BioPass 3000

Guía de Referencia PKI
BioPass Token USB

MacroSeguridad Latino América

Versión 1.2 Español BioPass

Abril de 2008

Acerca de MacroSeguridad Latino América

MacroSeguridad es un Mayorista exclusivo de Soluciones de Seguridad Informática. Es líder en seguridad digital, proveyendo seguridad para comercio electrónico e Internet desde 1994. MacroSeguridad atiende a clientes en toda Latino América, México, Brasil y Australia.

Los productos que MacroSeguridad distribuye incluyen: los dispositivos **ePass Token USB** para autenticación segura de usuarios, portabilidad, transporte de certificados digitales, y no repudio en comercio electrónico. Entre los mismos se pueden encontrar **ePass1000**, **ePass1000ND**, **ePass Token USB FT1**, **ePass Token USB FT12**, **ePass3000**, **BioPass Token USB**. Los sistemas de protección de software profesional basado en dongles que protegen la propiedad intelectual y los modos de licenciamiento de los desarrolladores como ser **Rockey2**, **Rockey4**, **Rockey4ND** y **Rockey6**. Soluciones para encriptado de discos, solución para loguearse a la red en forma segura. También se provee seguridad para SAP, como ser de criptografía, logon y autenticación robusta. Así como también soluciones de **OTP Tokens** (dispositivos generadores de números aleatorios) para aplicaciones de homebanking y de dispositivos token USB llamados **mIDentity** para portabilidad de la identidad digital de la empresa **KOBIL**, autenticación robusta para PDA y mobile phones.

Macroseguridad Latino América logra el equilibrio entre las necesidades de las empresas y sus soluciones. Para más información puede visitar el sitio web de MacroSeguridad en:

www.MacroSeguridad.org

Información de contacto

Por cualquier consulta, sugerencia o comentario que le surja sobre la utilización del ePass Token USB ó de esta guía en si misma, por favor contacte al soporte técnico de MacroSeguridad Latino América:

- Mail: **soporte@macroseguridad.net**
- TEL: +54 011 4833-5760 (Líneas Rotativas)
- FAX: +54 011 4831-6538
- Web: **www.MacroSeguridad.org**

Copyright y Marcas Registradas

Histórico de Versiones

Fecha	Versión	Descripción
December de 2006	1.0	1a. Edición (Inglés)
Mayo de 2007	1.1	Edición Portugués
Abril 2008	1.2	Edición Castellano

Acuerdo de Licencia

FEITIAN TECHNOLOGIES CO. LTD.

Todos los Productos de Feitian Technologies Ltd. (Feitian), 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. Si Ud. no está de acuerdo con los términos aquí incluidos, por favor devuélvanos el paquete de evaluación, empaque y contenido prepago, dentro de los siete días de su recepción, y le reembolsaremos a Ud. el precio del producto, con menos los gastos de envío y cargos razonablemente incurridos.

1. **Uso Permitido** – Ud. puede utilizar este Software con el único propósito de proteger las comunicaciones, firmar documentos, firmar/encriptar emails o encriptar archivos como se describe en esta Guía de Regencia PKI con la licencia de ePass. Puede hacer copias de archivo de este software. Ud. puede fusionar y conectar el Software con otros programas, de manera concordante con los usos descriptos en la Guía para Desarrolladores y de Referencia del ePass2000 Token USB. Ud. puede hacer copias de archivo del Software.

2. **Uso Prohibido** – El Software o Hardware o cualquier otra parte del producto no puede ser copiada, realizada reingeniería, desensamblada, descompilado, revisado, mejorado y/o modificado de alguna 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 Producto ni intentar descubrir el código fuente del Software. No puede utilizarse el dispositivo magnético u óptico incluido en el Producto con el propósito de transferir o almacenar datos que no integren una parte original del Producto o una mejora provista en el Producto por MacroSeguridad Latino América o Feitian.

3. **Garantía** – Feitian garantiza que el hardware y Software del medio de almacenaje está sustancialmente libre de defectos significativos en su fabricación o en sus materiales, por un período de doce meses contados desde la fecha de entrega del Producto a Ud.

