

ilustre colegio provincial de abogados de a coruña 1760 - 2010



Configuración de Adobe Reader 11 / Adobe Reader DC para la validación y firma de documentos PDF con certificados ACA en sistemas Mac OS:

Requisitos previos:

- Tener instalado el software Adobe Reader (versión 11 o DC): https://get.adobe.com/es/reader/
- Tener instalado el software de ACA (Bit4id-PinManager) correspondiente: Sistemas MAC OS X Catalina/Big Sur: PIN Manager - Bi4id Middleware (ZIP) Sistemas MAC OS X antiguos: PIN Manager - TS2048 (ZIP)

Mensajes de error en la validación de Firmas: El error más común que observamos al abrir, con Adobe Reader, documentos firmados digitalmente, es que aparentemente la firma del documento no puede ser validada. Esto sucede cuando Adobe Reader no es capaz de comprobar la validez de algunos certificados automáticamente. Este problema se soluciona importando manualmente los Certificados Raíz e Intermedios y estableciendo la confianza explícita en los mismos, como se verá más adelante.

Ejemplo de mensaje de error validando un documento firmado digitalmente en Adobe Reader:



1.- Establecer la confianza de MacOS en nuestro certificado ACA:

El primer paso es establecer la confianza en nuestro certificado almacenado en la tarjeta ACA. Esto se hace desde la aplicación "Acceso a Llaveros" (La encontraremos en el Finder: Aplicaciones -> Utilidades -> Acceso a LLaveros). Dentro de la aplicación seleccionamos la tarjeta ACA (1) y visualizaremos nuestro certificado. Hacemos doble click con el ratón sobre el certificado (2) para mostrar sus propiedades:



En la ventana de propiedades del certificado, desplegamos la opción de "Confiar" (1) para ver las opciones de confianza. En "Al utilizar el certificado" seleccionamos "Confiar siempre" (2):

🖲 😑 NOMBRE	JAVIER - NIF	😑 😑 🕒 NOMBRE	JAVIER - NIF
Certificate Emitido por: ACA - Cer Caduca: domingo, 15 d Pacífico) Este certificado ha s	JAVIER - NIF tificados Corporativos - 2014 e diciembre de 2019, 7:41:18 (hora estándar del ido firmado por una entidad desconocida	Certificato Emitido por: ACA - Certi Caduca: domingo, 15 de Pacífico) Sete certificado ha sio	JAVIER - NIF ficados Corporativos - 2014 diciembre de 2019, 7:41:18 (hora estándar del do firmado por una entidad desconocida
Confiar	-25	▼ Confiar	Usar ajustes por omisión
Al utilizar este certificado:	Usar ajustes por omisión 💿 ?	Al utilizar este certificad 🗸	Confiar siempre ?
SSL (Secure Sockets Layer)	ningún valor especificado 📀	SSL (Secure Sockets Layer)	ningún valor especificado 📀
Correo seguro (S/MIME)	ningún valor especificado ᅌ	Correo seguro (S/MIME)	ningún valor especificado 📀
Autenticación ampliable (EAP)	ningún valor especificado ᅌ	Autenticación ampliable (EAP)	ningún valor especificado 📀
Seguridad IP (IPsec)	ningún valor especificado ᅌ	Seguridad IP (IPsec)	ningún valor especificado ᅌ
Firma de código	ningún valor especificado ᅌ	Firma de código	ningún valor especificado 📀
Impresión de fecha	ningún valor especificado 😳	Impresión de fecha	ningún valor especificado ᅌ
Política básica X.509	ningún valor especificado ᅌ	Política básica X.509	ningún valor especificado 😳
♥ Detalles		▼ Detalles	
Nombre del sujeto		Nombre del sujeto	
Otro nombre		Otro nombre	
Apellidos		Apellidos	<u>8</u>

Vemos que todas las opciones de confianza aparecen ahora como "Confiar siempre". Cerramos la ventana de propiedades del certificado y, al hacer esto, se nos pedirá la <u>contraseña de usuario de Mac</u> para aceptar los cambios.



