe Acrobat Reader)

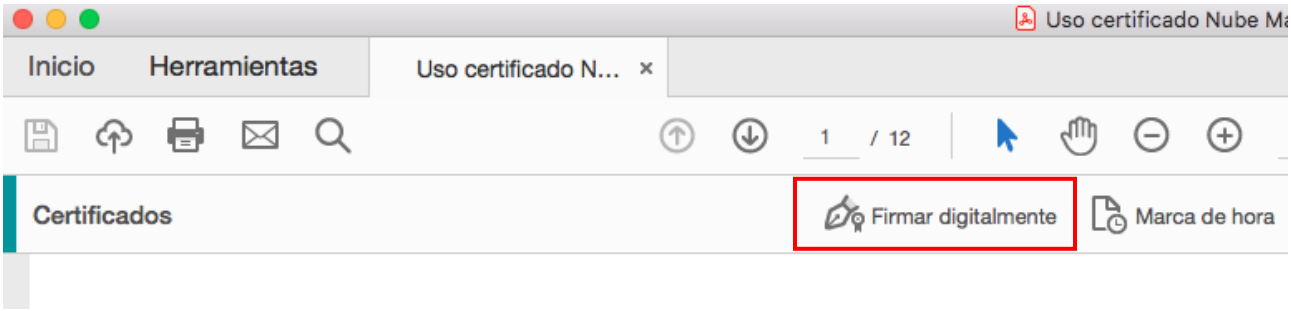

Figura 16. Firmar digitalmente en el sistema (PDF Adobe Acrobat Reader)

3. A continuación, aparece el menú de firma y los certificados digitales disponibles. Seleccione y pulse continuar.

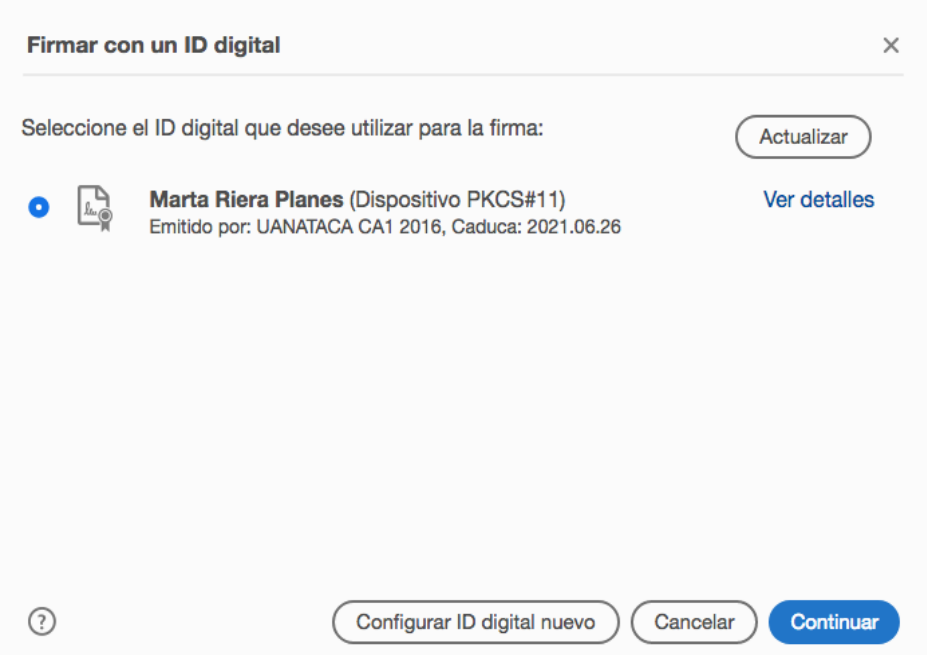

Figura 17. Seleccionar el certificado digital en el sistema (PDF Adobe Acrobat Reader)