4. **Incumplimiento de la Garantía** – Para el caso de incumplimiento de esta garantía, la única obligación de Feitian y/o Macroseguridad Latino América será la de reemplazar o reparar, a discreción de Feitian, cualquiera de los productos libre de cargos. Cualquiera de los productos reemplazados deviene de propiedad de Feitian.

   El reclamo de la garantía deberá ser realizado por escrito a Feitian o Macroseguridad Latino América mientras dure el período de garantía y dentro de los catorce (14) días posteriores de observado el defecto. Todos los reclamos de garantía deberán ser acompañados por evidencia del defecto que sea considerado satisfactorio a criterio de Feitian y/o Macroseguridad Latino América. Cualquier

producto que Ud. devuelva a Feitian o un distribuidor autorizado de Feitian deberá ser remitido con el envío y el seguro prepago.

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 de Feitian** – La responsabilidad total de Feitian 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 Feitian y/o Macroseguridad Latino América será responsabilizado por cualquier daño causado por un acto ajeno en el uso del producto, o el incumplimiento de las obligaciones en el presente asumidas, así como tampoco, por la pérdida de cualquier información, ganancia o ahorro, o cualquier otro daño consecuente o incidental, incluso si Feitian y/o Macroseguridad Latino América hubiese sido advertido de la posibilidad de daño, o de cualquier reclamo basado en cualquier reclamo de terceros.

6. **Finalización** – El acuerdo se considerará terminado frente al incumplimiento de los términos a su cargo. Los ítems 2, 3, 4 y 5 se mantendrán a pesar de la finalización del acuerdo.

Certificaciones y Estándares

- **Certificado de Aprobación FCC**

ePass Token USB ha sido probado y es compatible con límites para un dispositivo digital de clase B, de acuerdo a la sección 15 de las normativas FCC. Estos límites están diseñados para asegurar una protección razonable contra interferencias dañinas que pueden ocurrir en una instalación.

- **CE Compatible**

ePass Token USB cumple con los requerimientos primordiales para la Directiva EMC (directiva 89/336/EEC respecto a la compatibilidad electromagnética) basado en una prueba voluntaria.

Esta declaración se aplica solo a las muestras particulares del producto y a la documentación técnica provista para el testeo y certificación. El detalle de los resultados de las pruebas y todos los estándares usados, así como el modo de operación se encuentran listados en:

Reporte de Pruebas Nº: 70407310011
Estándares de Prueba: EN 55022/1998 EN 55024/1998

Posteriormente a la preparación de la documentación técnica necesaria y de la declaración de conformidad, el logo de CE mostrado puede ser incluido en el equipo, como se establece en el Artículo 10.1 de la Directiva.

- **USB**

Este equipo está basado en el estándar USB

- **Microsoft Windows Logo Program**

Este dispositivo ha superado las pruebas de Windows HCT, realizadas en los Laboratorios de Pruebas de Hardware de Windows (WHQL), las cuales determinan los productos que alcanzan los requerimientos del Programa de Logos de Windows

Compatibilidad de Hardware de Windows Vista:

Compatibilidad de Hardware de Windows XP:

- **CheckPoint OPSEC Partner**

ePass2000 ha alcanzado la certificación OPSEC (Open Platform for Security) de Check Point Software Technologies Ltd. (NASDAQ: CHKP), el líder mundial en seguridad a través de Internet. A través de la certificación OPSEC, ePass2000 se integra transparentemente con las soluciones de Check Point líderes del mercado: VPN-1®, FireWall-1® y Next-Generation®.

- **Entrust Ready Partner**

Los Tokens de seguridad de FeiTian son tokens criptográficos seguros y portátiles, ideal para Entrust/PKI y otras aplicaciones Smart Card: autenticación por dos factores, encripción de email, sitios seguros SSL, logon VPN y más. Se le ha otorgado a ePass el estado de Entrust Ready con el Entrust Entelligence client y Entrust Authority Securtity Manager.

- **ISO 9001:2000**

FeiTian Technologies LTD. es una compañía certificada ISO 9001:2000

- **RoHS (Restriction of the use of certain Hazardous Substances)**

Los dispositivos ePass Token cumplen con las directivas de la Unión Europea de cuidado del medio ambiente y de la salud humana estipuladas por RoHS, restringiendo el uso de sustancia como Plomo (Pb), Cadmio (Cd), Mercurio (Hg), Cromo hexavalente (Cr (VI)), Bifenil polibrominado (PBB), Éter bifenil polibrominado (PBDE).

