
**MANUAL PARA FIRMA DE
DOCUMENTOS PDF USANDO
UKC Y VALIDACIÓN DE
DOCUMENTOS.**

V1 – 2020/03/18

Dirección Nacional de
Tecnologías de la Información y
Comunicaciones

INDICE GENERAL

1	INTRODUCCIÓN.....	4
1.1	Precedentes.....	4
1.2	Requerimientos.....	4
2	Firma del documento (S.O. Windows).....	4
2.1	Instalación del Certificado Remoto.....	4
2.2	Instalación del UKC.....	5
2.3	Carga del Certificado Remoto en el UKC.....	7
2.4	Instalación de la cadena de confianza	9
2.4.1	Instalación del Certificado Raíz	9
2.4.2	Instalación del Certificado Subordinado	9
2.5	Firma de documentos	10
2.5.1	Configuración de Adobe Reader	10
2.5.2	Firma con Adobe Reader DC Versión.....	11
2.6	Validación de la firma en un documento.....	12
3	Firma del documento (S.O. MACOS).....	13
3.1	Instalación del Certificado Remoto.....	13
3.2	Instalación del UKC.....	13
3.3	Carga del Certificado Remoto en el UKC.....	17
3.4	Firma de documentos	19
3.4.1	Configuración de Adobe Reader	19
3.4.2	Firma con Adobe Reader DC Versión.....	22

INDICE DE FIGURAS

Figura: 1 Ejecutar archivo	5
Figura: 2 Asistente de instalación de UKC	6
Figura: 3 Acuerdo de licencia	6
Figura: 4 Instalación completa	7
Figura: 5 Carga del Certificado Remoto en el UKC	7
Figura: 6 Sobre de credenciales.....	8
Figura: 7 Identidades cargadas.....	9
Figura: 8 Integración con Windows.....	10
Figura: 9 Aceptar la integración con Windows.....	11
Figura: 10 Opción Certificados	11
Figura: 11 Certificados.....	12
Figura: 12 Icono	12
Figura: 13 Aplicación	12

1 INTRODUCCIÓN

La presente guía tiene como fin explicar la forma para:

- Firmar un documento PDF
- Validar un documento PDF

1.1 Precedentes

- Efectos de la firma electrónica de acuerdo a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.- “La firma electrónica tendrá igual validez y se le reconocerán los mismos efectos jurídicos que a una firma manuscrita en relación con los datos consignados en documentos escritos, y será admitida como prueba en juicio.¹”

1.2 Requerimientos

Requerimientos mínimos para poder realizar la certificación de un documento electrónico.

#	Elemento	Propósito
1	Windows XP (Service pack 3) o versiones superiores (con un puerto USB disponible y factibilidad de conexión a red.)	Gestionar conexiones a dispositivos y manejos del sistema de almacenamiento de documentos.
1	Conexión Intranet	Conexión a la red del Consejo de la Judicatura.
1	Firma electrónica, CERTIFICADO REMOTO	Para firmar documentos digitales.
1	Aplicación para visualización de documentos (Adobe Reader DC)	Permite visualizar el documento

2 Firma del documento (S.O. Windows)

2.1 Instalación del Certificado Remoto

Luego de haberse emitido el certificado al usuario es necesario que se realice la instalación de software y de los certificados raíz y subordinado que forman la cadena de confianza para la firma de documentos sin inconvenientes. El proceso de recopilación de documentos, según la solicitud del usuario requirente, y estos haber sido escaneados en un documento en formato PDF, se puede iniciar el proceso de firma electrónica de un archivo.

¹ Fuente: Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos; emitida mediante decreto ejecutivo del 17 de abril de 2002, RO No 557.

Nota: La digitalización de los documentos debe ser realizada con la suficiente definición para la lectura de los datos en el documento físico sin que esta sea muy alta para evitar documentos que ocupen más espacio del necesario.

Para el uso del certificado remoto del Consejo de la Judicatura es necesaria la instalación de la aplicación UKC.

2.2 Instalación del UKC

Primero se debe descargar la aplicación UKC (s.o. Windows) desde:

<https://www.icert.fje.gob.ec/web/guest/descargas3>

Nos dirigimos al archivo descargado y lo ejecutamos.

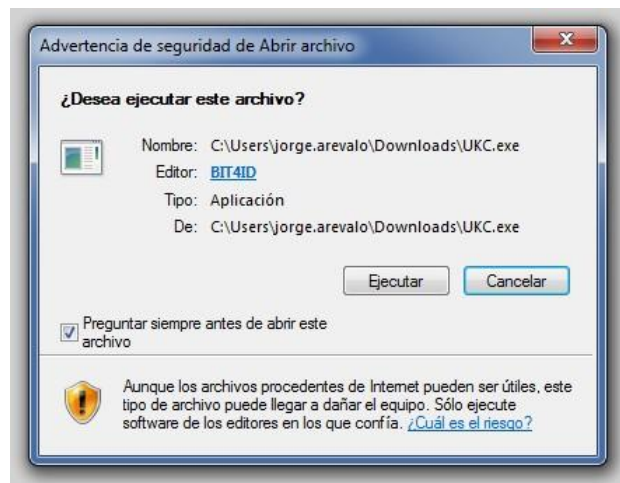


Figura: 1 Ejecutar archivo

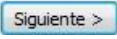
Damos clic en  y se abrirá la ventana que se muestra a continuación en donde presionamos .



Figura: 2 Asistente de instalación de UKC

A continuación aceptamos los acuerdos de licencia

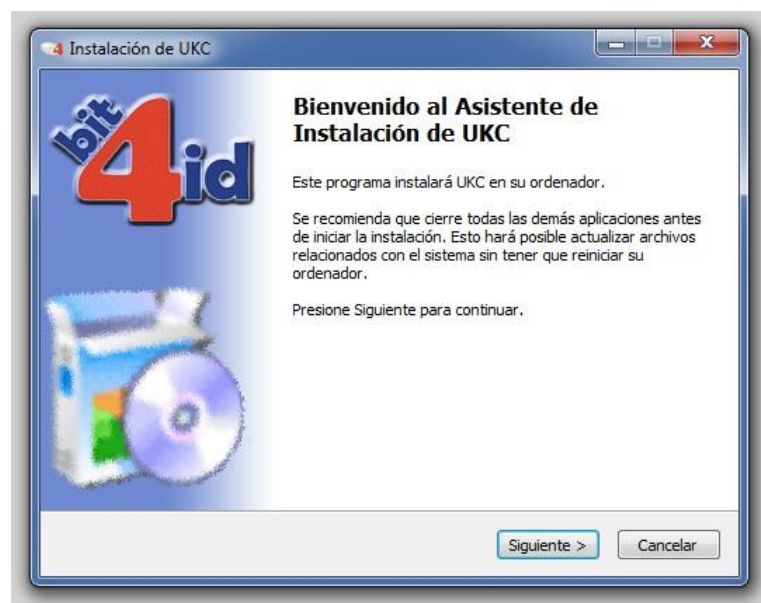


Figura: 3 Acuerdo de licencia

Y la instalación procederá:

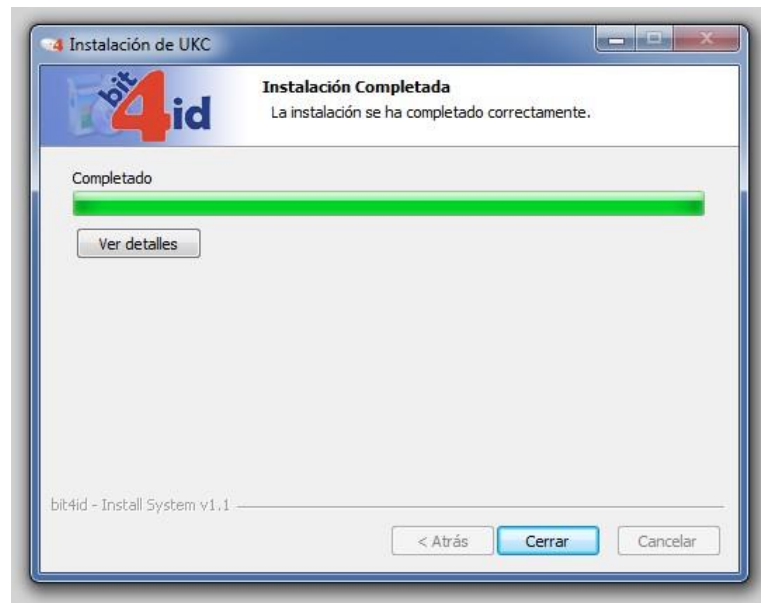


Figura: 4 Instalación completa

Finalmente damos clic en Cerrar y la instalación habrá finalizado. Reiniciar el equipo

2.3 Carga del Certificado Remoto en el UKC

Ejecutamos la aplicación UKC que se encuentra en la carpeta Bit4id del menú de inicio de Windows dando clic en el globo del logotipo:

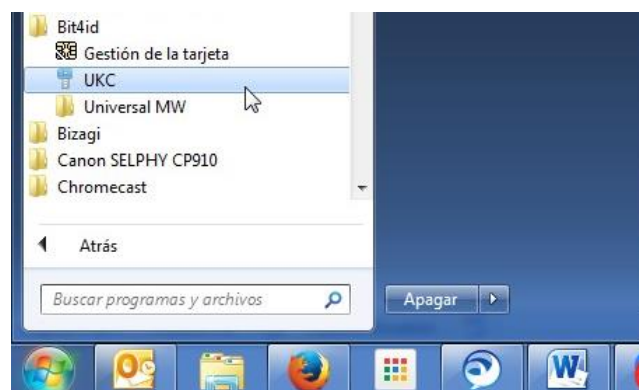
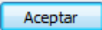


Figura: 5 Carga del Certificado Remoto en el UKC

Aquí se abrirá un pequeño cuadro de dialogo en donde nos solicita el usuario y la contraseña, las cuales fueron entregadas al cliente vía correo electrónico de manera similar de cómo se ve bajo este texto. Llenamos los datos de manera similar a la imagen y damos clic en  .

Se recomienda ubicar el visto en “Memorizar esta acción” ya que esta contraseña no puede ser cambiada, el elemento que un usuario si puede cambiar es el PIN, que es el código de 8 dígitos que la aplicación solicita cada vez que el usuario envía a firmar un documento.

Sobre de credenciales

Estimado solicitante,
estas son las credenciales correspondiente a su identidad en formato HSM.

USER ID	76c86e170ba39ad/FP/1
Contraseña:	c532ceff9186847a3
PIN	69987341
PUK	20254624
ERC	etHQTp5Oe3

Iniciar sesión

 **Iniciar sesión en el SFC**

Usuario

76c86e170ba39ad/FP/1

Contraseña

.....

☒ Memorizar esta acción

El User ID corresponde al nombre de usuario para autenticarse.
El PIN permite el uso normal del token para la firma electrónica.
El PUK permite restaurar el PIN en caso de bloqueo u olvido.
El ERC es el código de emergencia para suspender, revocar o reactiva el certificado

Gracias

Equipo ICERT-EC

This email has been generated by [Bit4id smartCMS](#)

Figura: 6 Sobre de credenciales

(Nota: si el equipo inicia antes de conectarse a una red de datos con acceso a internet las credenciales guardadas se descartan)

Hecho esto en la parte inferior derecha junto al reloj se mostrará un mensaje indicando:



Figura: 7 Identities loaded

Una vez cargado el certificado se encuentra listo para ser utilizado en la firma de documentos.

2.4 Instalación de la cadena de confianza

Para poder constatar la validez del certificado instalado se debe proceder a instalar la cadena de confianza y así evitar problemas futuros en la validación de los documentos firmados.

El Certificado Raíz y el Certificado Subordinado son los certificados de la Entidad de Certificación del Consejo de la Judicatura que forman la cadena de confianza que debemos instalar.

En el siguiente enlace se encuentra la información necesaria para la instalación de los certificados: <http://www.icert.fje.gob.ec/web/guest/descargas1> que se describe a continuación.

2.4.1 Instalación del Certificado Raíz

1. Guarde el archivo  CERTIFICADO RAIZ ICERT EC.cer en un directorio dentro de su computador.
2. Haga clic derecho sobre el archivo guardado.
3. Seleccione "Instalar Certificado".
4. En el asistente cuando le muestre las opciones de almacén de certificados seleccionar la opción:
 - Colocar todos los certificados en el siguiente almacén. Pulse examinar y seleccione la opción **Entidades de certificación raíz de confianza**.
5. Continuar con los pasos de la instalación.

2.4.2 Instalación del Certificado Subordinado

1. Guarde el archivo  CERTIFICADO SUBORDINADO ICERT EC.cer en un directorio dentro de su computador
2. Haga clic derecho sobre el archivo guardado.
3. Seleccione "Instalar Certificado".
4. En el asistente cuando le muestre las opciones de almacén de certificados. Seleccionar la opción:
 - Colocar todos los certificados en el siguiente almacén. Pulse examinar y seleccione la opción **Entidades de certificación intermedias**.