6. Seguidamente se muestra el menú de firma. Presionamos Firmar.

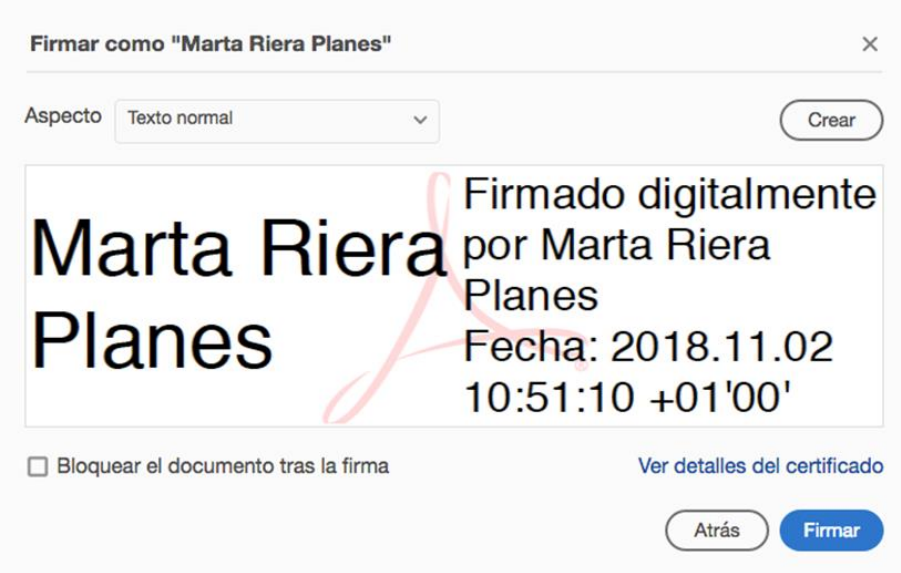

Figura 18. Menú de firma

8. Guardarmos el documento a firmar.

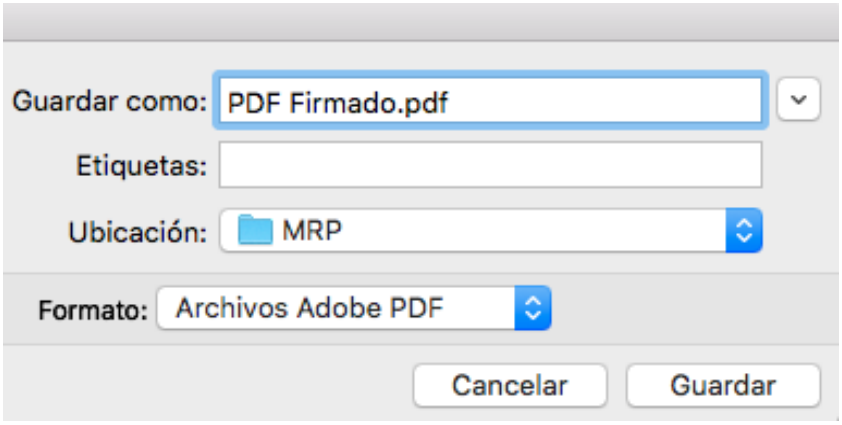

Figura 19. Guardar documento a firmar

7. UKC Desktop solicitará el código PIN para autorizar la firma electrónica del documento.

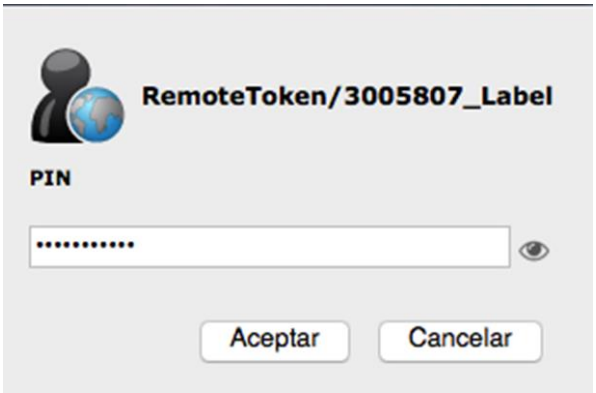

Figura 20. Inserción de PIN de firma por parte del usuario en UANATACA UKC Desktop

