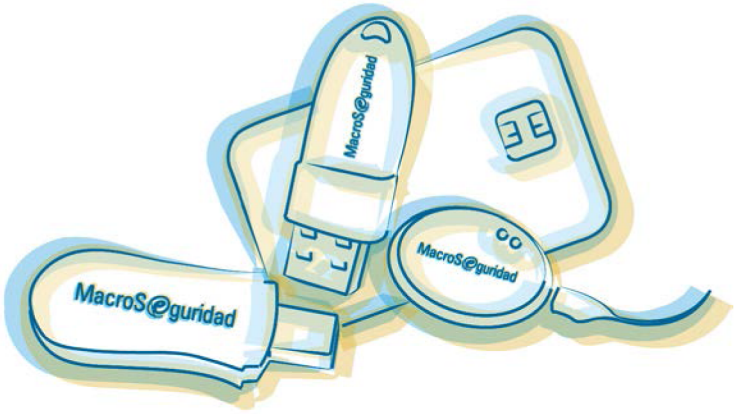
“Guía de Integración PKI Adobe Acrobat Reader DC con ePass2003 de Macroseguridad.org en macOS”



Nombre del Partner	ePass2003 FIPS #3202
Nombre de la Solución	Integración Adobe con Dispositivos Criptográficos de Macroseguridad (Tokens USB y Smartcards)
Fecha	5 de Enero de 2021

Desarrollado por el Departamento IT
de Macroseguridad y el Equipo de Integraciones

Revisiones:

Versión	Autor	Fecha	Comentarios
1.0	Guillermo Nievas	05/01/2021	Release inicial

Tabla de Contenidos

A Acerca de Macroseguridad

Macroseguridad.org es un Mayorista exclusivo de Soluciones de Seguridad Informática, Líder en seguridad digital y proveedor de seguridad para comercio electrónico e Internet. La compañía atiende a clientes en toda Latino América, México y Brasil.

Macroseguridad.org cuenta con una experiencia de más de 10 años en el área de seguridad y más de 20 años en el conocimiento y manejo de canales de distribución. Sus consultores y profesionales (Partners, Resellers, Integradores y Partners HI-TECH) demuestran un sólido expertise en los servicios y productos que ofrecen, gracias a un sistema orgánico de capacitación continua tanto en el país como en el exterior, con un amplio conocimiento en diferentes industrias para lograr la diversificación que nuestros clientes necesitan.

Macroseguridad.org incluye en su portfolio de productos: Tokens USB y Smartcards que brindan autenticación robusta, portabilidad y transporte seguro de certificados digitales para Firma Digital. A su vez son un mecanismo de doble factor de autenticación de usuarios en los accesos a la red para garantizar su identidad (VPN, SSLVPN, Web Portal). Tokens OTP (One-Time-Password), dispositivos generadores de números aleatorios para autenticación robusta de usuarios, software para single-sign-on y autenticación.

Tambien ofrece Lectoras de Smartcards (con o sin biometría, de contacto y contactless -NFC-, etc), junto con Lectoras Biométricas con estándares de seguridad mundial que poseen certificaciones del FBI IAFIS Appendix F, FBI PIV/FIPS 201 y FBI Mobile ID FAP 10 así como también cumplen con los estándares ANSI-378 y ISO19794-2/4. Ademas, provee Soluciones de Time Stamping, Timbre Digital, HSM (hardware security module), que son equipos utilizados para el resguardo, generación de claves privadas y Firma Digital Cloud. Y Soluciones para Medios de pago que cumplen los requerimientos y estándares de Payment Cards y EMV (PCI DSS).

Macroseguridad.org a su vez ofrece Certificados Digitales SSL para validación de dominios web y protección de datos sensibles en la red, con licencia para ilimitados servidores y compatibles con todos los webservers. Contamos con Certificados SSL para dominio único, certificados Wildcard, multi-dominios y certificados que cumplen con el estándar EV SSL (simple y multi-dominio). También certificados para encripción y firma digital de correos corporativos y certificados Code Signing (Firma de Código) que jerarquizan la venta de software vía Internet y evitan los mensajes de error en la descarga y ejecución de software.

Además, soluciones orientadas a los administradores de servidores como UserLock (orientada a robustecer las políticas de seguridad dentro de un Active Directory) y FileAudit (orientada a la auditoría de carpetas y archivos dentro de un File Server).

Por último, MacroSeguridad.org también distribuye soluciones para la Administración de Derechos Digitales, por ejemplo Dongles - sistemas de protección de software basados en hardware (llaves USB) – para la protección de la propiedad intelectual de los desarrolladores.

Macroseguridad Latino América logra el equilibrio entre las necesidades de las empresas y sus soluciones.

Para más información puede visitar www.macroseguridad.net

B Información de Contacto

Por cualquier consulta, sugerencia o comentario sobre la utilización de la solución o de esta guía, por favor contacte al soporte técnico de MacroSeguridad Latino América

Mail: soporte@macroseguridad.net

Portal de soporte: https://soporte.macroseguridad.la

Web: www.macroseguridad.net

C Copyright y Marcas Registradas

D Acuerdo de Licencia

MacroSeguridad Latino América

LEA ATENTAMENTE ANTES DE CONTINUAR CON LA INSTALACIÓN DE SOFTWARE Y/O HARDWARE.

Todos los Productos de Software y/o Hardware que en Latinoamérica son distribuidos por Macroseguridad Latino América (MS Argentina SRL) incluyendo, pero no limitados a, copias de evaluación, diskettes, CD ROMs, hardware y documentación, y todas las órdenes futuras, están sujetas a los términos de este Acuerdo de Licencia y Uso. Si Ud. no está de conforme con los términos aquí incluidos, por favor devuélvanos el paquete de evaluación, empaque y contenido prepago, dentro de los diez (10) días de su recepción, y le reembolsaremos el precio del producto, menos los gastos de envío y cargos incurridos.

1. **Uso Permitido** – Respecto del Software el presente es un acuerdo de Licencia de Uso. Usted no adquiere la propiedad sobre el Software objeto de este Acuerdo sino un Permiso (Licencia) para utilizarlo de conformidad a las siguientes especificaciones. TODOS LOS DERECHOS DE PROPIEDAD INTELECTUAL (incluyendo pero no limitando derechos de autor, secretos comerciales, marcas y patentes) relacionados con el Software, Hardware, sus códigos fuentes, guías de usuario y toda otra documentación comprensiva del mismo son de propiedad exclusiva de Macroseguridad Latino América (MS Argentina SRL) o de las compañías que ésta representa. Ud. puede utilizar este Software únicamente en modo ejecutable, utilizándolo sólo en las computadoras de su empresa u organización, y pudiendo hacer sólo las copias adquiridas en el proceso de compra. En relación al Hardware comercializado por Macroseguridad, usted deberá utilizarlo conforme todas las especificaciones y recomendaciones técnicas informadas. En caso de duda, comunicarlas en el portal de soporte **https://soporte.macroseguridad.la**:

   IMPORTANTE PARA DISPOSITIVOS CRIPTOGRÁFICOS: Si el dispositivo criptográfico provisto por MACROSEGURIDAD es utilizado apropiadamente y conforme su destino, en el entorno recomendado (Sistema operativo Windows) y con las PASSWORDS correctas, el mismo no bloquea en ningún caso el acceso a la información.

