



Manual de Usuario

UKC Desktop para PC y SignCloud App para iPhone y Android

Contenido

1. Introducción.....	3
2. Certificado digital remoto desde PC con UKC Desktop.....	3
2.1. Instalar el programa UKC Desktop.....	3
2.2. Configuración del programa UKC Desktop	4
2.2.1. Contenido y configuración	5
2.2.2. Inicio de sesión en SignCloud.....	6
2.3. Cómo utilizar el programa UKC Desktop.....	7
2.3.1. Ejemplo de firma electrónica de un documento	8
3. Certificado digital remoto desde dispositivos móviles	9
3.1. Instalar la App Digifirma SignCloud en iPhone	9
3.2. Instalar la App Digifirma SignCloud en Android.....	10
3.3. Configurar la App Digifirma SignCloud.....	11, 20
3.3.1. Menú de la App Digifirma SignCloud	11
3.3.2. Botón “Home”	12
3.3.2.1. Firmar archivos	13
3.3.2.2. Verificar una firma electrónica	16
3.3.2.3. Histórico	16
3.3.3. Botón Identidad	17
3.3.4. Botón Ajustes	18
3.3.4. Botón Soporte	19
3.4. Desbloqueo de PIN.....	20

1. Introducción

El presente manual recoge una guía de usuario para el uso de los certificados digitales remotos almacenados en SignCloud (nube de Digifirma) desde PC y desde dispositivos móviles iPhone y Android.

En el capítulo 2 se explica cómo utilizar el certificado digital remoto desde un PC. En el capítulo 4 se explica cómo utilizarlo desde un dispositivo móvil iPhone o Android

2. Certificado digital remoto desde PC con UKC Desktop

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 Digifirma.

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

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

1. Descargar el programa UKC Desktop.
2. Ejecutar el archivo y seguir el proceso de instalación.
3. Aceptar el acuerdo de licencia.
4. Cerrar el instalador una vez completada la instalación.



Figura 1. Asistente de instalación de UKC Desktop

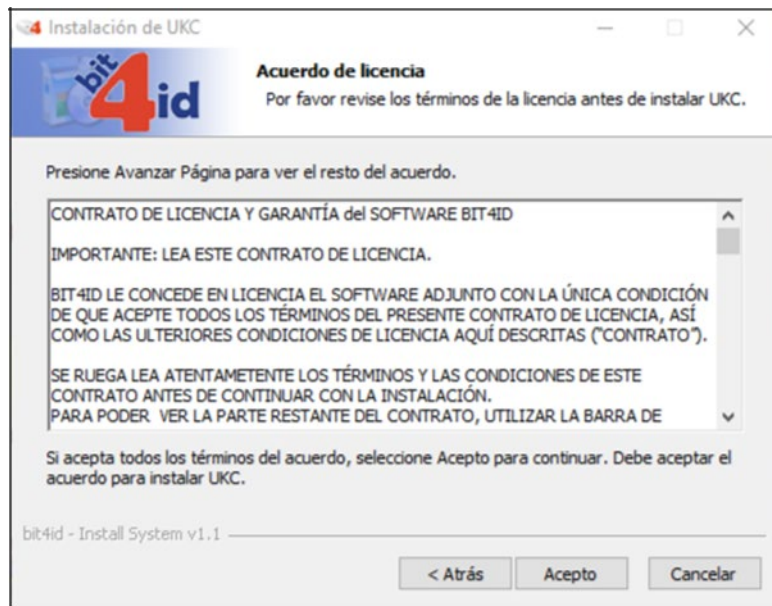


Figura 2. Acuerdo de licencia UKC Desktop

2.2. Configuración del programa UKC Desktop

Para poder utilizar las funcionalidades de UKC Desktop con certificados remotos es necesario disponer de un certificado digital emitido en el sistema SignCloud de Digifirma. 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 PC. Para acceder a la aplicación, debemos presionar el icono que aparece en la barra de tareas (*figura 3*), también se puede abrir directamente desde el icono del escritorio. (*figura 4*)

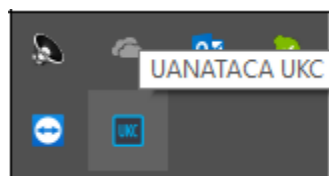


Figura 3. UKC Desktop en la barra de tareas



Figura 4. Icono UKC Desktop en el escritorio de Windows

2.2.1. Contenido y configuración

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



Figura 5. 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 PC.
- **SignCloud:** Esta opción permite gestionar los certificados digitales custodiados en el sistema SignCloud de Digifirma.
 - 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.