Nuestro certificado ACA aparece ahora como certificado de confianza para el MacOS:

			_	-	
Certificate Similar Coduce domin Coduce domin Street Emitido por: A Coduce domin					
Nombre		Clase	Modificación	Caducidad ^	Llavero
R NOMBRE	JAVIER - NIF	certificado		15 dic 2019 7:41:18	SmartCard
Private Key 0 - SIGN		clave privada			SmartCard
	Nombre Nombre Nombre Private Key 0 - SIGN	NOMBRE Emitido por: ACA - Certificados Corpo Coducos demines - SE da disiombra de Control de Contro	NOMBRE JAVIEI Emitido por: ACA - Certificados Corporativos - 2014 Caluea demingo - 16 da disiombro do 2010, 7:41:18 (bera actéricado está marcado como fiable para esta cuenta) Nombre Clase Nombre Clase Nombre JAVIER - NIF OPrivate Key 0 - SIGN clave privada	NOMBRE JAVIER - NIF Emitido por: ACA - Certificados Corporativos - 2010 7:41:19 (boro portándar del Pacífico) © Este certificado está marcado como flable para esta cuenta Nombre Clase MOMBRE JAVIER - NIF © Private Key 0 - SIGN	NOMBRE JAVIER - NIF Emitido por: ACA - Certificados Corporativos - 2010 7:41:18 (bera actándar del Pacífico) © Este certificado está marcado como fiable para esta cuenta Nombre Clase MOMBRE JAVIER - NIF © Private Key 0 - SIGN Clave privada 15 dic 2019 7:41:18 © Private Key 0 - SIGN

2.- Estableciendo el formato de Firma en Adobe Reader:

Abrimos las preferencias de Adobe Reader:



Seleccionamos, dentro del catálogo de Categorías de la izquierda "Firmas" (1), y en el apartado Firmas digitales: Creación y aspecto pinchamos en el botón "Más..." (2):

	Preferencias	
ategorías:	Planet distant	
Comentario	Firmas digitales	
Documentos	Creación y aspecto	
General		
Pantalla completa	Opciones de control de creación de firma Establecer el aspecto de las firmas en un documento	Más Z
Presentación de página		
2D v mutimodia	Verificación	
Accesibilidad		
Administrador de confianza	 Controlar como y cuándo se verifican las firmas 	Más
Buscar		
Confianza en contenido multimedia (heredado)	Identidades y certificados de confianza	
Cuentas de correo electrónico		
Firmas 1	Crear y administrar identidades para firmar	Más
Formularios	Administrar credenciales usadas para confiar en documentos	
Identidad		
Idioma	Marca de hora del documento	
Internet	. Configure single de servides de mars de bars	
JavaScript	Comigural ajustes de servidor de marca de nora	Mas
Lectura		
Medición (2D)		
Medición (3D)		
Medición (Geo)		
Multimedia (heredado)		
Ortografía		

En la ventana de Preferencias de creación y aspecto, comprobamos que esté seleccionada la opción "Equivalente a CadES" (1) en el desplegable y a continuación pinchamos en "Aceptar" (2):