- **<u>WEEE (Waste Electrical and Electronic - Descarte de Equipos Eléctricos y Electrónicos)</u>**

Este equipo se debe desechar por separado

La directiva Europea 2002/96/CE exige que el equipo que muestra este símbolo en el producto y/o su embalaje no sea desechado junto con los residuos municipales. El símbolo indica que este producto debe ser desechado por separado de los residuos domésticos regulares. Es su responsabilidad desechar este y cualquier otro equipo eléctrico y electrónico a través de los puestos de recolección designados por las autoridades gubernamentales o locales. La eliminación y el reciclaje correcto ayudarán a prevenir las consecuencias negativas para el medio ambiente y la salud humana. Para obtener información mas detallada sobre la forma de desechar su viejo equipo, contáctese con las autoridades locales, servicios de recolección de residuos o el establecimiento comercial donde adquirió el producto.

Índice

1 Visión General

El BioPass 3000 token USB, es el estado del arte en autenticación de usuarios y portabilidad de certificados ya que provee el método de autenticación más reconocido a nivel mundial.

1.1 Autenticación Robusta de Usuarios - ¿Qué es?

Existen varios métodos para lograr autenticar a un usuario en forma efectiva.

Lamentablemente eso solo no alcanza, ya que para que el usuario además pueda probar su identidad en forma univoca, debemos agregar otro concepto muy diferente a la autenticación. El concepto es poder probar "*quien realmente es*", Identificando al usuario.

¿Qué entendemos por una robusta autenticación de usuarios? es un proceso que se basa en al menos 2 factores, incrementando considerablemente la seguridad y a su vez logrando reducir significativamente los costos asociados a la utilización de passwords,

1.2 Conceptos y Factores de Autenticación

Los métodos y conceptos más difundidos de autenticación los podemos expresar en el detalle que se muestra a continuación:

- **Algo que conocemos** - Información confidencial como por ejemplo el PIN o una password
- **Algo que poseemos** – un dispositivo físico, por ejemplo un **ePass Token USB**
- **Algo que somos** – una característica biológica, como ser su huella dactilar o el escaneo de iris. Esto marca indefectiblemente la Identificación univoca de la persona

Una de las formas por la cual se identifica fehacientemente a una persona y podríamos decir que es una de las mas ampliamente aceptada, es a través de las huellas dactilares que son únicas e irrepetibles.

El **BioPass 3000** token USB es la única solución que se provee con la interfaz de usuario totalmente en castellano y a su vez genera una autenticación univoca de la persona a través de las huellas dactilares. Con lo cual se garantiza la identidad de la persona al momento utilizar el certificado digital como por ejemplo para firmar correo, firmar un PDF, o abrir una VPN o el acceso a un homebanking o servicios para banca empresas.

El BioPass almacena las huellas dentro de si mismo en forma encriptada “identificando” al usuario, haciendo totalmente seguro el proceso de validación en si mismo.

Hasta hoy se debía ingresar un PIN de acceso sobre el teclado para ganar acceso cualquier dispositivo token USB. La posibilidad que da el **BioPass 3000** token USB es **reemplazar ese PIN por las huellas dactilares del usuario** y acceder a una solución realmente segura.

> *“El BioPass Token USB, marca una revolución en las soluciones de portabilidad de certificados y autenticación, ya que el propio producto no solo autentica sino IDENTIFICA fehacientemente al usuario”.*

2 Utilizando el Administrador PKI del BioPass3000

Este capítulo tratará los siguientes tópicos:

- Requisitos previos
- Visión General
- Administrador de Huellas Dactilares
- Login
- Administrador de Certificados
- Opciones de Sistema
- Cambiar el nombre del BioPass Token

2.1 Requisitos Previos

Debe haber instalado correctamente el Middleware del BioPass3000 (drivers y aplicativos) en su PC antes de intentar hacer uso del Administrador PKI de BioPass para tener acceso al Token USB.