2.2.2. Inicio de sesión en SignCloud

El inicio de sesión permite acceder al certificado digital custodiado en el sistema SignCloud de Digifirma, cargándola en el PC 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...**”:

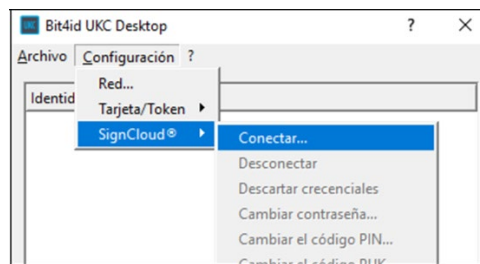


Figura 7. Conectarse al sistema SignCloud

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

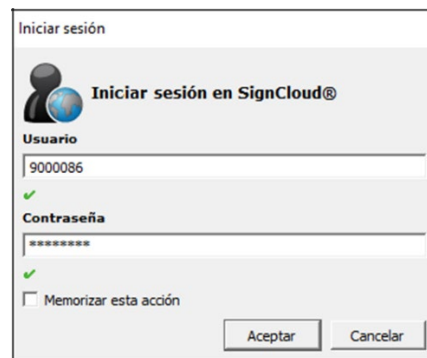


Figura 8. Iniciar sesión en SignCloud

Si el inicio de sesión se lleva a cabo con éxito, se mostrará la siguiente notificación.

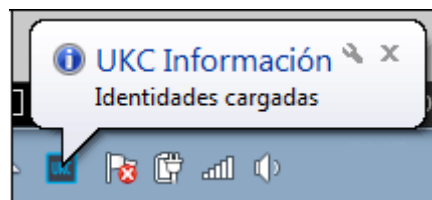


Figura 9. Notificación de inicio de sesión satisfactorio

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

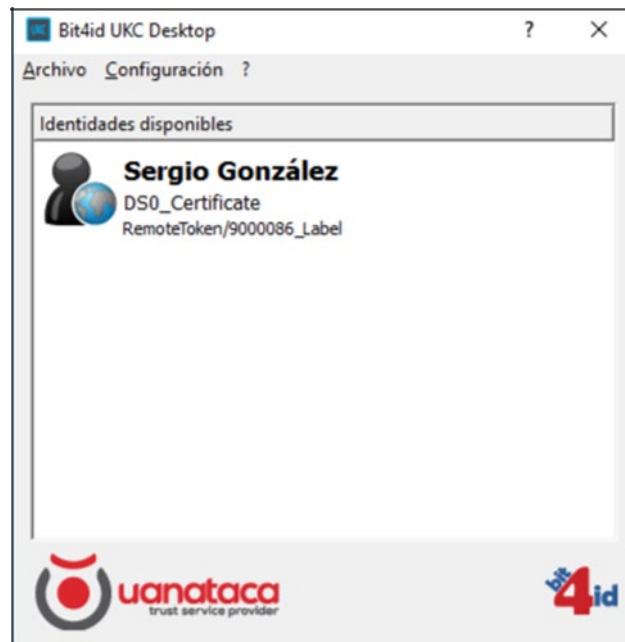


Figura 10. Vista de certificados digitales disponibles

UKC Desktop actúa como un proveedor de identidades digitales. En el caso de certificados digitales remotos, el sistema operativo Windows, a través de su servicio criptográfico CSP, es agnóstico al contenedor criptográfico de estas identidades. Esto quiere decir que la trata de igual forma que a unas claves y certificado digital alojado en una tarjeta/token o instalado en el propio PC. Para comprobarlo, se puede acceder al almacén de certificados de Windows y ver como los certificados digitales remotos se visualizan, estando preparados para ser utilizados.