Creación Método de firma predeterminado: Seguridad predet. de Adobe C Formato de firma predeterminado: PKCS#7: separado Al firmar: Equivalente a CAdES 1 Mostrar motivos Mostrar ubicación e información de contacto Incluir estado de revocación de la firma Ver documentos en modo de vista previa Activar revisión de advertencias de documento: Al certificar un documento C Impedir firmar hasta que se hayan revisado las advertencias: Nunca C Utilizar la interfaz de usuario moderna para la configuración de firma e ID digital Aspectos Nuevo Editar Duplicar Eliminar		cholds de credelon y dispecto
Método de firma predeterminado: Seguridad predet. de Adobe © Formato de firma predeterminado: PKCS#7: separado Al firmar: Equivalente a CACES 1 Mostrar motivos Mostrar ubicación e información de contacto Nuclai estado de revocación de la firma Ver documentos en modo de vista previa Activar revisión de advertencias de documento: Al certificar un documento © Impedir firmar hasta que se hayan revisado las advertencias: Nunca © Utilizar la interfaz de usuario moderna para la configuración de firma e ID digital Aspectos	Creación	
Formato de firma predeterminado: PKCS#7: separado Al firmar: Mostrar motivos Mostrar ubicación e información de contacto Mostrar ubicación de información de contacto Incluir estado de revocación de la firma Ver documentos en modo de vista previa Activar revisión de advertencias de documento: Al certificar un documento © Impedir firmar hasta que se hayan revisado las advertencias: Nunca Utilizar la interfaz de usuarlo moderna para la configuración de firma e ID digital Aspectos	Método de firma predeterminado:	Seguridad predet. de Adobe
Mostrar motivos Mostrar ubicación e información de contacto Incluir estado de revocación de la firma Ver documentos en modo de vista previa Activar revisión de advertencias de documento: Al certificar un documento Impedir firmar hasta que se hayan revisado las advertencias: Nunca Impedir firmar hasta que se hayan revisado las advertencias: Nunca Impedir firmar hasta que se hayan revisado las advertencias: Nunca Impedir firmar hasta que se hayan revisado las advertencias: Nunca Impedir firmar hasta que se hayan revisado las advertencias: Nunca Impedir firmar hasta que se hayan revisado las advertencias: Nunca Impedir firmar hasta que se hayan revisado las advertencias: Nunca Impedir firmar hasta que se hayan revisado las advertencias: Nunca Impedir firmar hasta que se hayan revisado las advertencias: Nunca Impedir firmar hasta que se hayan revisado las advertencias: Nunca Impedir firmar hasta que se hayan revisado las advertencias: Nunca Impedir firmar hasta que se hayan revisado las advertencias: Nunca Impedir firmar hasta que se hayan revisado las advertencias: Nunca Impedir firmar hasta que se hayan revisado las advertencias: Nunca Impedir firmar hasta que se hayan revisado las advertencias: Nunca Impedir firmar hasta que se hayan revisado las advertencias: Nunca Impedir firmar hasta que se hayan revisado las advertencias: Nunca Impedir firmar hasta que se hayan revisado las advertencias: Nunca Impedir firmar hasta que se hayan revisado las advertencias: Nunca Impedir firmar hasta que se hayan revisado las advertencias: Nunca Impedir firmar hasta que se hayan revisado las advertencias: Nunca Impedir firmar hasta que se hayan revisado las advertencias: Nunca Impedir firmar hasta que se hayan revisado las advertencias: Impedir firmar hasta que se hayan revisado las advertencias: Impedir firmar hasta que se hayan revisado las advertencias: Impedir firmar hasta que se hayan revisado las advertencias: Impedir firmar hasta que se hayan revisado las advertencias: Impedir firmar hasta	Formato de firma predeterminado: Al firmar:	✓ PKCS#7: separado Equivalente a CAdES 1
Mostrar ubicación e información de contacto Incluir estado de revocación de la firma Ver documentos en modo de vista previa Activar revisión de advertencias de documento: Al certificar un documento C Impedir firmar hasta que se hayan revisado las advertencias: Nunca C Utilizar la interfaz de usuario moderna para la configuración de firma e ID digital Aspectos Nuevo Editar Duplicar Eliminar	Mostrar motivos	
Incluir estado de revocación de la firma Ver documentos en modo de vista previa Activar revisión de advertencias de documento: Al certificar un documento C Impedir firmar hasta que se hayan revisado las advertencias: Nunca C Utilizar la interfaz de usuario moderna para la configuración de firma e ID digital Aspectos Nuevo Editar Duplicar Eliminar	Mostrar ubicación e informa	ción de contacto
Ver documentos en modo de vista previa Activar revisión de advertencias de documento: Al certificar un documento 3 Impedir firmar hasta que se hayan revisado las advertencias: Nunca 3 Vullizar la interfaz de usuario moderna para la configuración de firma e ID digital Aspectos Nuevo Editar Duplicar Eliminar	🕑 Incluir estado de revocación	n de la firma
Activar revisión de advertencias de documento: Al certificar un documento 3 Impedir firmar hasta que se hayan revisado las advertencias: Nunca 3 Utilizar la interfaz de usuario moderna para la configuración de firma e ID digital Aspectos Nuevo Editar Duplicar Eliminar	🗌 Ver documentos en modo de	e vista previa
Impedir firmar hasta que se hayan revisado las advertencias: Nunca S Utilizar la interfaz de usuario moderna para la configuración de firma e ID digital Aspectos Nuevo Editar Duplicar Eliminar	Activar revisión de advertencias de o	documento: Al certificar un documento 📀
Aspectos Nuevo Editar Dupilcar Eliminar	Indedi Infidi fidsta que se fidvari le	
Nuevo Editar Dupilcar Eliminar	Utilizar la interfaz de usuario mo	derna para la configuración de firma e ID digital
Editar Dupilcar Eliminar	Utilizar la interfaz de usuario mo	derna para la configuración de firma e ID digital
Dupilcar Eliminar	Utilizar la interfaz de usuario mo	derna para la configuración de firma e ID digital
Eliminar	Utilizar la interfaz de usuario mo	derna para la configuración de firma e ID digital
Eliminar	Utilizar la interfaz de usuario mo	derna para la configuración de firma e ID digital
	Utilizar la interfaz de usuario mo	derna para la configuración de firma e ID digital
	Utilizar la interfaz de usuario mo	derna para la configuración de firma e ID digital Nuevo Editar Duplicar Eliminar
	Utilizar la interfaz de usuario mo	derna para la configuración de firma e ID digital Nuevo Editar Duplicar Eliminar