8. Al introducir el código PIN de forma satisfactoria, la firma electrónica del documento se llevará a cabo.

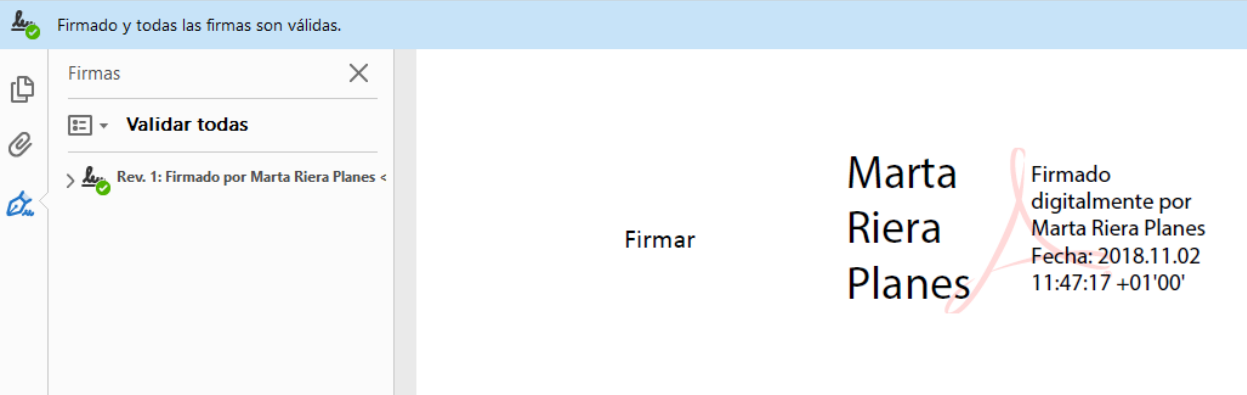

Figura 21. Firma electrónica válida

2.6 Autenticación con certificado en macOS.

Para poder hacer uso de nuestro certificado digital en macOS, recomendamos utilizar el navegador Firefox.

Antes de la primera autenticación, debemos configurar nuestro certificado digital en dicho navegador.

Para ello, debemos seguir los siguientes pasos:

1. Si no tenemos el navegador Firefox, lo podemos descargar en: https://www.mozilla.org/es-ES/firefox/new/

Una vez descargado el navegador Firefox:

2. Ir a “Preferences”.

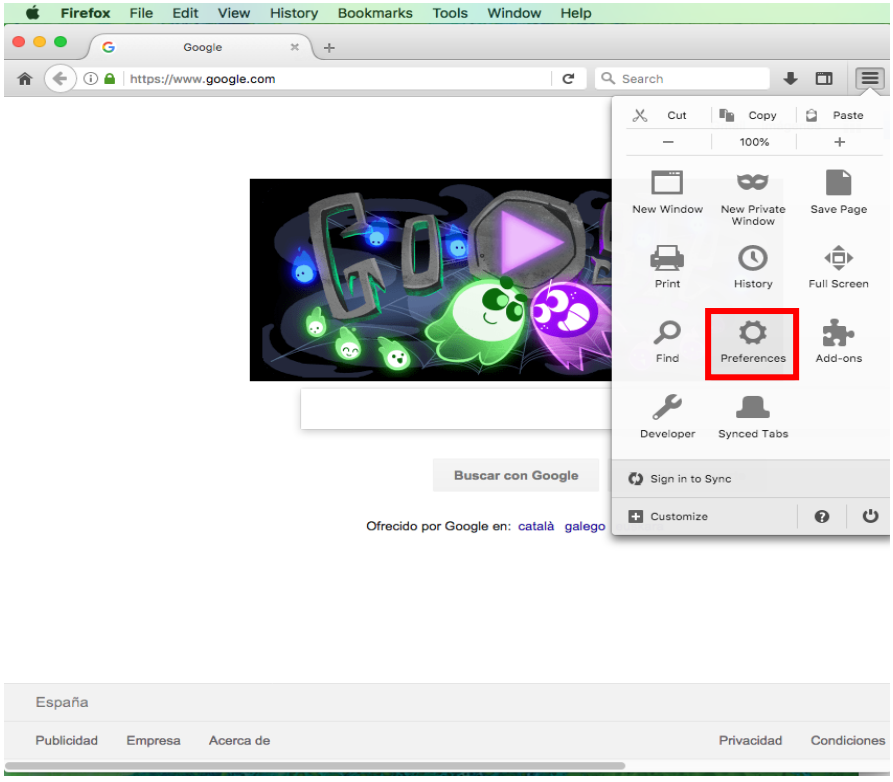

Figura 22. Configuración de certificados digitales en Firefox

3. Ir a “Advanced”
4. Seleccionar “Dispositivos de Seguridad”.

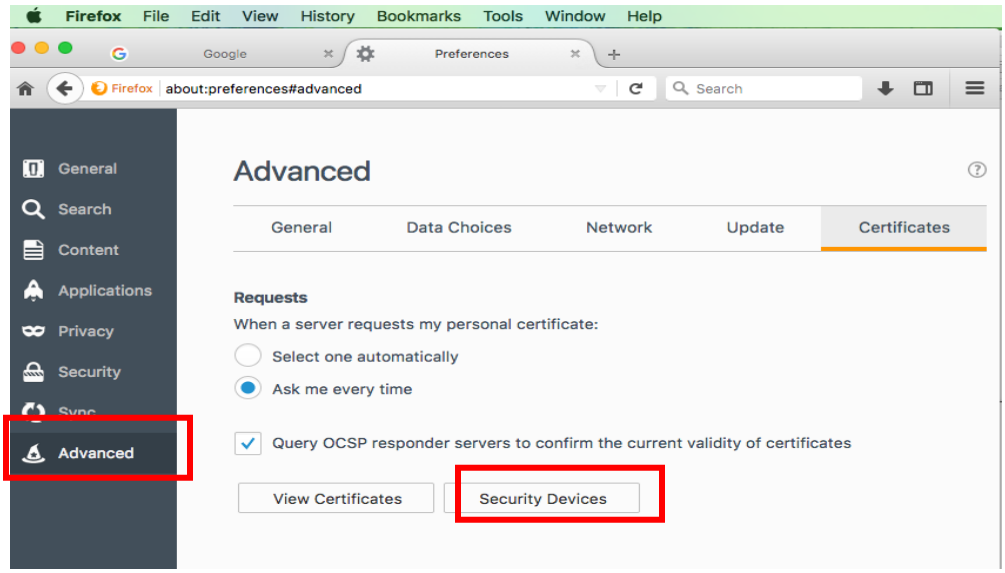

Figura 23. Configuración de certificados digitales en Firefox

5. Seleccionar “Load”.

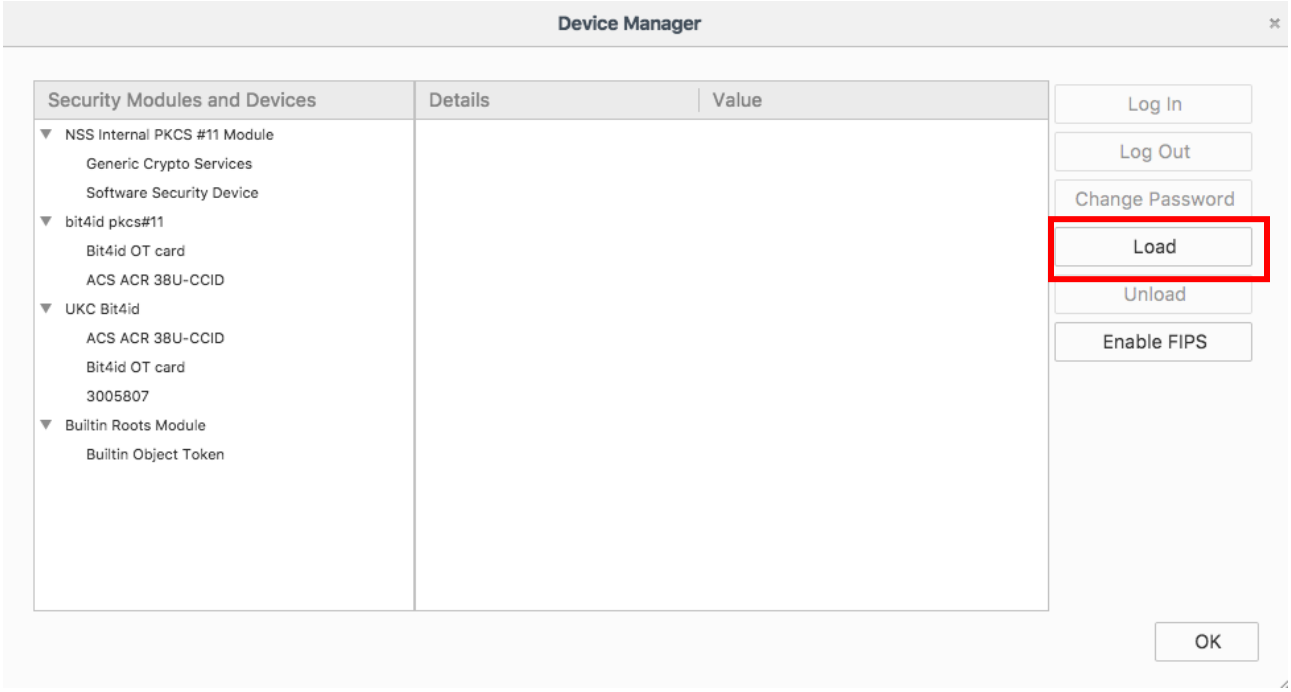