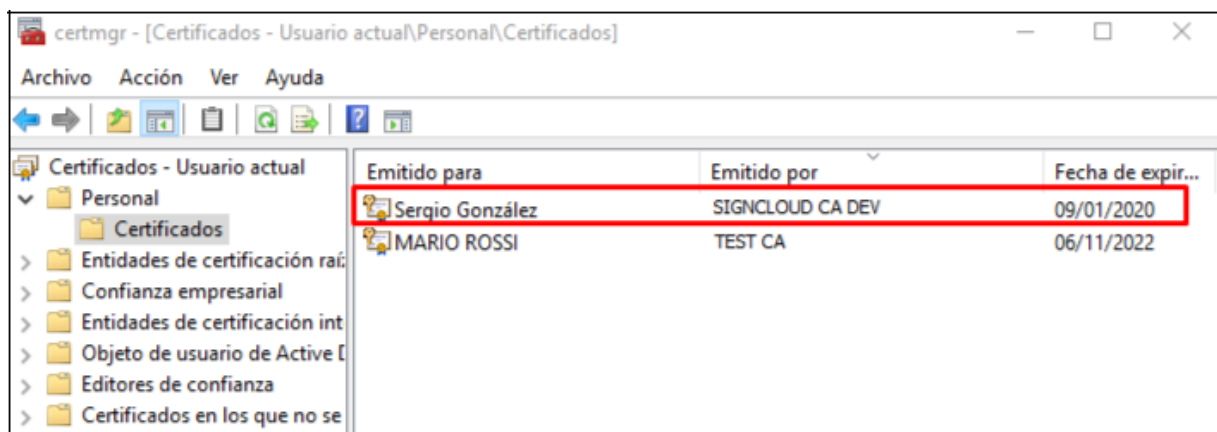


Figura 11. Almacén de certificados de Windows mostrando los certificados digitales remotos custodiados en SignCloud

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.

2.3.1. Ejemplo de firma electrónica de un documento

A continuación, se muestra un ejemplo de cómo firmar un documento utilizando PDF Adobe Acrobat Reader en su última versión.

1. Abrir el documento PDF que se desea firmar desde la aplicación Adobe Acrobat Reader.
2. Acceder al menú "Herramientas" y seleccione "Certificados".
3. En la barra "Certificados" abrir la opción "Firmar Digitalmente".
4. A continuación, aparece el menú de firma y los certificados digitales disponibles.



Figura 12. Certificados digitales disponibles en el sistema (PDF Adobe Acrobat Reader)

5. Seguidamente se muestra el menú de firma. Hacemos los cambios necesarios y presionamos Firmar.

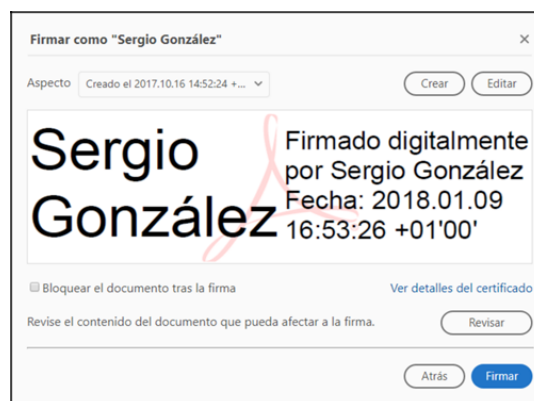


Figura 13. Menú de firma

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

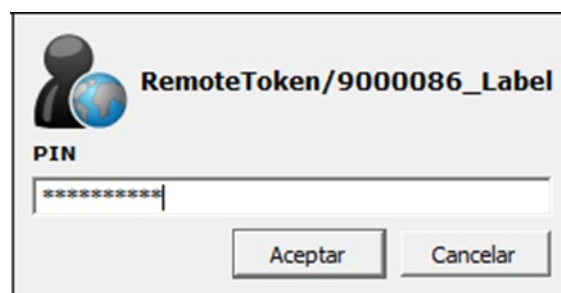


Figura 14. Inserción de PIN de firma por parte del usuario en DIGIFIRMA UKC Desktop