5. Continuar con los pasos de la instalación.

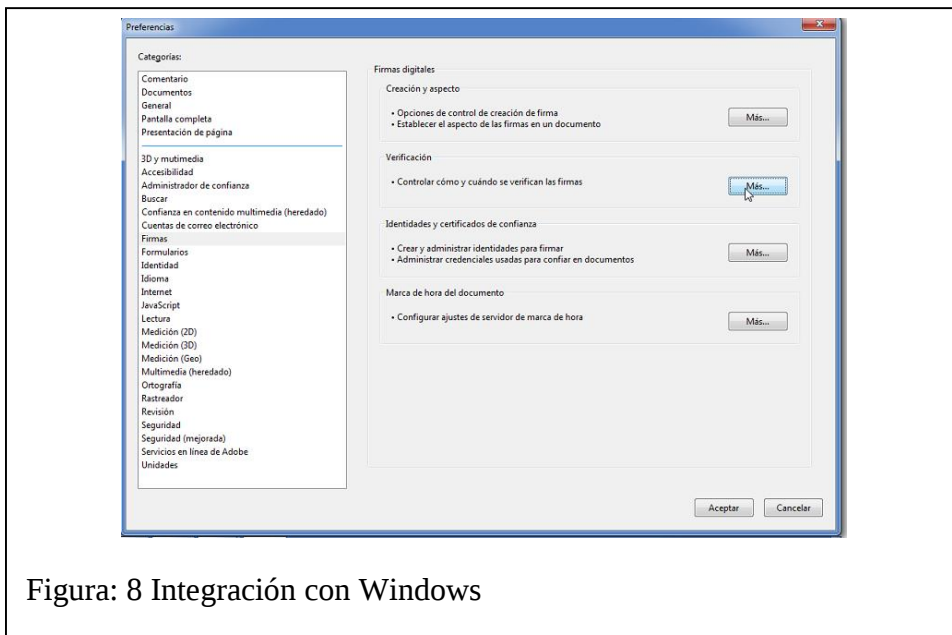
2.5 Firma de documentos

Existen varias aplicaciones con la que se pueden firmar documentos, pero la que vamos a usar es el Adobe Reader DC para evitar instalar más aplicaciones y generar una confusión al agregar firmas en los documentos en formato PDF.

2.5.1 Configuración de Adobe Reader

Para que al firmar un documento no indique que la firma no es válida debemos realizar los siguientes pasos:

1. En un documento de Adobe ingrese al Menú y seleccione sucesivamente: Edición > Preferencias > Firmas > Verificación > Más



Entonces aparecerá la siguiente imagen:

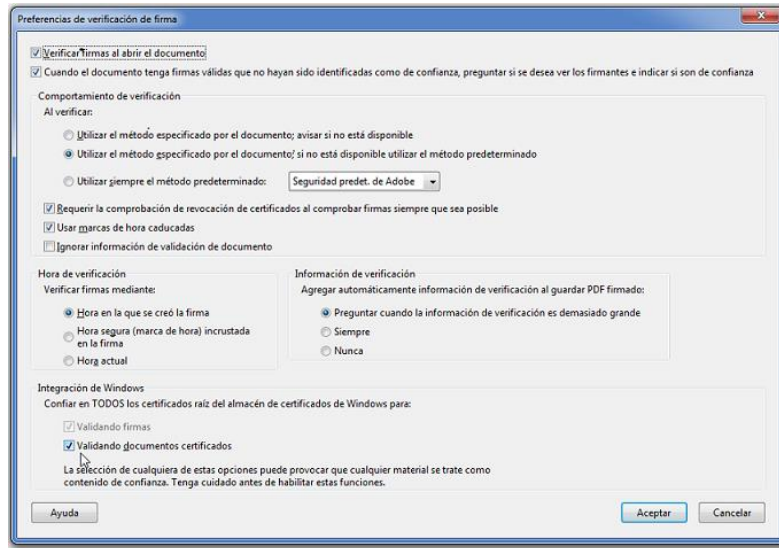
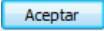


Figura: 9 Aceptar la integración con Windows

2. En la sección Integración de Windows (Confiar en todos los certificados del almacén de certificados de Windows para:) coloque el check o visto en: Validando documentos certificados.
3. Finalmente de clic en 

2.5.2 Firma con Adobe Reader DC Versión

Para firmar un documento en esta aplicación se debe realizar lo siguiente:

1. Abrir el documento a firmar.
2. En el menú superior seleccionar Herramientas
3. Seleccionar Certificados

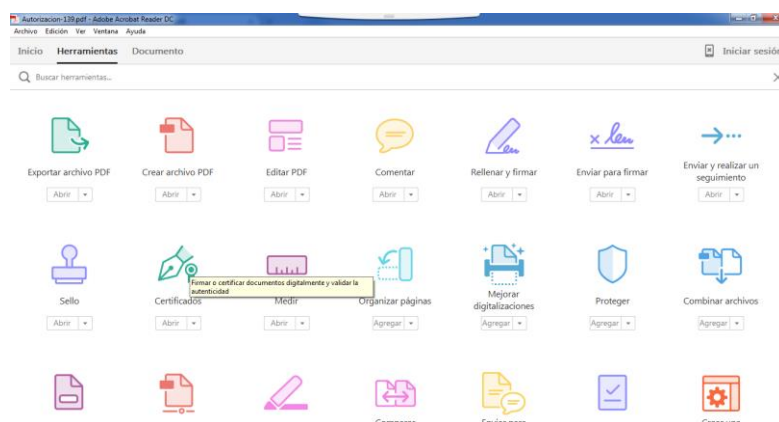


Figura: 10 Opción Certificados

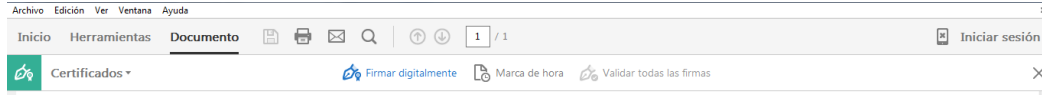


Figura: 11 Certificados

4. Dar clic en **Firmar digitalmente**. Hecho esto el puntero del mouse cambiará para que seleccionemos un recuadro al mantener presionado el botón derecho del mouse sobre el sitio del documento en el que deseamos ubicar la firma gráfica. A continuación se presentará un recuadro en el cual podemos seleccionar el certificado que deseamos usar para la firma y en donde se visualizará una vista previa de la firma.
5. Damos clic en **Firmar** entonces se presentará un explorador de archivos para establecer la ubicación y el nombre con el que queremos guardar el documento firmado.

2.6 Validación de la firma en un documento

Para validar la firma electrónica de un documento luego de conocer su ubicación, se debe instalar la aplicación de escritorio Valida4NG, la aplicación puede descargarse de: <https://www.icert.fje.gob.ec/web/guest/descargas3>

Luego de instalar la aplicación en el computador un nuevo ícono aparecerá en el escritorio.