Figura 24. Configuración de certificados digitales en Firefox

6. Insertar la siguiente ruta en “Load PKCS#11 Device”:

/Applications/UniversalKeychain/UniversalKeychain.app/Contents/Resources/pkcs11/libbit4p11.so

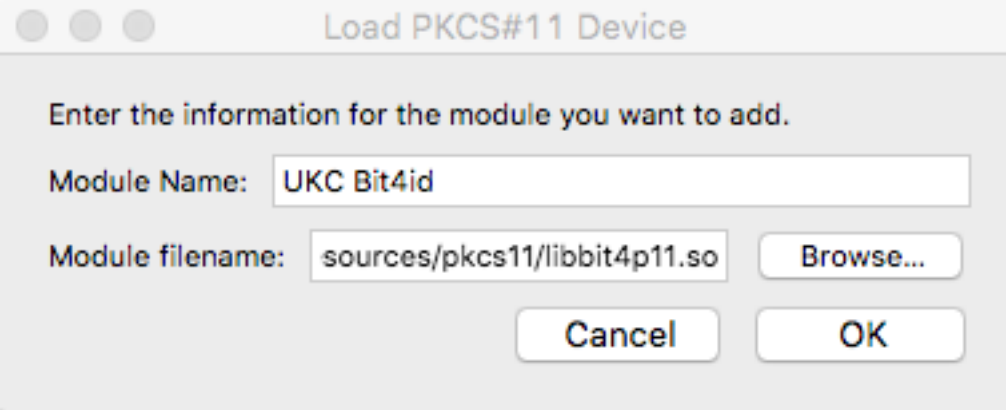

Figura 25. Insertar la ruta en Load PKCS#11 Device en Firefox

La configuración estará realizada.