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

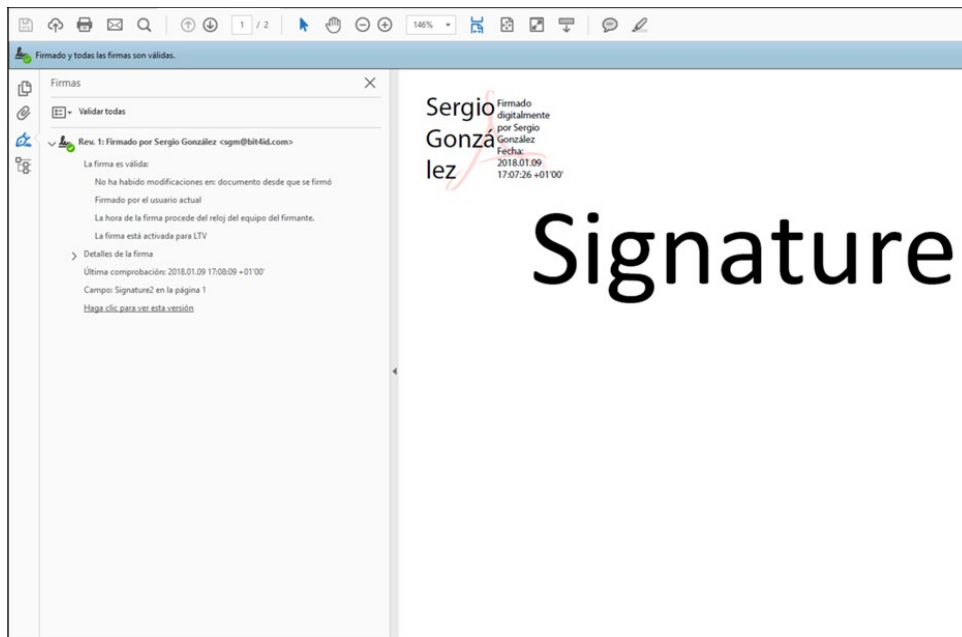


Figura 15. Firma electrónica válida

3. Certificado digital remoto desde dispositivos móviles

El presente documento tiene el objetivo de guiar al usuario a través de la App Digifirma SignCloud para el uso de certificados digitales custodiados remotamente en el sistema SignCloud de Digifirma.

A través de la App, el usuario puede firmar y validar documentos, así como autenticarse en entornos web, haciendo uso de sus certificados remotos. Para ello se requieren las credenciales utilizadas en el proceso de generación del certificado (Usuario, Contraseña y Código PIN)

3.1. Instalar la App Digifirma SignCloud en iPhone

Para descargar la App Digifirma SignCloud desde iOS, es necesario buscar la App en Apple Store 

La aplicación se encuentra disponible bajo la siguiente información:

- Nombre: **“Digifirma SignCloud”**
- Vendedor: **“Uanataca”**

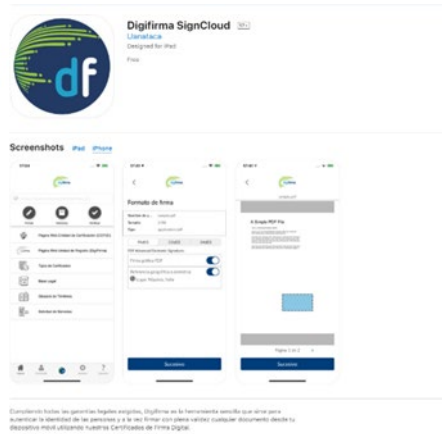


Figura 16. Instalar Digifirma SignCloud desde App Store

3.2. Instalar la App Digifirma SignCloud en Android

Para descargar la App Digifirma SignCloud desde iOS, es necesario buscar la App en Play Store. 🌈

La aplicación se encuentra disponible bajo la siguiente información:

- Nombre: **"DigiFirma SignCloud"**
- Vendedor: **"Uanataca SA"**



Figura 17. Digifirma SignCloud desde Play Store

3.3. Configurar la App Digifirma SignCloud

Para poder utilizar las funcionalidades de la App Digifirma SignCloud con certificados remotos es necesario disponer de un certificado digital emitido en el sistema SignCloud de Digifirma. Este certificado tiene asociadas las siguientes credenciales:

- 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)



Figura 18. Inicio de sesión

El inicio de sesión permite acceder a la información de nuestro certificado digital en la App Digifirma SignCloud y constituye la fase de identificación. No obstante, para poder utilizar el certificado necesitaremos el código PIN (pudiendo ser estático o dinámico).

3.3.1. Menú de la App Digifirma SignCloud

La App contiene un menú de navegación situado en la parte inferior, que permite al usuario cambiar de sección. En función de la sección en la que ese encuentre el usuario, el icono de navegación aparecerá de un color diferente al resto. Éstas son:

- La sección principal o **“Home”**. Representa la vista principal, donde se da la opción de acceder a las funcionalidades principales (firma, validación y acceso al navegador web que posibilita la autenticación web).
- **Identidad**. Permite gestionar los certificados digitales que se encuentren configurados en la App.
- **Ajustes**. Se puede optar entre varios idiomas/países o definir la opción “Automático”, donde se seleccionará el idioma y país donde se encuentra el usuario.
- **Soporte**. Esta opción brinda información de soporte al usuario, haciendo uso de las FAQs o utilizando el asistente de Tour Virtual.