Al dar doble clic en el ícono se ejecutará la aplicación.



Figura: 122 Icono



Figura: 133 Aplicación

1. Se puede arrastrar con el ratón (manteniendo aplastado el botón izquierdo del ratón) el archivo desde la carpeta que se encuentra sobre el icono de “**Validar**”.
 - a. Arrastrar con el ratón el archivo sobre el ícono.

- b. Soltar el botón del ratón y la aplicación se abrirá.
2. Al dar clic en el icono “**Validar**” se mostrará una ventana de navegación de archivos, propia del sistema operativo, para dirigirse a la ubicación del archivo a ser firmado.
 - a. Luego de encontrar la ubicación del archivo seleccionarlo
 - b. Clic en el botón “Abrir” y la aplicación se abrirá.
3. Luego se abrirá la aplicación mostrando la ventana en la que se puede visualizar el o los firmantes del documento.
4. Los vistos verdes confirman que se trata de una firma electrónica válida en el documento.
5. Si se ejecuta “doble clic” sobre el elemento dentro de la lista de firmantes se puede visualizar los datos de quien firmó el documento.

3 Firma del documento (S.O. MACOS)

3.1 Instalación del Certificado Remoto

Luego de haberse emitido el certificado al usuario es necesario que se realice la instalación de software y de los certificados raíz y subordinado que forman la cadena de confianza para la firma de documentos sin inconvenientes. El proceso de recopilación de documentos, según la solicitud del usuario requirente, y estos haber sido escaneados en un documento en formato PDF, se puede iniciar el proceso de firma electrónica de un archivo.

Nota: La digitalización de los documentos debe ser realizada con la suficiente definición para la lectura de los datos en el documento físico sin que esta sea muy alta para evitar documentos que ocupen más espacio del necesario.

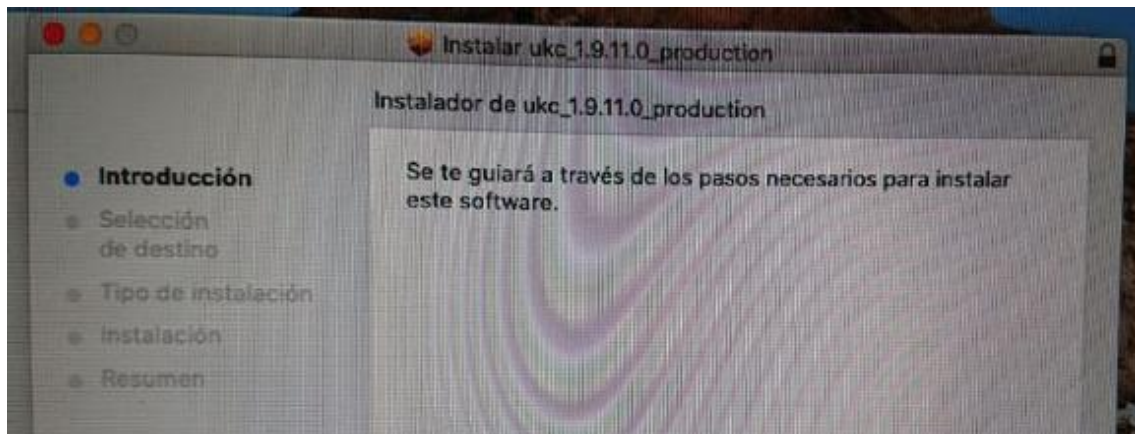
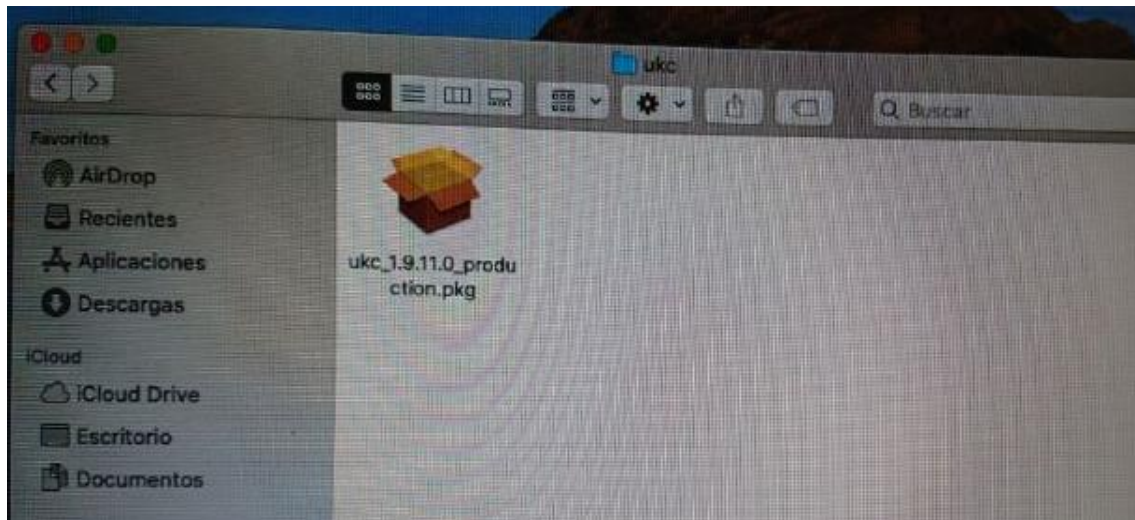
Para el uso del certificado remoto del Consejo de la Judicatura es necesaria la instalación de la aplicación UKC.