   Si esto ocurre, no es por un defecto del producto, sino que, se produce para el resguardo de la información contenida en el dispositivo ante intentos no autorizados o erróneos (por impericia o negligencia del usuario), cumpliendo de esta manera su finalidad.

   Se debe tener especial cuidado y precaución en el manejo del dispositivo en el entorno recomendado, así como en el resguardo y respaldo de PASSWORDS de USUARIO y/o ADMINISTRADOR. Al adquirir el producto, el Usuario se compromete a seguir TODAS las recomendaciones técnicas provistas por MACROSEGURIDAD y ante cualquier duda, consultar al equipo de soporte técnico en **https://soporte.macroseguridad.la**

2. **Uso Prohibido** – No puede utilizarse el Software ni el Hardware con otro propósito que el descripto en el apartado 1. El Software o el Hardware o cualquier otra parte del producto no puede ser copiado, realizarse reingeniería, desensamblarse, descompilarse, revisarse, ser mejorado y/o modificado de ninguna otra manera, excepto como específicamente se encuentra admitido en el item 1. Ud. no pude utilizar ingeniería inversa en el Software ni en ninguna otra parte del mismo ni intentar descubrir su código fuente. No está permitido tampoco: (1) usar, modificar, fusionar o sublicenciar el Software, salvo lo expresamente autorizado en este contrato; (2) vender, licenciar o sub-licenciar, arrendar, asignar, transferir, comprometerse o compartir sus derechos bajo esta licencia con terceros ;(3) modificar, desensamblar, descompilar, realizar ingeniería inversa, revisar o mejorar el Software o el intento de descubrir el código de fuente del Software; (4) Colocar el Software en un servidor para que sea accesible a través de una red pública; o (5) utilizar cualquier copia de respaldo o archivo del Software (o permitir a otra persona a usar dichas copias) para cualquier propósito distinto del establecido en la presente Licencia.

3. **Garantía** – Se garantiza el Software y el Hardware está sustancialmente libre de defectos significativos en su manufactura o en sus materiales, por el período legal que corresponda contado desde la fecha de entrega del producto conforme factura. La presente garantía no regirá cuando se trate de errores que pueden ser subsanados fácilmente y no implican afectación del rendimiento, cuando los defectos descubiertos hayan sido modificados o alterados sin consentimiento previo del fabricante o cuando el error provenga del mal uso o negligencia o defectos en la instalación. El reclamo deberá realizarse por escrito durante el período de garantía y dentro de los 7 siete días de la observación del defecto acompañado de prueba de los errores detallados. Cualquier producto que Ud. devuelva al fabricante o a un distribuidor autorizado de Macroseguridad deberá ser remitido con el envío y el seguro prepago.
4. **Incumplimiento de la Garantía** – Para el caso de incumplimiento de esta garantía, Macroseguridad Latino América podrá reemplazar o reparar, a discreción del fabricante y con cargo al adquirente /usuario, cualquiera de los productos involucrados.

CON EXCEPCION DE LO DISPUESTO EXPRESAMENTE EN EL PRESENTE, NO EXISTE NINGUNA OTRA GARANTIA O REPRESENTACIÓN DEL PRODUCTO, EXPRESA O IMPLÍCITA, INCLUYENDO, PERO NO LIMITADA A, CUALQUIER GARANTIA IMPLICITAS DE COMERCIALIZACIÓN Y/O ADAPTABILIDAD PARA UN PROPÓSITO PARTICULAR.

5. **Limitación de la Garantía del fabricante y/o Macroseguridad** – La responsabilidad total del fabricante frente a cualquier persona o causa, sea contractual como extracontractualmente, incluyendo negligencia o dolo, no podrá exceder el precio de la unidad de producto por Ud. pagado que ha causado el daño o resulta ser el objeto que directa o indirectamente se encuentra relacionado con el hecho dañoso. En ningún caso Macroseguridad Latino América o el fabricante serán responsabilizados por cualquier daño causado por un acto ajeno, impropio, o negligente en el uso del producto, o el incumplimiento de las obligaciones en el presente asumidas, así como tampoco, por la pérdida de cualquier información, dato, ganancia o ahorro, o cualquier otro daño consecuente o incidental, incluso si el fabricante y/o Macroseguridad Latino América hubiese sido advertido de la posibilidad de daño.
6. **TERMINACIÓN DEL ACUERDO DE LICENCIA**. El Acuerdo se considerará terminado frente al incumplimiento de los términos a su cargo. Al término de este contrato expirará la Licencia otorgada y deberá suspender todo uso posterior del Software, y borrar o eliminar cualquier información vinculada al mismo y de propiedad del fabricante. Los items 2, 3, 4 y 5 se mantendrán a pesar de la finalización del acuerdo.

1 Introducción

1.1 ¿Qué es un Token USB de Macroseguridad?

Los Tokens USB de Macroseguridad.org son dispositivos de autenticación de usuarios y portabilidad de certificados digitales, plug-and-play, ligeros, portátiles, pequeños, que proveen la mejor seguridad al menor costo y que se conectan al puerto USB (Universal Serial Bus) de cualquier PC. Para trabajar con los tokens USB no se requiere ninguna fuente de energía adicional, ni se requiere lectora, ni ningún otro tipo de dispositivo.

1.2 ¿Para qué sirve un Token USB de Macroseguridad?

Es la solución para poder transportar su identidad digital que le permite al usuario almacenar su certificado digital en un dispositivo físico (Smartcard USB) altamente seguro. De esta forma sus credenciales pueden ser transportadas de una PC a otra sin perder la seguridad, integridad y confiabilidad que Macroseguridad.org le brinda a través de su mecanismo de autenticación de doble factor o triple factor: algo que tengo físicamente, un “Token USB de Macroseguridad”, algo que conozco que es “la password del Token” y quien soy (ADN, Iris, Biometría, etc) que brinda el tercer factor de autenticación.

2 Antes de Comenzar

2.1 Sistemas operativos soportados

Actualmente **ePass2003** soporta las siguientes plataformas:

- macOS
- Windows 10
- Windows 8.1
- Windows 8
- Windows 7
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012
- Windows Server 2008
- Linux

Las capturas de esta guía de instalación se realizaron en macOS HighSierra y con Adobe Acrobat Reader DC versión 2020.012.20048.