En el resto de la vista se muestra el contenido de la sección en la que nos encontramos, permaneciendo siempre el logo de la App en la parte superior.

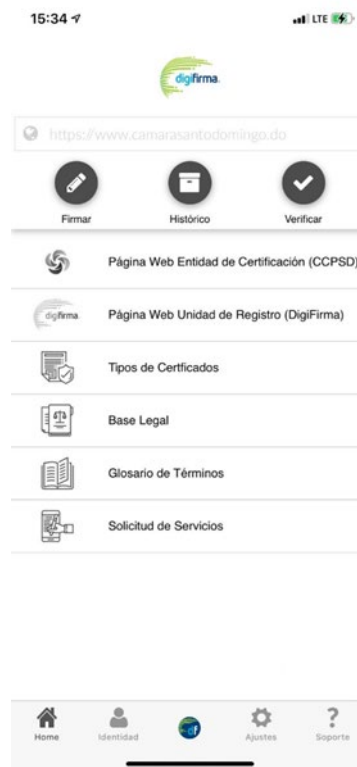


Figura 19. Página principal App

3.3.2. Botón “Home”

Desde esta pantalla el usuario puede utilizar las principales funcionalidades que ofrece la App:

- Firma de archivos
- Validación de archivos firmados
- Autenticación en entornos web haciendo uso del navegador web que incorpora la App
- Ver el histórico de documentos firmados

3.3.2.1. Firmar archivos

La App Digifirma SignCloud permite firmar documentos en varios formatos estándar de firma. La firma puede realizarse de dos maneras.

La primera, haciendo uso del botón "Firmar" que se encuentra en la vista Inicio.

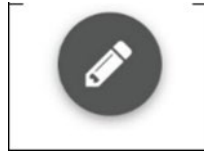


Figura 27. Botón 'Firmar'

Utilizando esta opción, la App ofrece la posibilidad de navegar en el sistema de archivos del dispositivo y seleccionar el archivo a firmar.