Ya podrá autenticarse en las sedes electrónicas y hacer trámites on-line.

2.7 Ejemplo de autenticación con certificado en macOS.

Una vez configurado nuestro certificado digital en el navegador Firefox, podremos autenticarnos y firmar electrónicamente en cualquier sede electrónica.

Como ejemplo de esta funcionalidad, accederemos al servicio de Sede Electrónica de la Agencia Tributaria española.

Figura 26. Sección 'Mis expedientes' de la Agencia Tributaria española

En el cuadro de diálogo, seleccionamos la opción de acceder “Con certificado electrónico de identificación o DNI electrónico”.

Figura 27. Tipos de acceso a la sección 'Mis expedientes'

Seleccionamos el certificado a utilizar para la autenticación.

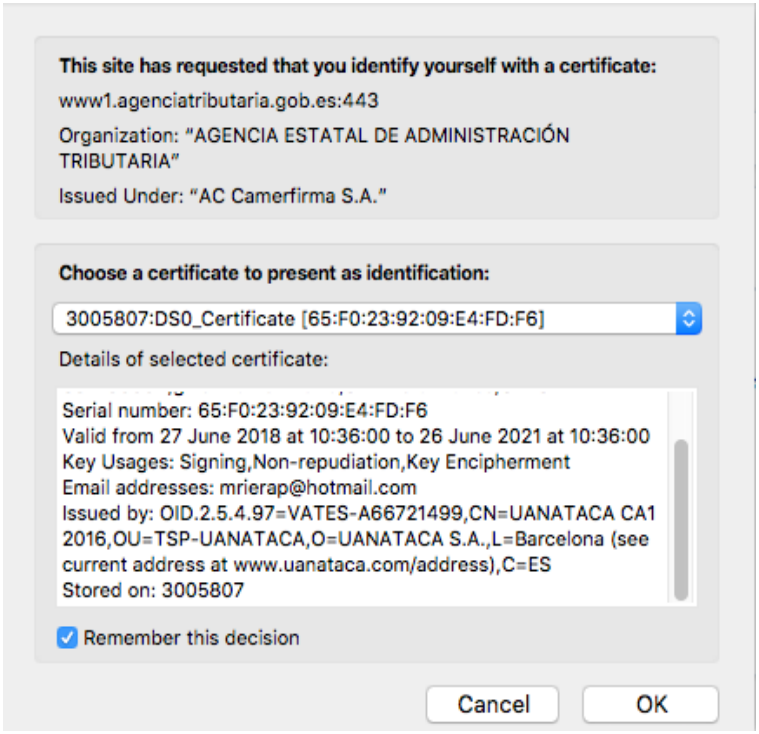

Figura 28. Selección del certificado digital

UKC Desktop nos solicita el PIN del certificado remoto para llevar a cabo la autenticación.

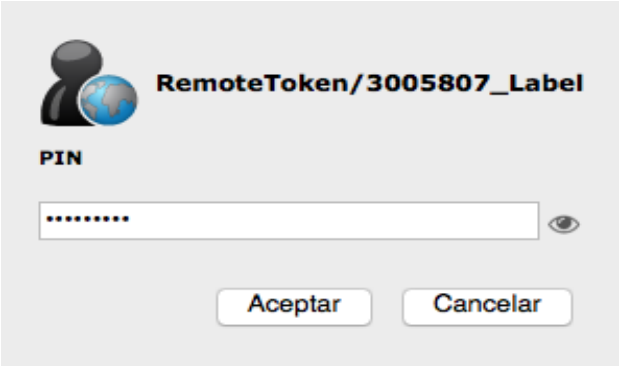

Figura 29. Insertar el PIN del certificado digital

Al introducir el PIN de forma satisfactoria, la plataforma web, como resultado, nos da el acceso a nuestros datos.

Figura 30. Página 'Mis expedientes'