2.2 Requisitos mínimos para la configuración

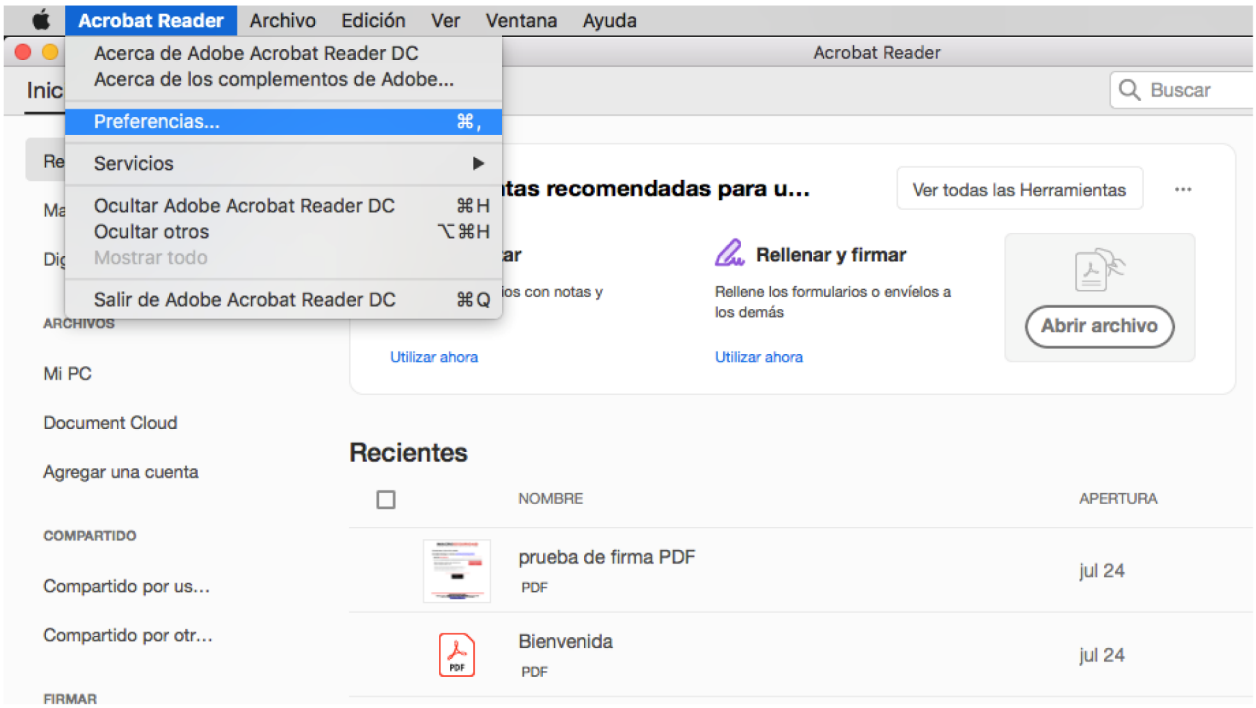
Antes de comenzar con la configuración deberá verificar que los siguientes requisitos se cumplan:

- El sistema operativo debe ser macOs Sierra o superior.
- Tener instalado Adobe Acrobat Reader.DC versión 2020.012.20048 o superior
- Tener instalado los drivers ***MSePass2003_Mac_Spanish_V1.1.20.1103*** o superior
- Permisos de Administrador.
- Un puerto USB disponible.
- Un dispositivo criptográfico de Macroseguridad.org listo para usar.
- Debe estar habilitado en el MotherBoard el soporte USB.

3 Configuración del dispositivo ePass2003 en Acrobat Reader

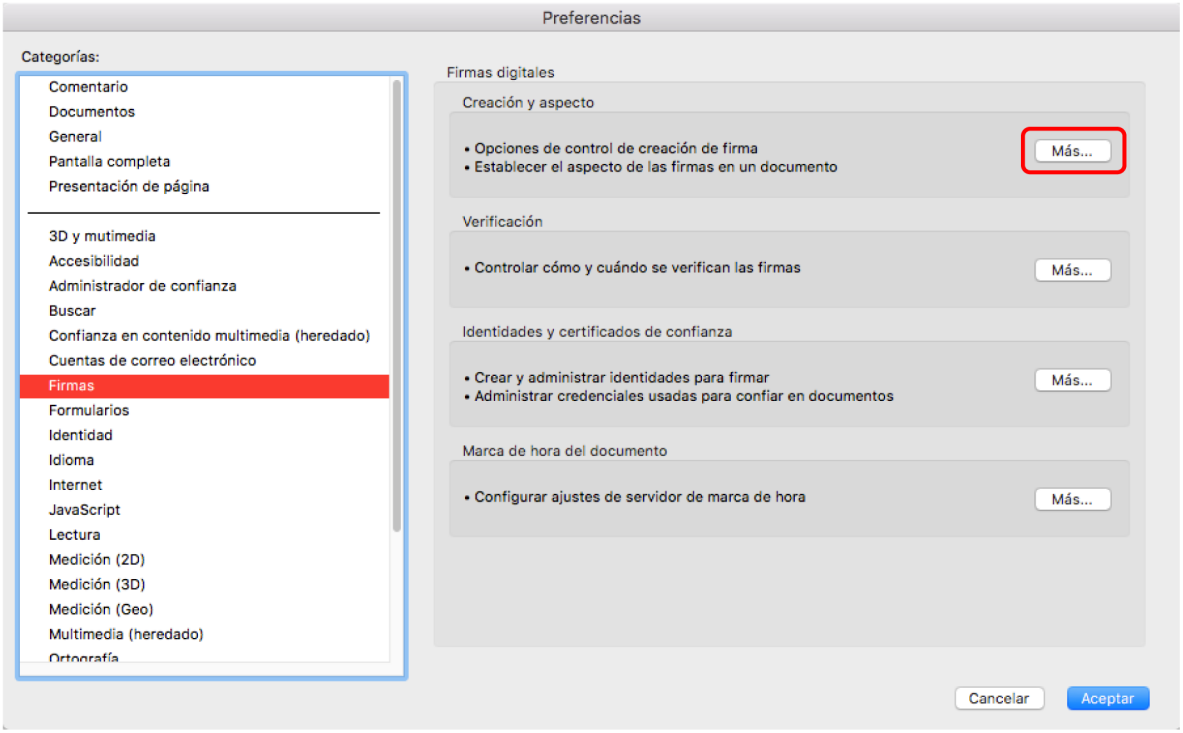
1) Inicie la herramienta Adobe Acrobat Reader DC en su Mac.

2) Haga click en el menú superior en “Acrobat Reader” y del menú desplegado seleccione la opción *“Preferencias…”*.