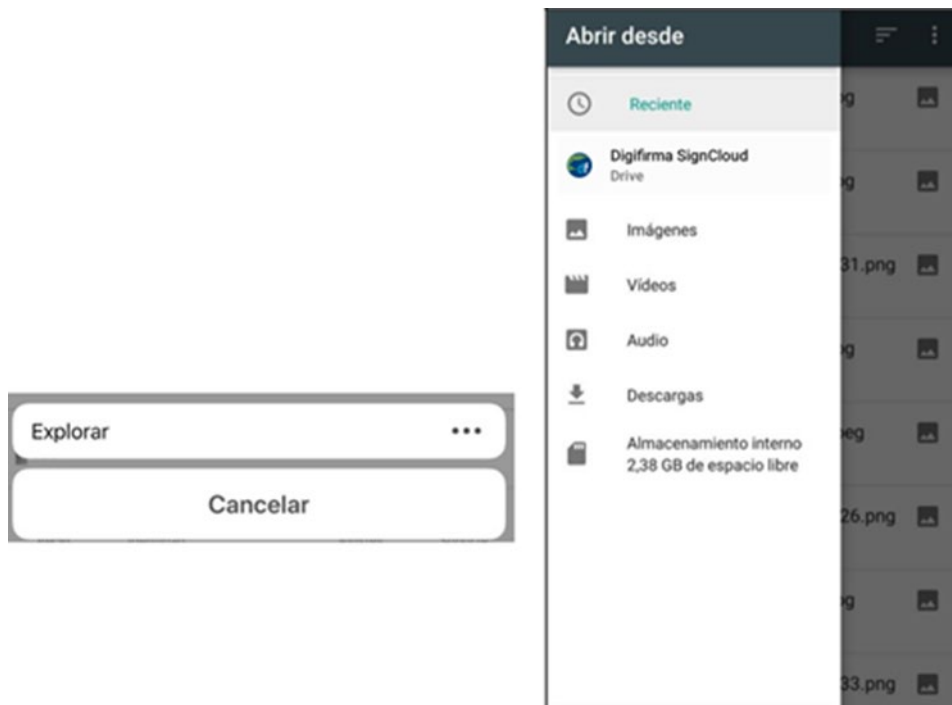


Figura 20. Selección del archivo a firmar desde

La segunda vía consiste en la llamada a la App Digifirma SignCloud desde otra aplicación externa, utilizando la opción "Compartir" sobre el archivo que queremos firmar y seleccionando Digifirma SignCloud como aplicación destino. Esta opción puede aparecer con diferente formato, en función de la App que utilicemos, entre los nombres alternativos de dicha función se encuentran: 'Exportar', 'Abrir con', etc. El ejemplo más común consiste en la firma de un archivo gestionado por la aplicación de correo electrónico (p. ej. Gmail o Microsoft Outlook), por una aplicación de mensajería instantánea (p. ej. WhatsApp o Facebook) o por un gestor de almacenamiento en la nube (p. ej. OneDrive o Dropbox).

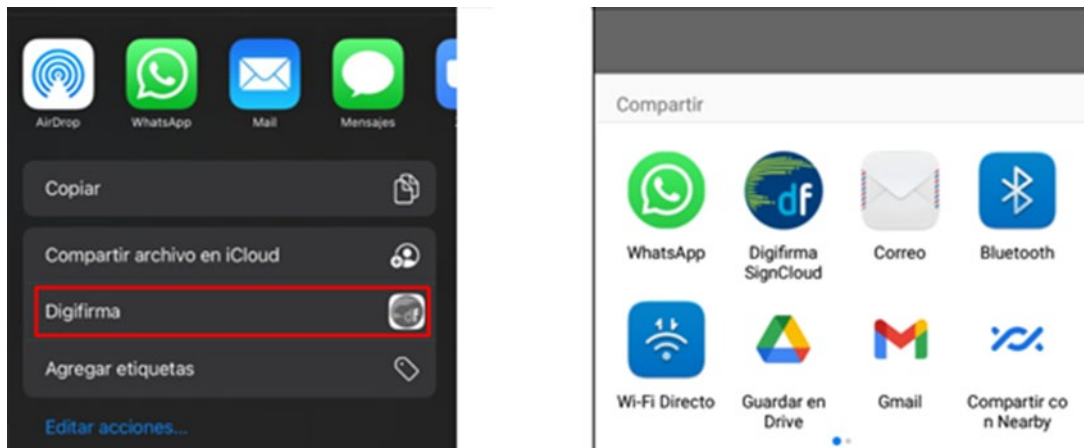


Figura 21. Firma de archivos desde Apps externas (iOS/Android)

Inmediatamente después de la selección del archivo, la App Digifirma SignCloud detecta el tipo de archivo y muestra los estándares de firma disponibles.



Figura 22. Asistente de firma (**paso 1**) – **Opciones de firma**

Desde el asistente de firma, el usuario puede ver la información del archivo a firmar y seleccionar el estándar de firma a utilizar (**paso 1**). Si se trata de una firma del tipo PAdES, el usuario podrá aplicar una marca gráfica a la firma, así como incluir una georreferencia en ésta si lo desea. En la siguiente fase del asistente de firma, se muestra una vista previa del archivo a firmar (siempre que el formato del archivo lo permita) (**paso 2**).

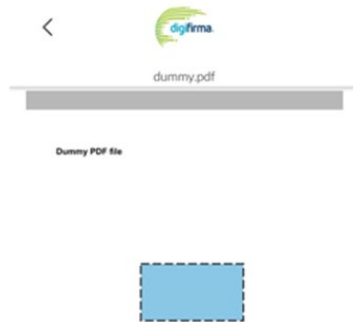


Figura 23. Asistente de firma
(paso 2) – Vista previa



Figura 24. Asistente de firma
(paso 3) - Autenticación



El último paso antes de la firma de documento es el de “Autenticación” (**paso 3**). El usuario, después de haber configurado las opciones de firma y pre-visualizar el documento, debe autenticarse en el sistema SignCloud para autorizar la firma. En esta sección se selecciona el certificado a utilizar (si hubiera más de uno configurado en la App) y se introduce el código PIN.

El modo de autenticación puede configurarse también como “TouchID” (huella digital) en aquellos dispositivos que lo permitan o como una combinación de ambos (PIN + TouchID).

Después de haber realizado la autenticación con éxito, se lleva a cabo la firma. En el último paso, el asistente nos notifica si ha sido satisfactoria y nos permite compartir el archivo firmado.