3.2 Instalación del UKC

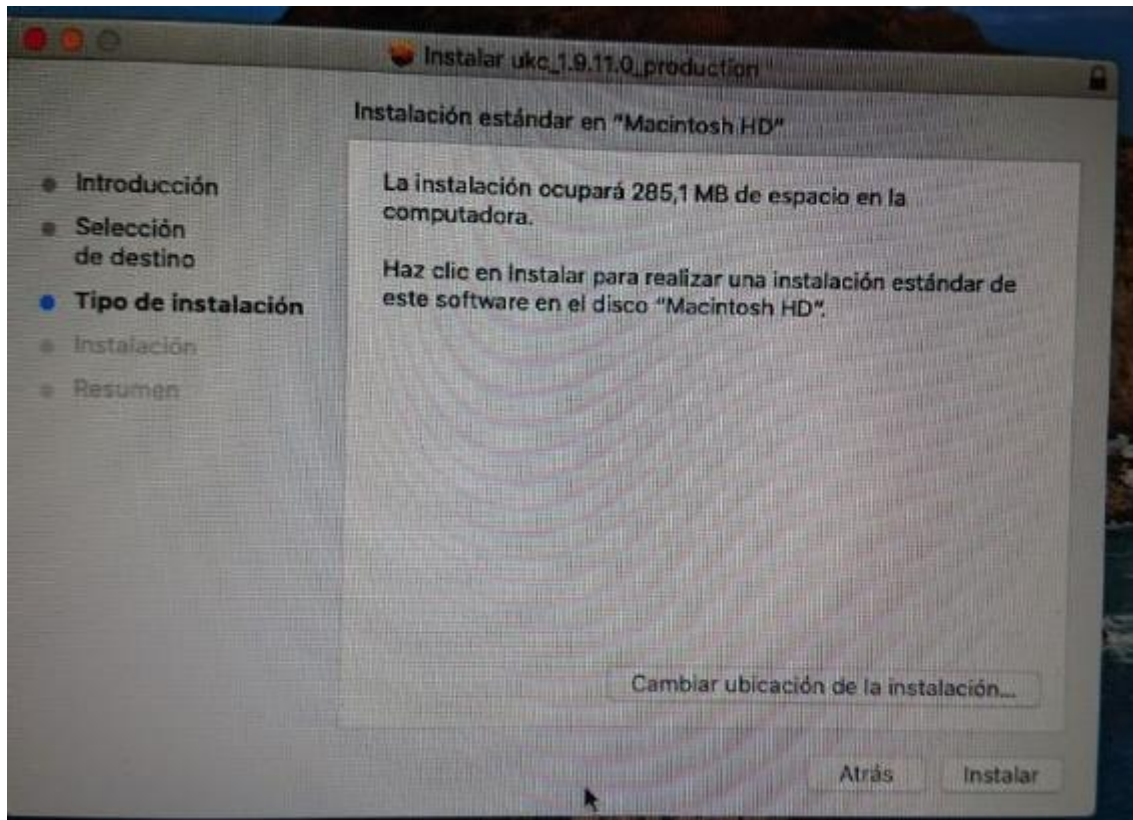
Primero se debe descargar la aplicación UKC (s.o. Windows) desde:

<https://www.icert.fje.gob.ec/web/guest/descargas3>

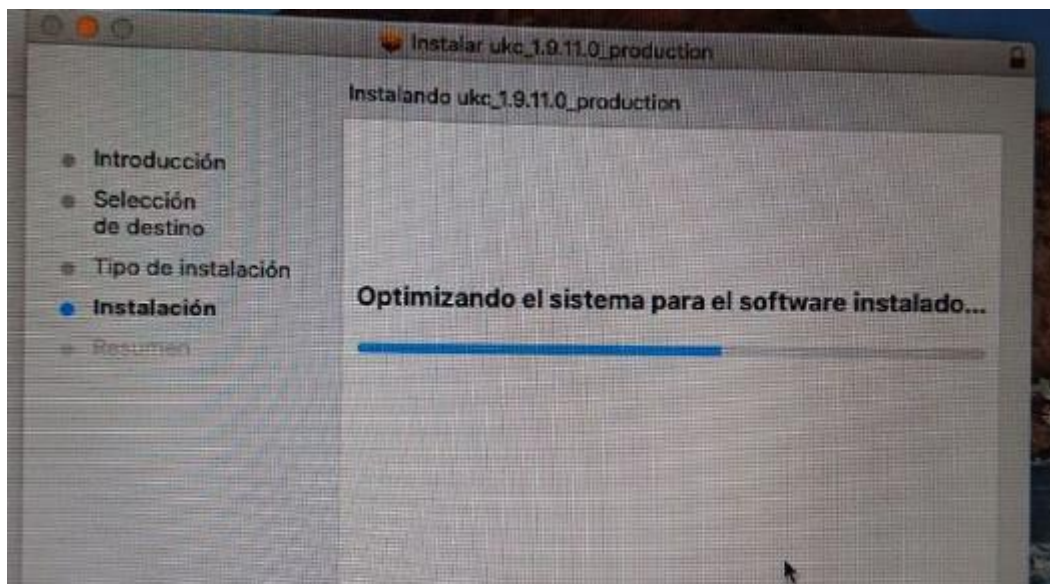
Nos dirigimos al archivo descargado y lo ejecutamos.

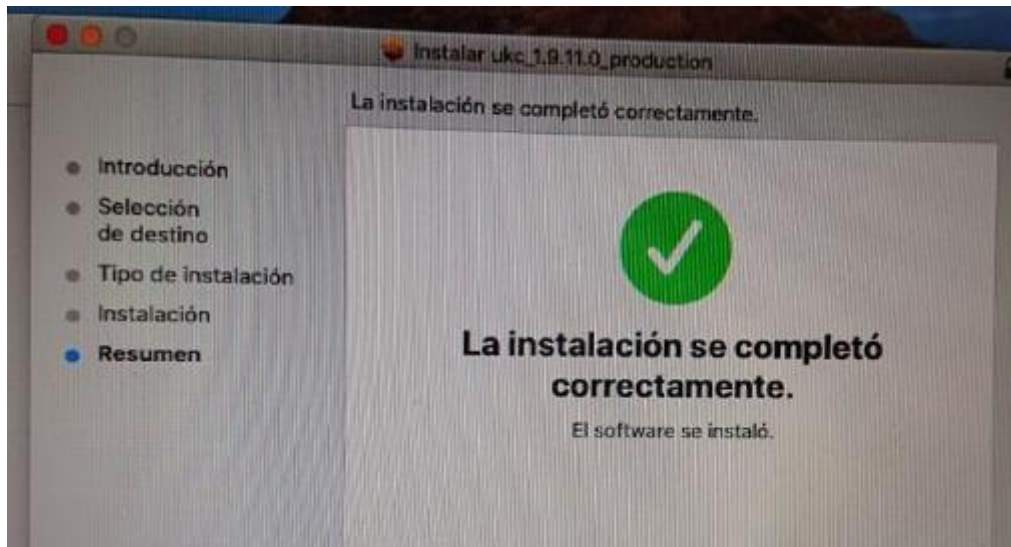


A continuación aceptamos los acuerdos de licencia.