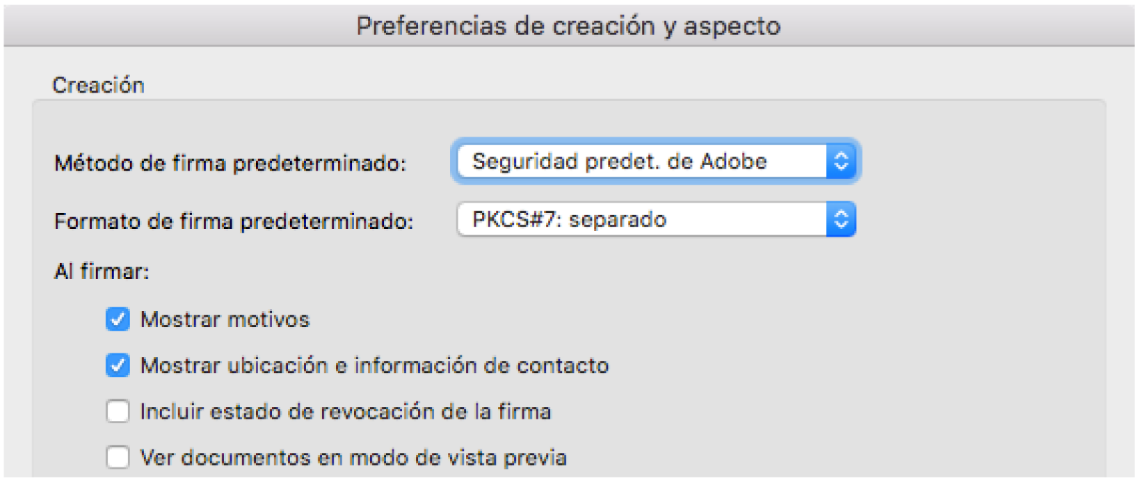


3) Se le desplegará una ventana donde en la columna situada a la izquierda llamada *“Categorías”* deberá seleccionar la opción *“Firmas”*.

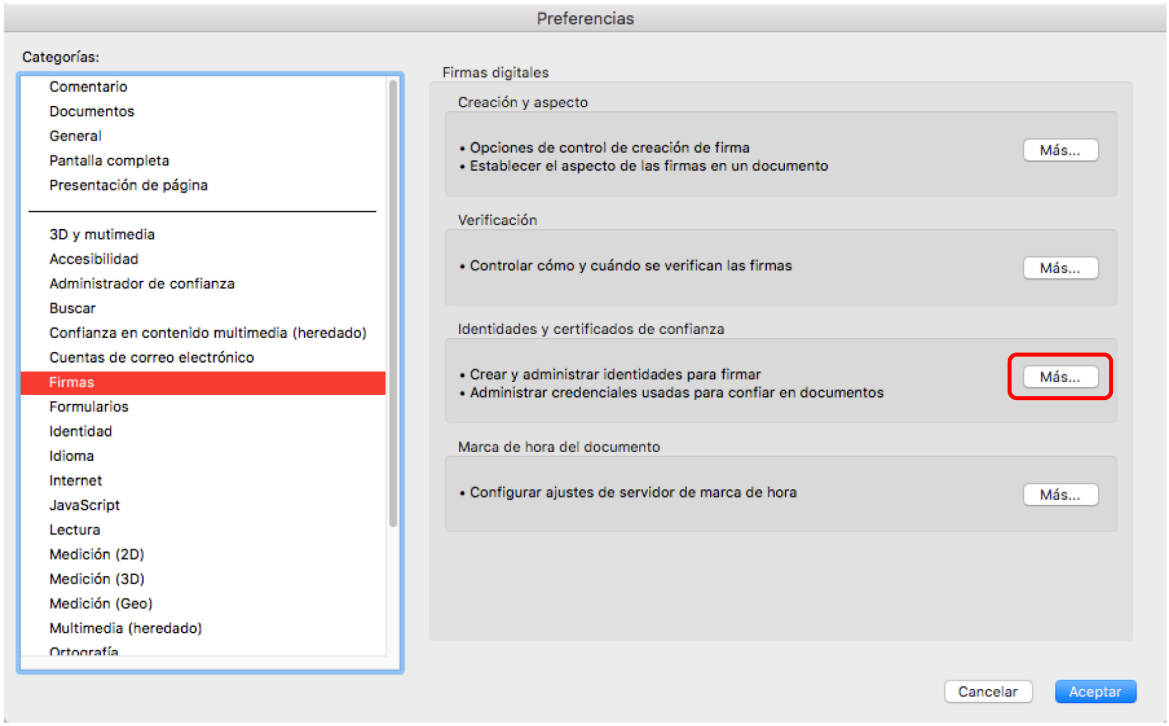
4) Luego, en la opción “Creación y aspecto” haga click en el botón “Más…”



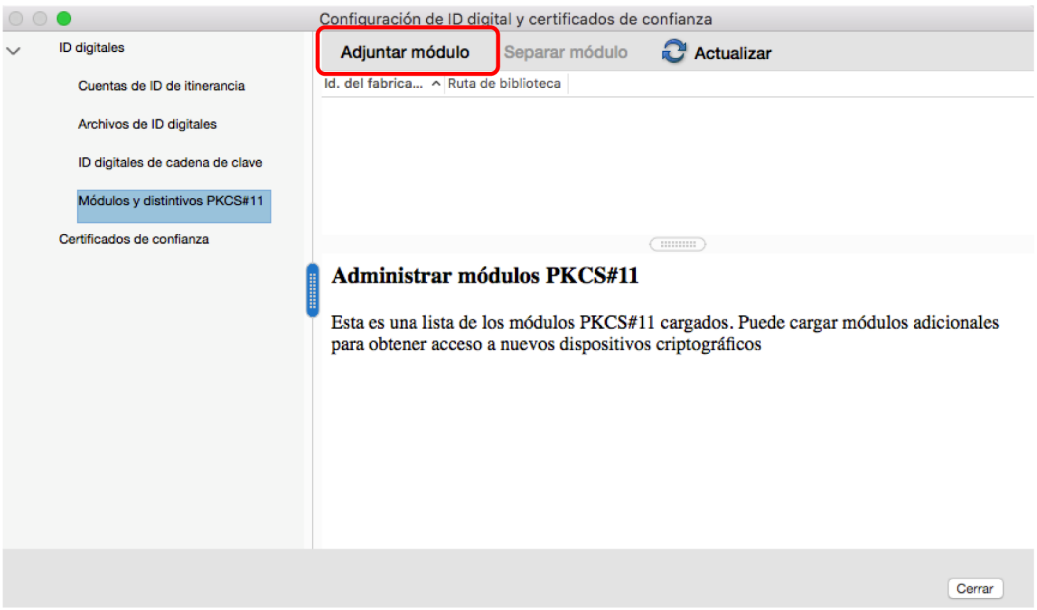
5) Dentro de la ventana de “Preferencias de creación y aspecto”. Seleccione las opciones como se detalla a continuación. Luego haga click en “Aceptar”