Con esto ya habremos configurado el formato correcto a utilizar en el proceso de firma.

3.- Configuración para la Firma de PDFs con certificados ACA:

El primer paso será adjuntar el Módulo criptográfico que nos permitirá acceder a la tarjeta ACA y usar el certificado:

Para ello, como en los pasos anteriores, abrimos las preferencias de Adobe Reader y seleccionamos la Categoría "Firmas" (1) y en el apartado "Identidades y certificados de confianza" y pinchamos en el botón "Más..." (2):

	Preferencias	
tegorías:		
Comentario	Firmas digitales	
Documentos	Creación y aspecto	
General		
Pantalla completa	Opciones de control de creación de firma Establecer el aspecto de las firmas en un decumento	Más
Presentación de página	Establecer el aspecto de las inmas en un documento	
	Verificación	
3D y mutimedia		
Accesibilidad	 Controlar cómo y cuándo se verifican las firmas 	Más
Administrador de confianza		
Buscar	Mantidadas y sortificadas da configeras	
Confianza en contenido multimedia (heredado)	identidades y certificados de comanza	-
Cuentas de correo electronico	Crear v administrar identidades para firmar	Más 2
Firmas 1	Administrar credenciales usadas para confiar en documentos	(Widow) Z
Formularios		
Identidad	Marca de hora del documento	
Idioma		
Internet	Configurar ajustes de servidor de marca de hora	Más
JavaScript		And a second second
Lectura		
Medición (2D)		
Medición (3D)		
Medición (Geo)		
Multimedia (heredado)		
Ortografía		

En el menú de la izquierda seleccionamos "Módulos y distintivos" (1) y a continuación en "Adjuntar módulo" (2):



Después de pinchar en "Adjuntar Modulo" nos aparece la siguiente ventana:

Busc	ar un modulo PRCS#11
Ruta de biblioteca	libbit4ipki.dylib
	Cancelar Aceptar

En "Ruta de biblioteca", escribimos libbit4ipki.dylib, y pinchamos en "Aceptar". <u>AVISO IMPORTANTE:</u> En las versiones de Adobe Reader DC (a partir de octubre de 2019), es necesario escribir la ruta completa /Library/bit4id/pkcs11/libbit4ipki.dylib

Al expandir la opción "Módulos y distintivos" observamos que se ha cargado correctamente el módulo criptográfico "bit4id PKCS#11" y se muestra el acceso a la tarjeta ACA denominada "DSD":

0.0	•	Configur	ación de ID dig	ital y	/ certificados de confianza	
~	ID digitales Cuentas de ID de itin	Adjuntar módulo Id. del fabrica A	Separar módulo Ruta de bibliotec	3	Actualizar	
~	Archivos de ID digital ID digitales de caden Módulos y distintivos	bit4id srl	libbit4ipki.dylib			
	bit4id PKCS#11					
	DSD Certificados de confianz		Id. de I	l fab Descr Versi Ve	pricante del módulo: bit4id srl rripción del módulo: bit4id PKCS#11 sión de la biblioteca: 1.2 ersión criptográfica: 2.20 Ruta de biblioteca: libbit4ipki.dylib	
1						Cerrar

Seleccionamos la tarjeta "DSD" (1) y a continuación pinchamos en "Agregar ID Digital" (2)

		Configuración de ID	digital y certificados de o	confianza		
ID) digitales	👔 🎾 Opciones de uso 👻	Detalles del certificado	🚧 Exportar	C Actualizar	🙆 Eliminar ID
	Cuentas de ID de itin Nor	nbre ^ Emisor	Caduca			
	Archivos de ID digital					
	ID digitales de caden					
,	Módulos y distintivos					
	bit4id PKCS#11					
~						
	DSD 1					
Ce	ertificados de confianz					
						(a

Ahora se nos pedirá el PIN de nuestra tarjeta ACA, lo introducimos y pinchamos el botón "Aceptar":

tiqueta de d	listintivo: DSD	
Contraseña:		

Se mostrará la siguiente ventana, donde pincharemos el botón "Cancelar":

Agrega	ar un ID digital
Este asistente permite agregar un ID digital	al distintivo criptográfico seleccionado.
Importar un ID digital existente	
Buscar un ID digital existente para agre	gar al distintivo criptográfico seleccionado.
🔿 Agregar un nuevo ID digital con firma	personal
Cancelar	e Atric
Cancelar	S Atras

Se visualizará el certificado de la tarjeta ACA, que seleccionaremos pinchando sobre él. Una vez seleccionado se visualizará resaltado en azul, como en la imagen (1). A continuación, en el menú superior, pinchamos "Opciones de uso" y seleccionamos la opción "Usar para firmar" (2):

0:0	•	Configuración de ID digital y cer	tificados de confianza		
~	ID digitales	💼 🥖 Opciones de uso 👻 Detalles	del certificado 🛛 🧀 Exporta	r 🔁 Actualizar 🔕 Eliminar I	ID
	Cuentas de ID de itin	Nombre / Usar para firmar 🛛 💍	> Cade	uca	
	Archivos de ID digital	NOMB Administrar certificados de	atributos - 2014 201	9.12.15 15:41:18 Z	
	ID digitales de caden				
\sim	Módulos y distintivos				
	bit4id PKCS#11		(100000)		_
	DSD	NOMBRE		JAVIER - NIF	
	Certificados de confianz	Ilustre Colegio Provincia Emitido por: Consejo General de la Abo Válido desde: Válido 2019/12/15 07:41:18 -08'0 Válido hasta: Uso Firma digital, Sin rechazar deseado: clave, Autenticación de cli	l de Abogados de A C o ativos - 2014 ogacia 0' 0' , Codificar claves, Codi ente, Protección de corr	ruña / ICACOR / 2037 ficar documento, Acuerdo de eo electrónico	B
				Cerra	r)

Tras el paso anterior, nuestro certificado debe aparecer con la imagen de una estilográfica delante 🥒, tal y como se muestra en la siguiente imagen:



Cerramos todas las ventanas de configuración y a continuación salimos de Adobe Reader.