Y la instalación procederá:

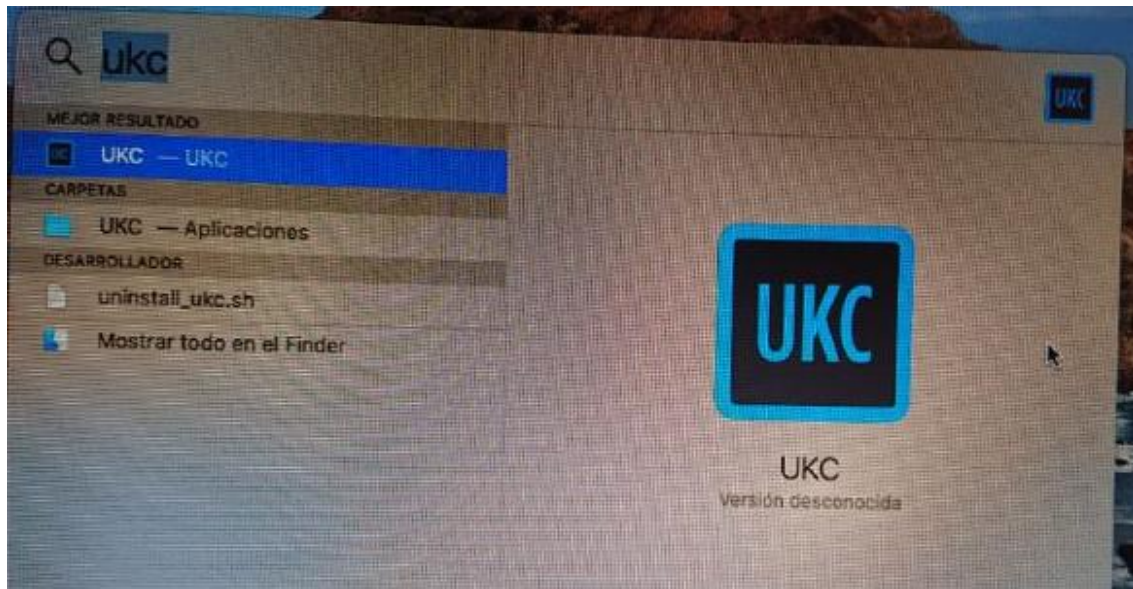




Finalmente damos clic en Cerrar y la instalación habrá finalizado. Reiniciar el equipo

3.3 Carga del Certificado Remoto en el UKC

Buscar el programa UKC.



Aquí se abrirá un pequeño cuadro de dialogo en donde nos solicita el usuario y la contraseña, las cuales fueron entregadas al cliente vía correo electrónico de manera similar de cómo se ve bajo este texto. Llenamos los datos de manera similar a la imagen y damos clic en  .



Se recomienda ubicar el visto en “Memorizar esta acción” ya que esta contraseña no puede ser cambiada, el elemento que un usuario si puede cambiar es el PIN, que es el

código de 8 dígitos que la aplicación solicita cada vez que el usuario envía a firmar un documento.

Sobre de credenciales

Estimado solicitante,
estas son las credenciales correspondiente a su identidad en formato HSM.

<u>USER ID</u>	76c86e170ba39ad/FP/1
Contraseña:	c532ceff9186847a3
PIN	69987341
<u>PUK</u>	20254624
ERC	etHQTp5Oe3

Iniciar sesión

 **Iniciar sesión en el SFC**

Usuario

76c86e170ba39ad/FP/1

Contraseña

.....

☒ Memorizar esta acción

El User ID corresponde al nombre de usuario para autenticarse.
El PIN permite el uso normal del token para la firma electrónica.
El PUK permite restaurar el PIN en caso de bloqueo u olvido.
El ERC es el código de emergencia para suspender, revocar o reactiva el certificado

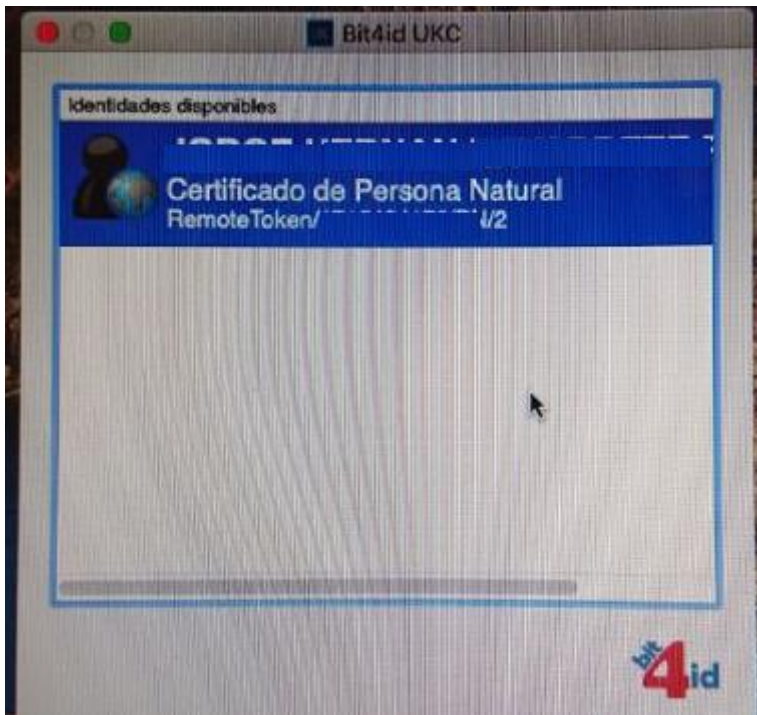
Gracias

Equipo ICERT-EC

This email has been generated by [Bit4id smartCMS](#)

Figura: 14 Sobre de credenciales

(Nota: si el equipo inicia antes de conectarse a una red de datos con acceso a internet las credenciales guardadas se descartan)



Una vez cargado el certificado se encuentra listo para ser utilizado en la firma de documentos.

3.4 Firma de documentos

Existen varias aplicaciones con la que se pueden firmar documentos, pero la que vamos a usar es el Adobe Reader DC para evitar instalar más aplicaciones y generar una confusión al agregar firmas en los documentos en formato PDF.