6) Luego al volver a la ventana de “Preferencias”, en la opción *“Identidades y certificados de confianza”* haga click en el botón *“Más…”*

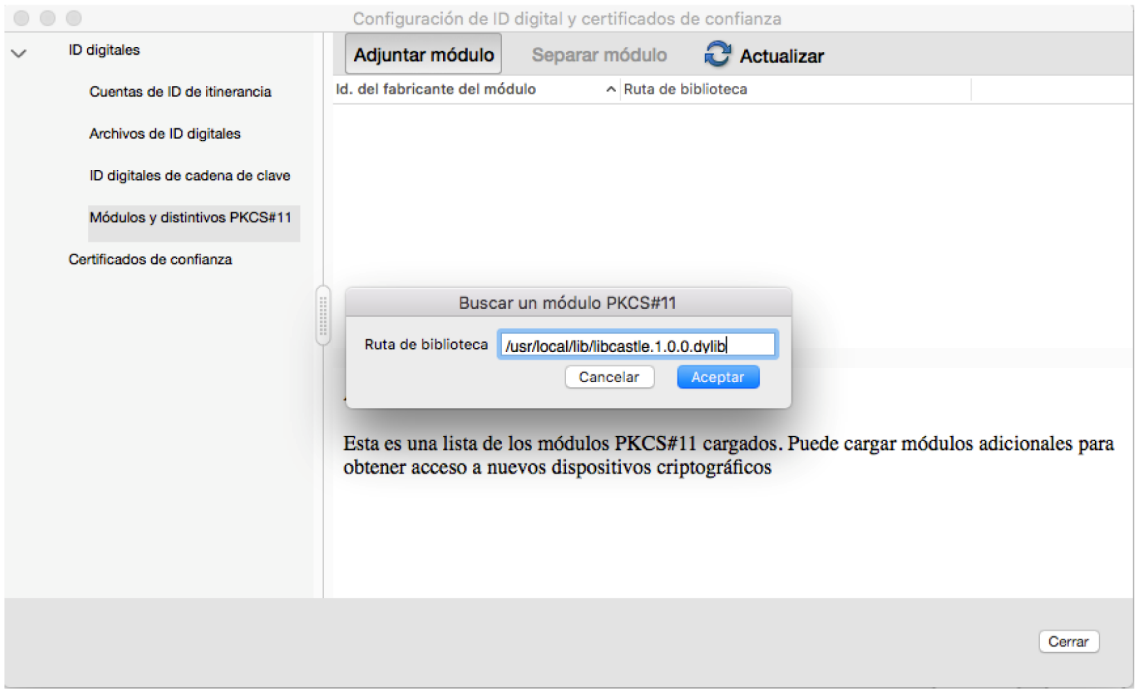


7) En la ventana *“Configuración de ID digital y certificados de confianza”*, deberá seleccionar la opción *“Módulos y distintivos PKCS#11”* que se encuentra a la izquierda de la ventana y luego en *“Adjuntar módulo”*.

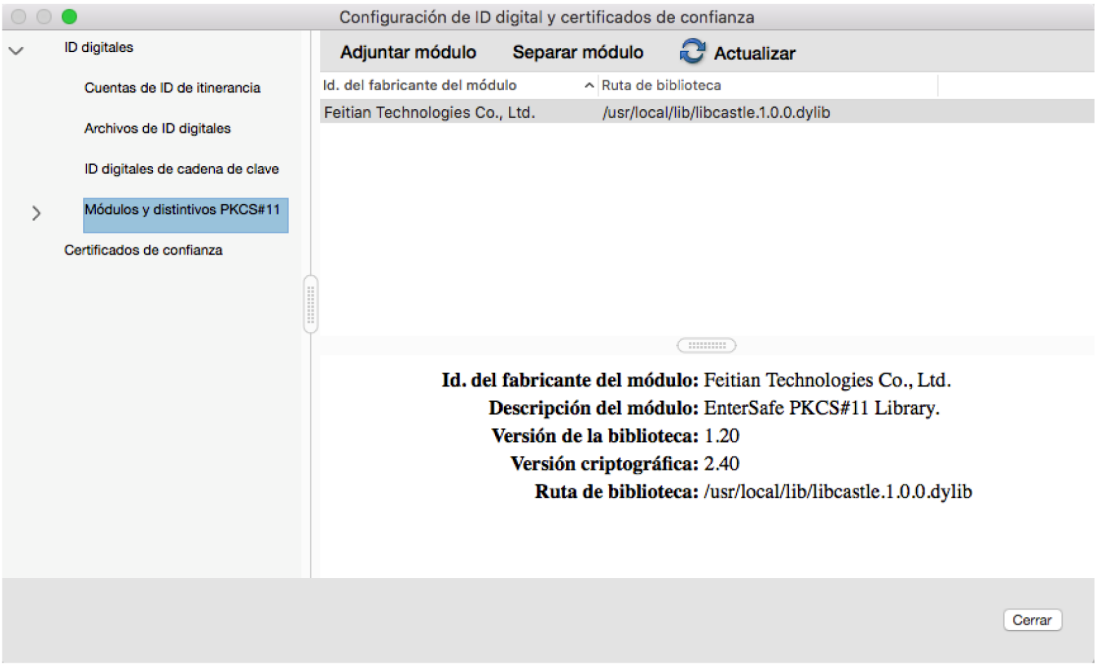


Sobre la ventana que le aparece, llamada *"Buscar un módulo PKCS#11",* deberá pegar la ruta a la librería PKCS#11 del dispositivo provisto por Macroseguridad.org ***ePass2003*** y luego haga click en *"Aceptar"*.