Ya tenemos la aplicación lista para firmar archivos PDF con nuestro certificado ACA.

4.- Firmando PDFs en Adobe Reader con certificados ACA:

Abrimos el PDF que deseamos firmar. A continuación pinchamos en el menú "Herramientas" (1) y seguidamente en la imagen "Certificados" (2)



Se visualizará el PDF que hemos abierto previamente con una nueva barra de herramientas, donde pincharemos en la opción "Firmar digitalmente":

	Documento de Pruebapdf								
Inic	io Herramient	tas Documento	de Pr ×		? Ini	ciar sesión			
Ð	ቀ 🖶 🖂	Q 🔿 🕀 🕹	1 / 1	• 🕛 🖸 🕂	81,3% -				
Óq	Certificados *	🖧 Firmar digitalmente	Marca de h	nora 🧞 Validar toda	as las firmas	×			
Ø									
Ø									

Se mostrará el siguiente mensaje de aviso, indicando que dibujemos con el ratón el área donde queremos visualizar la firma visible en el documento.



A continuación dibujamos con el ratón, manteniendo pulsado el botón izquierdo, el área donde se insertará la firma visible. (Normalmente lo haremos al final de la última página del documento PDF) Una vez dibujada el área soltamos el botón del ratón para finalizar.

Chaves en equil de la incessor revestre déride se vieveliseré le finnes del sis



Automáticamente se nos pedirá que seleccionemos el certificado para la firma. Comprobamos que realmente está leyendo el certificado almacenado en la tarjeta si visualizamos (Dispositivo PKCS#11), como en la siguiente imagen. Pinchamos en el botón "Continuar":

n un ID digital		×
el ID digital que desee utilizar	r para la firma:	Actualizar
NOMBRE Emitido por: ACA - Certificados	(Dispositivo PKCS#11) s Corporati, Caduca: 2019.12.15	Ver detalles
_		
	n un ID digital el ID digital que desee utilizar NOMBRE Emitido por: ACA - Certificados	el ID digital que desee utilizar para la firma: NOMBRE (Dispositivo PKCS#11) Emitido por: ACA - Certificados Corporati, Caduca: 2019.12.15

Ahora se nos pedirá el PIN de la tarjeta para proceder a la firma. Introducimos el Pin (1) y pinchamos en "Firmar" (2)

Firmar como "NOMBRE	×
Aspecto Texto normal 🗸	Crear
NOMBRE	Firmado digitalmente por NOMBRE
FRANCISCO JAVIER	JAVIER - NIF Fecha: 2018.02.12 09:29:17 +01'00'
🔲 Bloquear el documento tras la firma	Ver detalles del certificado
Escriba el PIN o la contraseña del ID digital:	Atrás Firmar
Pin introducido y listo para firmar]
Bloquear el documento tras la firma	Ver detalles del certificado
	Atrás Firmar

Adobe Reader nos preguntará dónde queremos guardar el PDF firmado. Seleccionamos la ubicación y el nombre de archivo deseado y guardamos el PDF. (También podemos sobreescribir el fichero si lo deseeamos)

		Guardar como	
Guard	ar como: tiquetas:	Documento de Prueba	
U	bicación:	Escritorio	0
Formato:	Archivos	Adobe PDF 📀	
		Cancelar	Guardar

Al abrir el documento que acabos de firmar, veremos que la firma se valida correctamente (1). Si pinchamos en el panel de firmas (2) veremos los detalles de la firma y del certificado. Asimismo, comprobaremos que la firma visible también se visualiza documento (3)