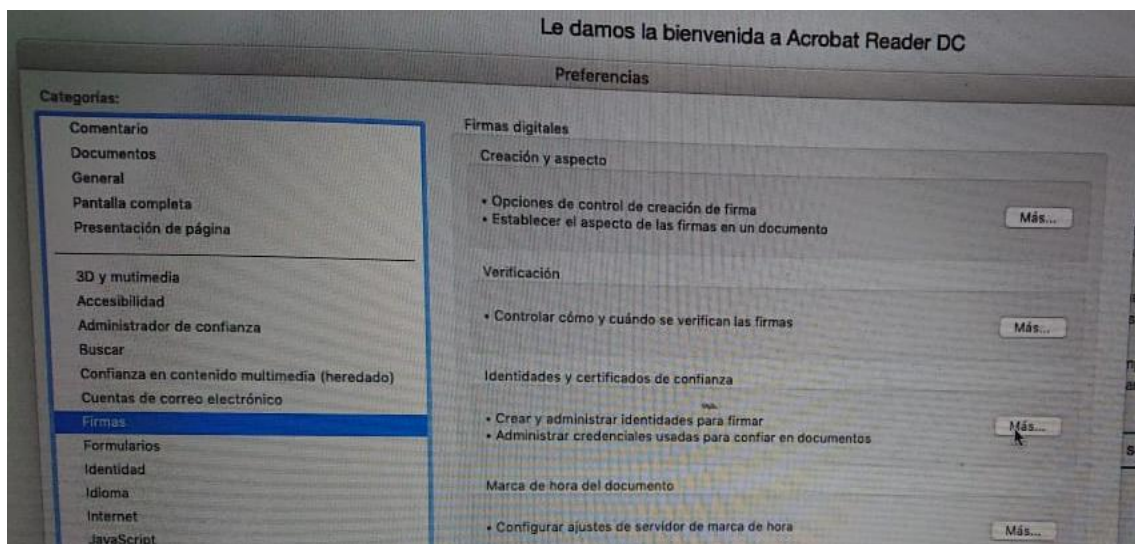
3.4.1 Configuración de Adobe Reader

Para que al firmar un documento no indique que la firma no es válida debemos realizar los siguientes pasos:

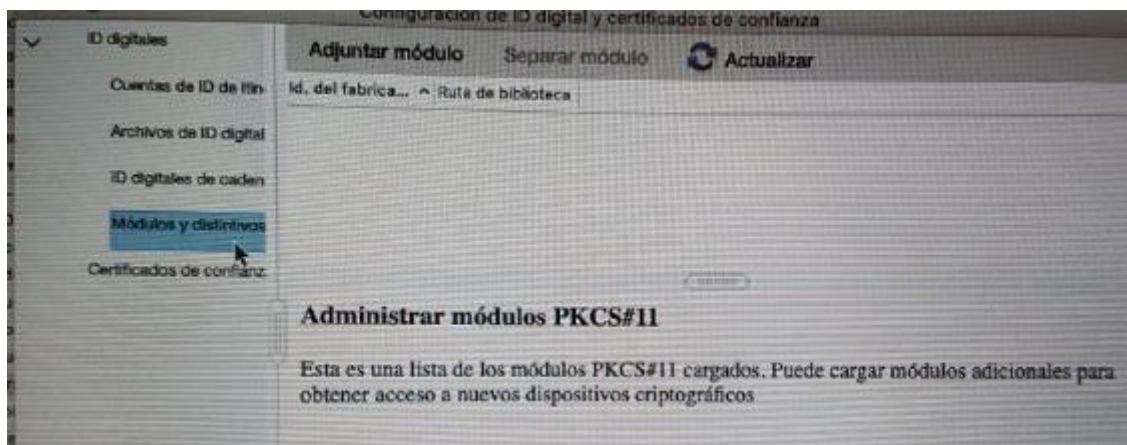
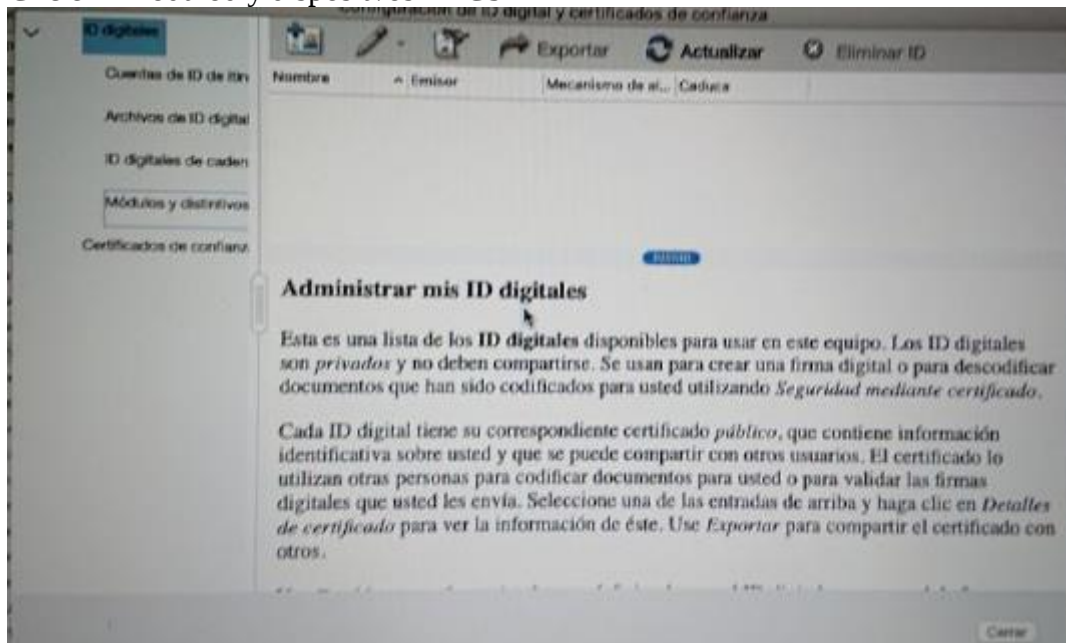
4. En un documento de Adobe ingrese al Menú y seleccione sucesivamente: Edición > Preferencias > Firmas > Identidades y certificados de confianza > Más



Clic en botón “Más”

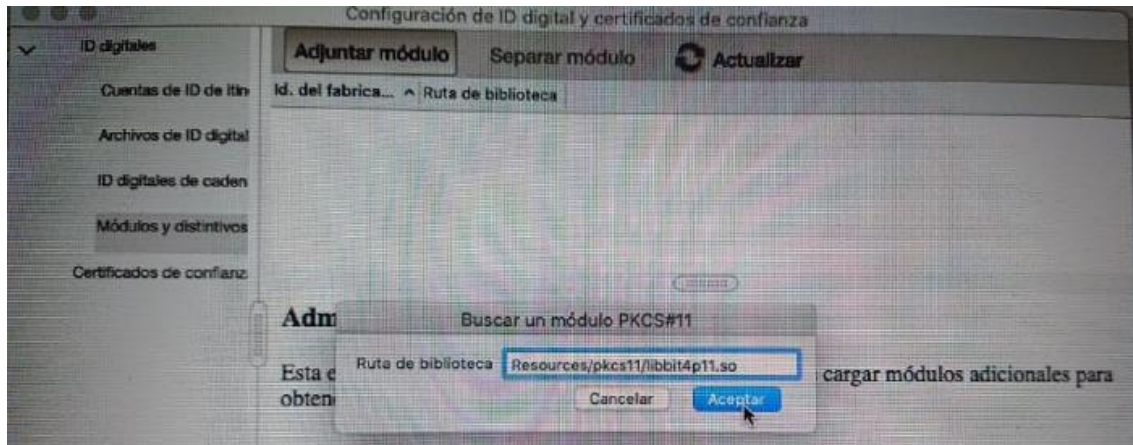


Clic en “Módulos y dispositivos PKCS#11”