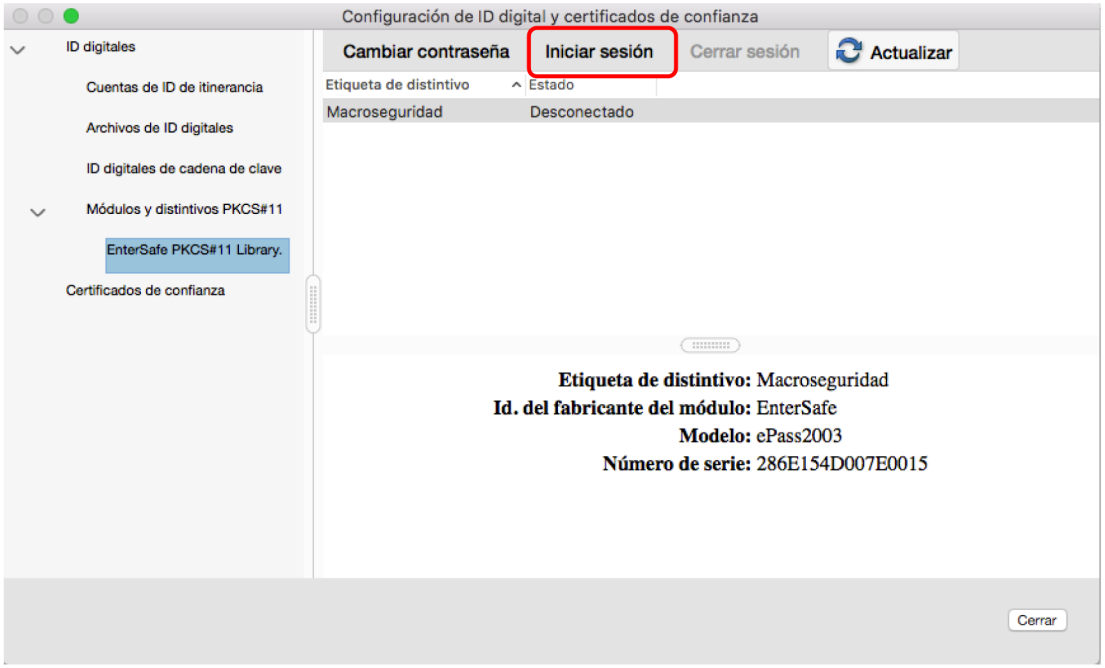
La ruta será *"**/usr/local/lib/libcastle.1.0.0.dylib**"*



8) Luego de cargar el módulo, podrá visualizarlo en la lista izquierda como *"EnterSafe PKCS#11 Library"*

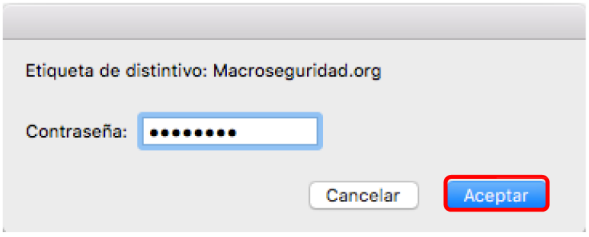


9) Luego de hacer click en *"EnterSafe PKCS#11 Library"*, con el dispositivo provisto por Macroseguridad.org ***ePass2003*** conectado, deberá hacer click en *"Iniciar sesión"*.

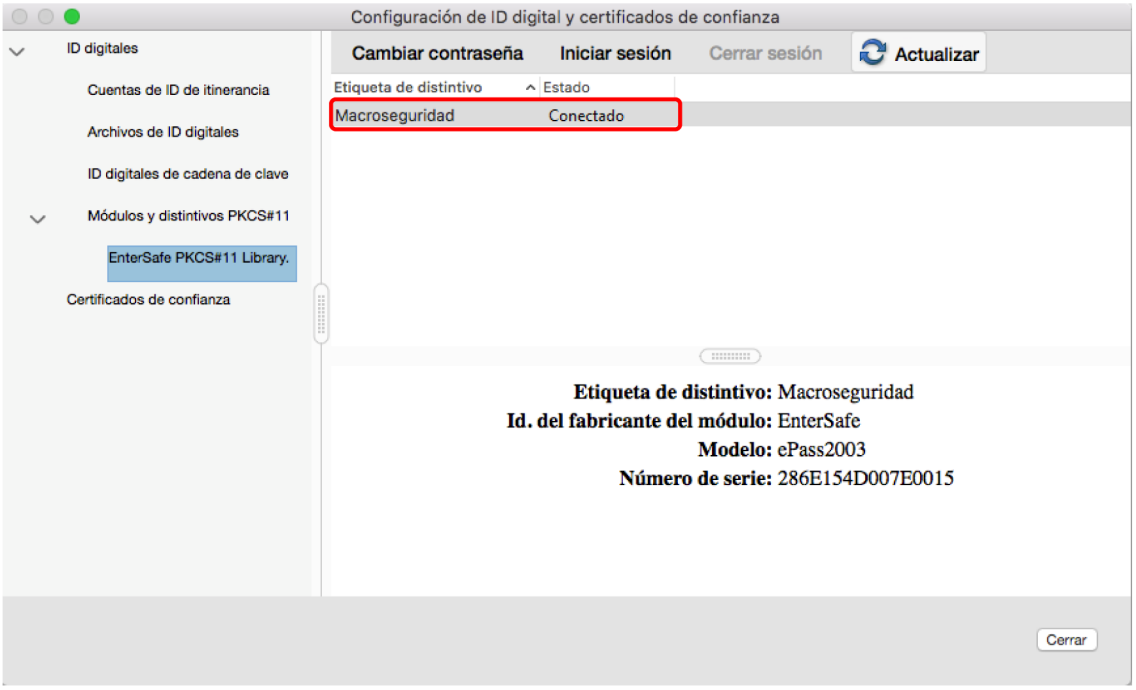


Le pedirá ingresar el PIN de Usuario como se visualiza en la imagen inferior.

Recuerde que el PIN de Usuario es la password que Ud. utiliza para todas las operaciones de firma con su Token USB.