Figura 25. Resultado final de firma

3.3.2.2. Verificar una firma electrónica

A través de esta opción, la App Digifirma SignCloud permite verificar la firma de cualquier archivo alojado en el dispositivo móvil. Esta función, de forma análoga al botón 'Firmar', abrirá el explorador de archivos del dispositivo para buscar y seleccionar el archivo correspondiente.

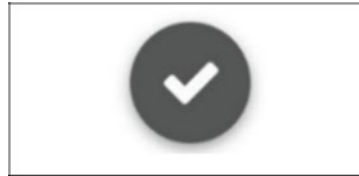


Figura 26. Botón 'Verificar'

Tras el proceso de verificación, la App Digifirma SignCloud muestra un informe con el resultado de ésta. Desde esta página se puede optar también por compartir el informe de verificación generado.



Figura 27. Reporte de verificación

3.3.2.3. Histórico

Esta funcionalidad muestra un registro de todos los archivos firmados por la App Digifirma SignCloud, así como el historial de los sitios web donde se han llevado a cabo procesos de autenticación.

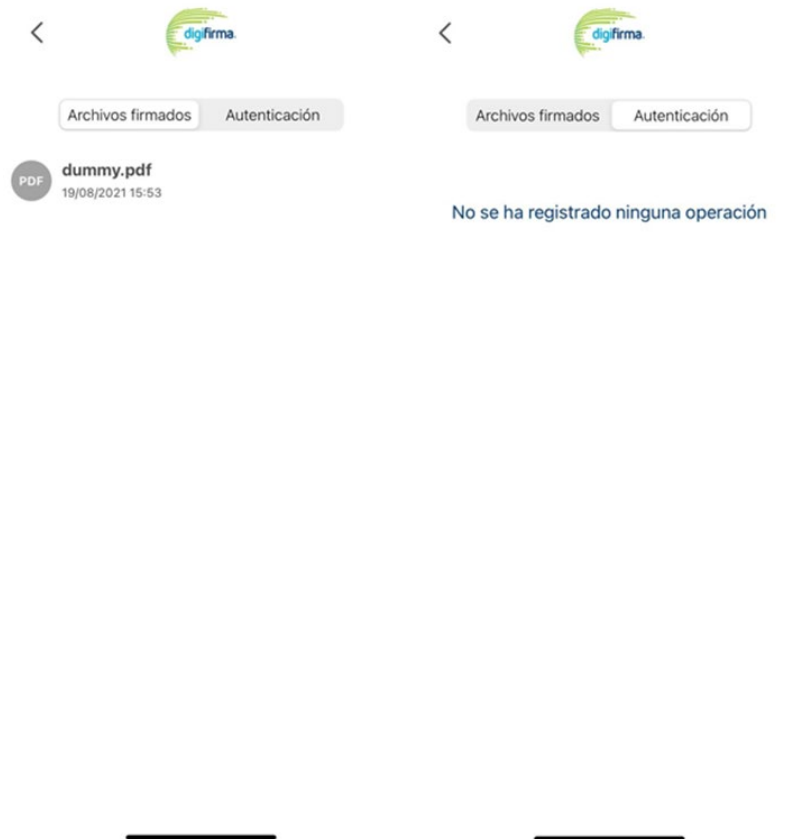


Figura 28. Visionado del Historial de archivos firmados y autenticaciones

El **historial de archivos firmados** proporciona no sólo una vía directa a éstos sino también la posibilidad de llevar a cabo una verificación de la firma, de compartir el archivo o de borrarlo.

El **historial de autenticación** ofrece la posibilidad de acceder directamente a los sitios web. Desde aquí se puede borrar también cualquiera de los registros.

3.3.3. Botón Identidad

Desde esta opción, el usuario puede gestionar sus certificados digitales custodiados remotamente en SignCloud.

Lista de identidades

La App SignCloud permite configurar múltiples certificados digitales custodiados en SignCloud, cada una definida por Usuario/Contraseña y PIN. En esta vista podemos ver todas aquellas cuentas vinculadas en la App y acceder a la información de cada una de ellas.

Gestión de una Identidad

Dentro de cada Identidad Digital (certificado digital) se muestra el Usuario vinculado (ej. 3000089), detalles del certificado digital y las opciones de gestión del PIN.