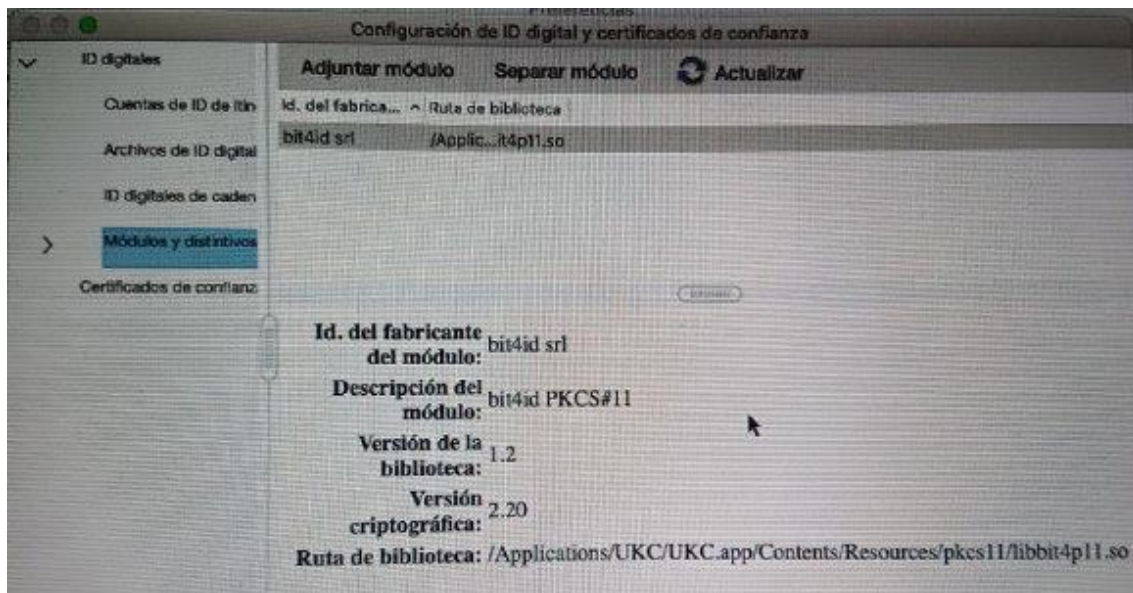


Clic en el botón “Adjuntar módulo”

El módulo suele estar instalado en la siguiente dirección dentro del sistema:
/Applications/UKC/UKC.app/Contents/Resources/pkcs11/libbit4p11.so



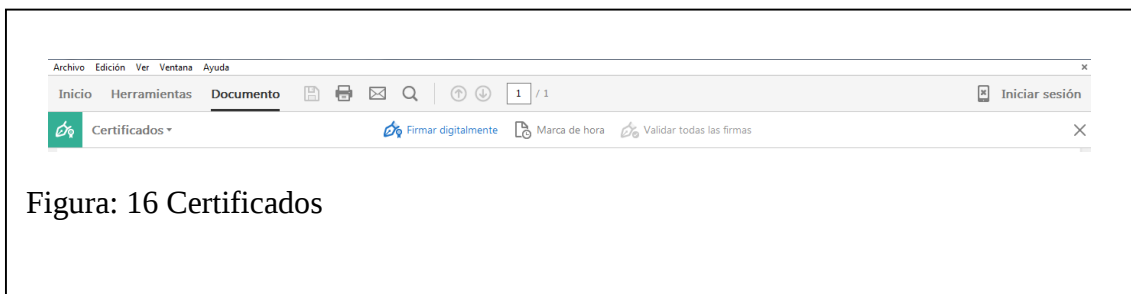
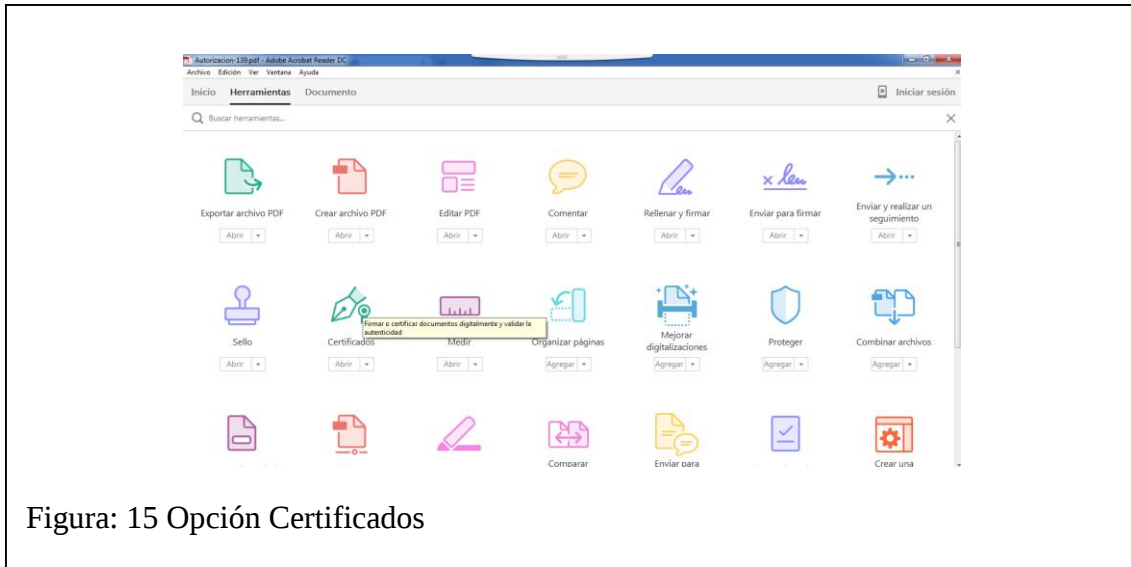
Cerrar el menú de preferencias.



3.4.2 Firma con Adobe Reader DC Versión

Para firmar un documento en esta aplicación se debe realizar lo siguiente:

1. Abrir el documento a firmar.
2. En el menú superior seleccionar Herramientas
3. Seleccionar Certificados



4. Dar clic en **Firmar digitalmente**. Hecho esto el puntero del mouse cambiará para que seleccionemos un recuadro al mantener presionado el botón derecho del mouse sobre el sitio del documento en el que deseamos ubicar la firma gráfica. A continuación se presentará un recuadro en el cual podemos seleccionar el certificado que deseamos usar para la firma y en donde se visualizará una vista previa de la firma.
5. Damos clic en **Firmar** entonces se presentará un explorador de archivos para establecer la ubicación y el nombre con el que queremos guardar el documento firmado.