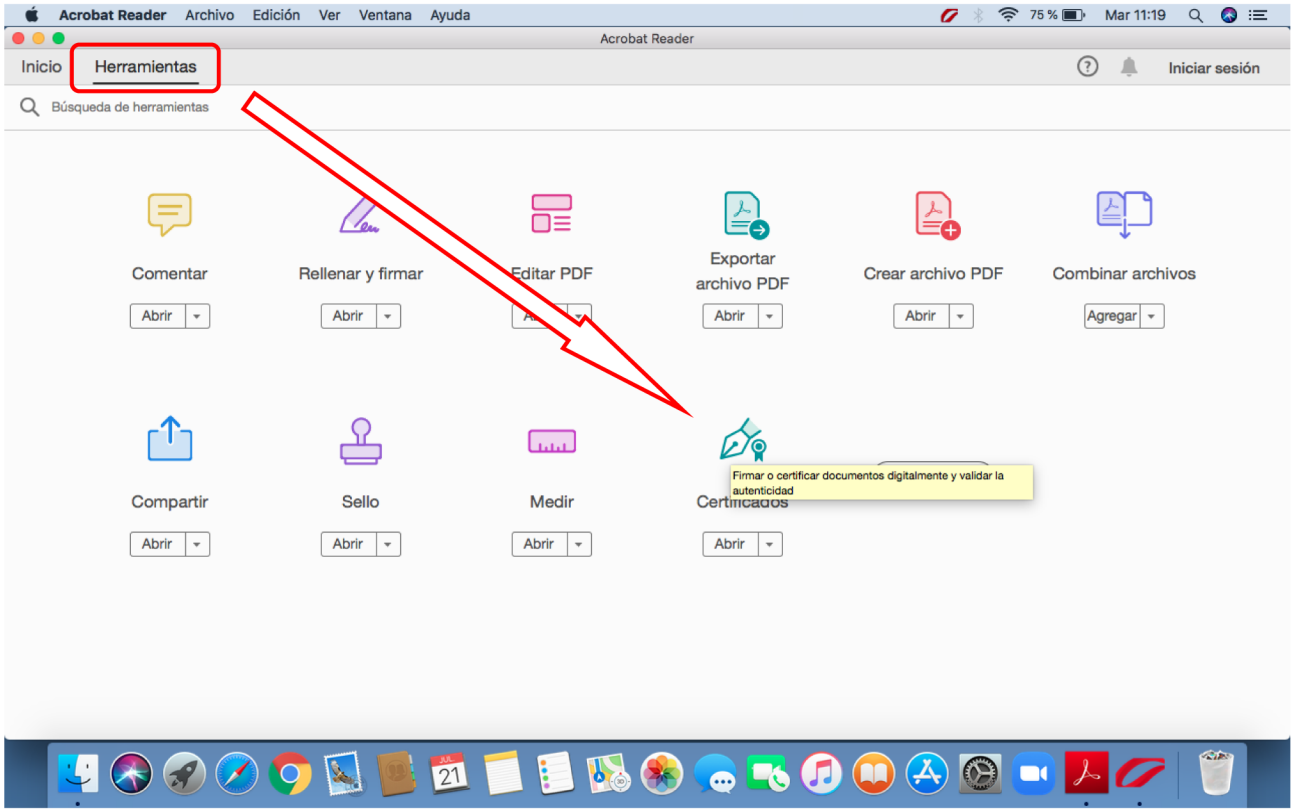
10) Luego de ingresar su PIN de Usuario y hacer click en *"Aceptar"* podrá visualizar el dispositivo con el mensaje *"Conectado"*.



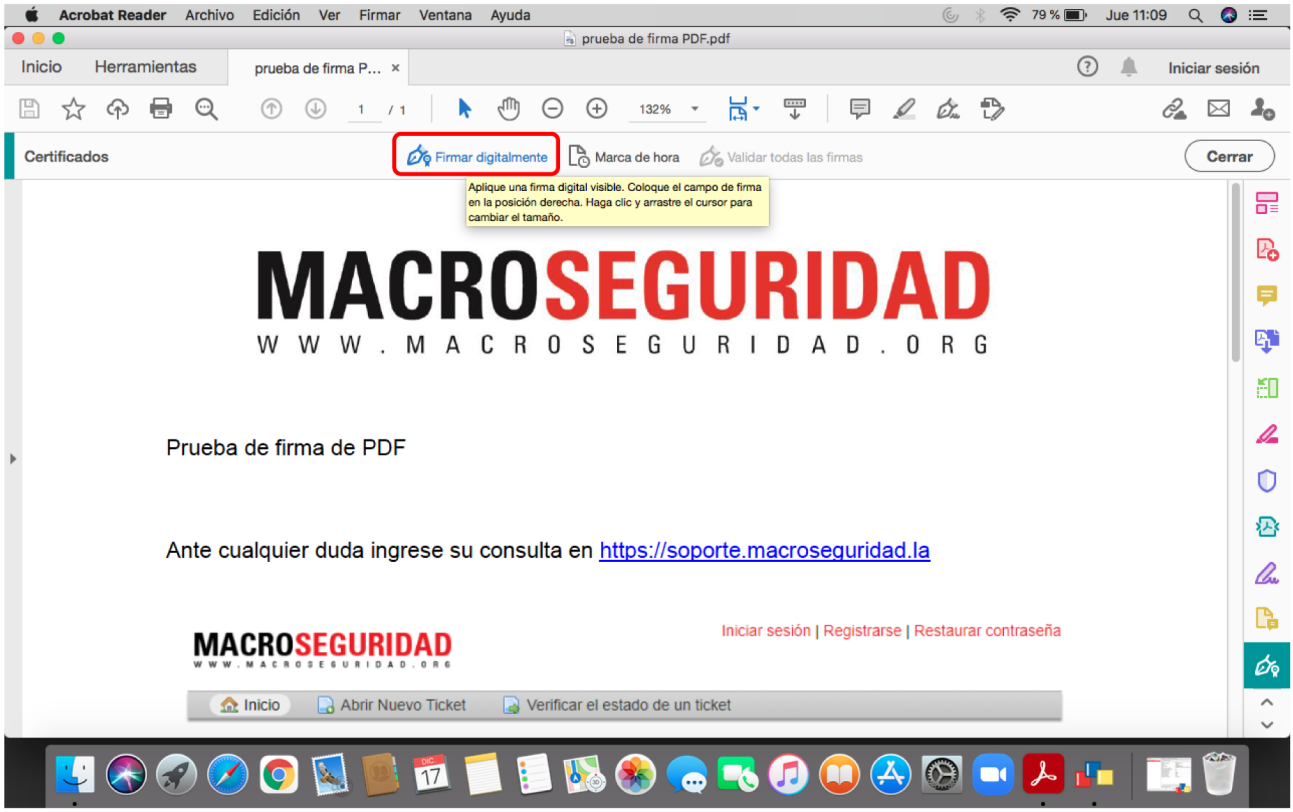
11) Teniendo el dispositivo de Macroseguridad.org **ePass2003** conectado en Adobe Acrobat Reader DC, ya puede firmar digitalmente un documento PDF con el certificado que posee almacenado en su dispositivo Token.

4 Firmar digitalmente un documento PDF con Acrobat Adobe Reader DC y un ePass2003 de Macroseguridad.

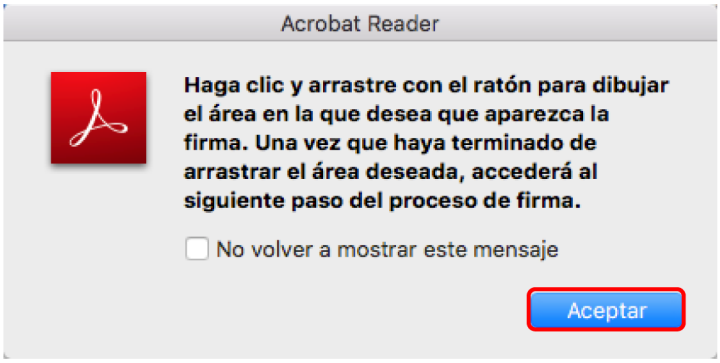
Luego de realizar los pasos anteriores, diríjase al menú *"Herramientas"* y luego haga click en el ícono *"Certificados"*.