Figura 29. Información del certificado

Eliminar Identidad

Esta funcionalidad permite eliminar un certificado digital de la App Digifirma SignCloud. Esto no significa que el certificado digital desaparezca del sistema de custodia remota SignCloud, sino que lo desvincula únicamente de la App. Habiendo utilizado esta opción sobre una cuenta, ésta podrá ser vinculada de nuevo en la App Digifirma SignCloud.

3.3.4. Botón Ajustes

Los ajustes necesarios dentro de la App se llevan a cabo a través de esta pestaña. Una de estas configuraciones es la selección del país. Se puede optar entre varios países o definir la opción en 'Automático', de esta forma se seleccionará el idioma del dispositivo móvil por defecto. La selección de un país hace que cambie el idioma de interfaz, así como los enlaces predeterminados del navegador web.



Figura 30. Muestra las preferencias de la App

3.3.4. Botón Soporte

Esta opción proporciona información de soporte al usuario. Consta de tres secciones:

- **CONTACTOS.** Se detallan las vías disponibles para contactar con el servicio de soporte, entre ellas información de atención al cliente, así como un correo electrónico donde enviar consultas.
- **FAQ.** En este apartado se incluyen las preguntas más frecuentes con sus respectivas respuestas (Frequently Asked Questions), con el objetivo de ayudar al usuario antes de utilizar las vías del apartado anterior.
- **Información.** Da asistencia a través de un Tour Virtual, destacando las funcionalidades principales de la App. También se puede consultar en este apartado información de gran relevancia, ya sean condiciones legales o de uso.



Figura 31. Muestra contenido Ayuda

3.4. Desbloqueo de PIN

En caso su PIN quede bloqueado por intentos fallidos, debe acceder al siguiente enlace para restablecer el mismo: <https://www.uanataca.com/lcimpl/reset?customer=digifirma>



Figura 32. Pantalla Desbloqueo PIN

En esta pantalla debe colocar sus credenciales: nombre de usuario y contraseña, luego recibirá en el correo electrónico registrado un código OTP/confirmación que deberá introducirlo y posteriormente introducir su nuevo PIN dos veces.

NOTA: Este código PIN debe contener al menos por 2 números, 2 letras y 8 caracteres.

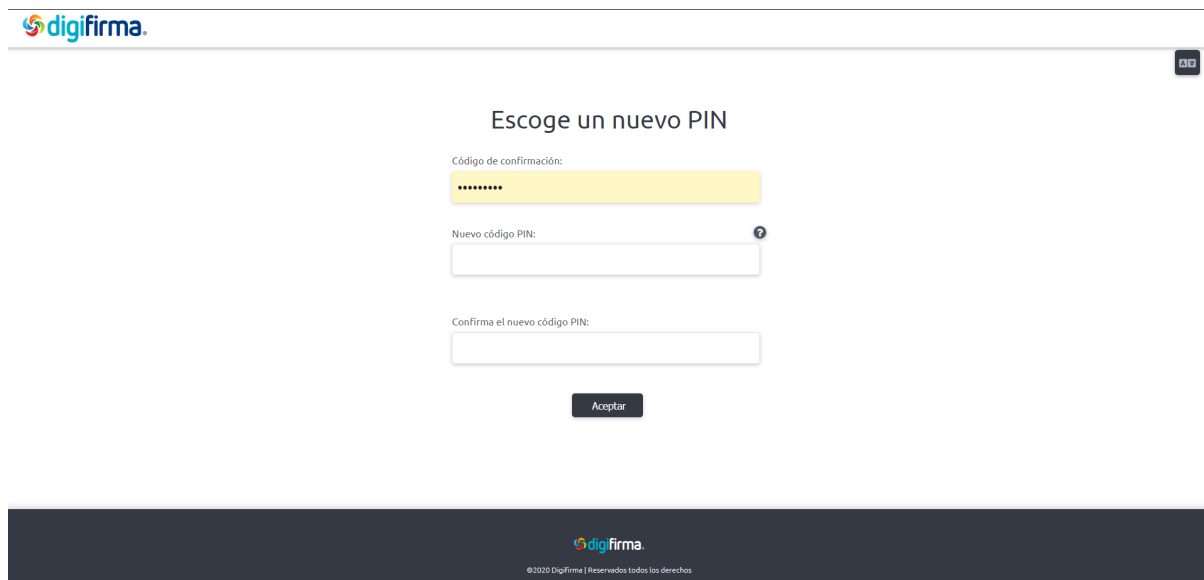


Figura 33. Pantalla para escoger nuevo PIN