Le mostrará sobre su documento una barra donde deberá hacer click en *"Firmar digitalmente"*.

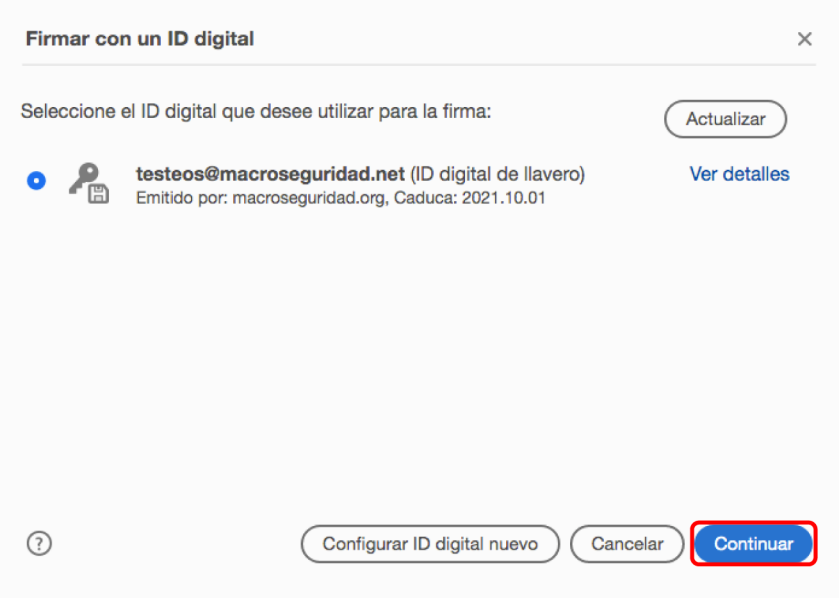


Luego de hacer click, seleccione el área donde quiere ubicar su firma digital sobre el documento PDF manteniendo el click hasta que se forme un rectángulo del tamaño deseado como indica el mensaje.



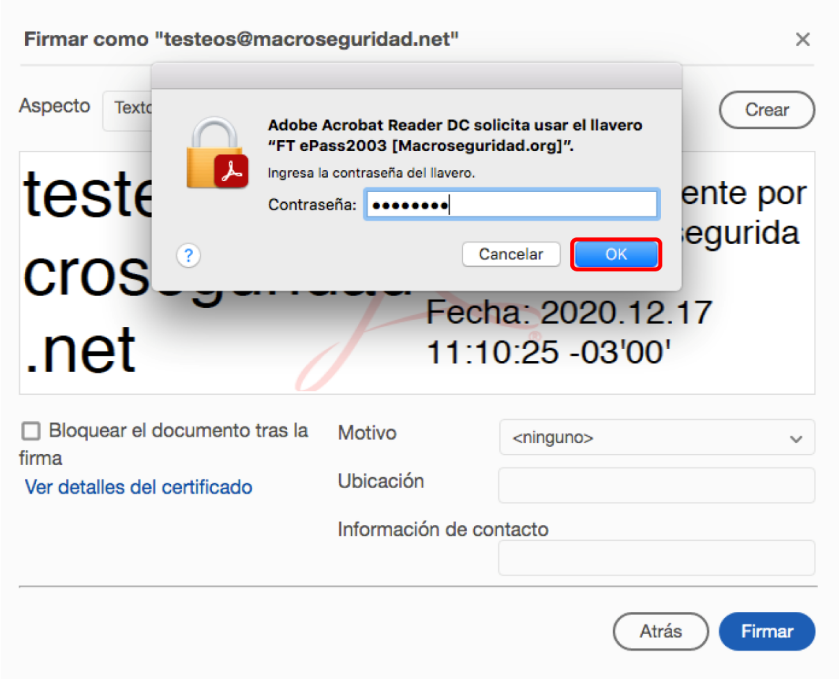
Al dibujar el rectángulo deberá visualizarlo de la siguiente manera:

A continuación luego de soltar el click, se le desplegará una ventana donde deberá elegir su certificado con el cual firmará este documento, seleccione el certificado y luego haga click en *"Continuar"*.

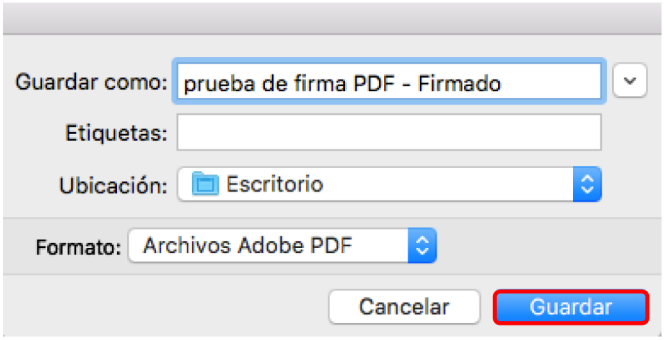


En la siguiente ventana se visualizará la información de firma como la fecha y hora de firma que Ud. puede personalizar, si así lo desea, agregando mas datos como su nombre o el motivo de firma. Para firmar el documento haga click en *"Firmar"*.

Le solicitará el PIN de Usuario de su dispositivo ePass2003. Ingréselo y luego haga click en *"OK"*



Realizada la firma le solicitará guardar este documento. En este paso puede, si Ud. lo desea, cambiar el nombre del archivo y la ubicación del mismo. Para continuar haga click en *"Guardar"*.



Al finalizar, en el rectángulo seleccionado anteriormente verá su firma. Además sobre el archivo, se leerá un mensaje *"Firmado y todas las firmas son válidas"* indicando que la firma fue correcta y el certificado utilizado, es de confianza.

Nota: De informarle un mensaje que el documento tiene firmas desconocidas, esto sucede porqué no se instaló el certificado Raíz de modo que no puede validarse su firma.

Para ver una guía sobre cómo instalar este certificado en un navegador Web en su PC ingrese en:

https://www.macroseguridad.net/confianza

5 Integraciones y aplicaciones de los Tokens USB / Smartcards de Macroseguridad

Macroseguridad.org ha desarrollado varias guías de integración para utilizar sus dispositivos criptográficos con las aplicaciones de uso común. Los Tokens USB y SmartCards le permiten robustecer la seguridad de dichas aplicaciones de modo totalmente transparente. Si desea conocer mayor información al respecto de estas guías puede visitar:

https://www.macroseguridad.net/documentacion

Para mayor información o dudas sobre esta guía contacte al equipo de tecnología de Macroseguridad.org por el medio que usted prefiera:

- ☞ Mail: soporte@macroseguridad.net
- ☞ Portal de soporte: https://soporte.macroseguridad.la
- ☞ Web: www.macroseguridad.net