Podrá obtener mayor información sobre como instalar el middleware de BioPass Token USB accediendo a la Guía de Instalación de BioPass, en el siguiente vínculo:

www.macroseguridad.net/download/ePass

El dispositivo debe ser inicializado en formato PKI antes de ser usado. Los productos comúnmente ya salen de fábrica con la inicialización realizada (antes del envío por parte de MacroSeguridad Latino América). Pero si su dispositivo no fuese reconocido, usted deberá formatearlo utilizando la herramienta que se encuentra dentro del CD-ROM del SDK del BioPass. Para mayor información acerca del uso de esta herramienta lo invitamos a que contacte al departamento de tecnología de MacroSeguridad vía mail a **soporte@macroseguridad.net** o bien desde nuestra página web:

www.macroseguridad.net/soporte/ePass

Si Ud. simplemente estuviese recibiendo el BioPass 3000 Token como un usuario, deberá contactarse con su administrador o responsable de sistemas.

2.2 Interface Antes de Conectar el BioPass Token

El "*BioPass 3000 – Administrador PKI*" podrá ser encontrado en "Inicio" → "Programas" → "MacroSeguridad.org" → "BioPass". Haga click en el icono para iniciar el Administrador de Certificados. Se mostrará la siguiente ventana:

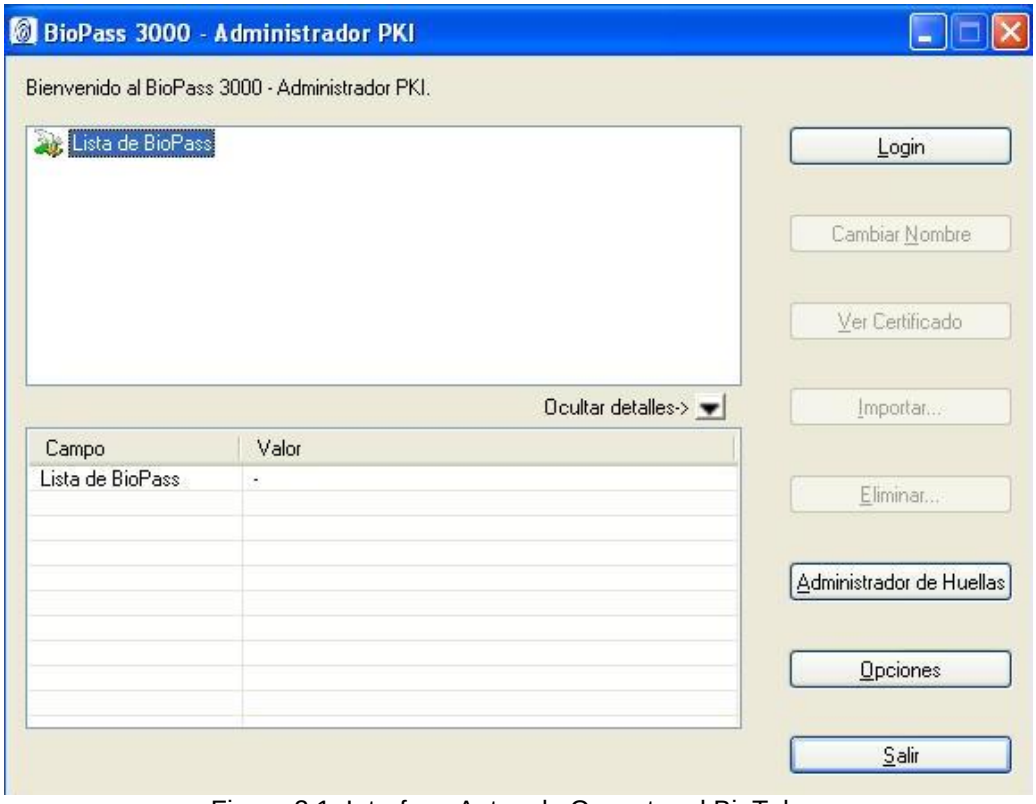


Figura 2.1. Interface Antes de Conectar el BioToken

2.2.2 Interface Luego de la Conexión del Token

En nuestro ejemplo, conectamos un dispositivo criptográfico llamado "BioPass3000" en uno de los puertos USB disponibles de la PC. El "*BioPass 3000 - Administrador PKI*" reconocerá la información básica del BioPass automáticamente.

La interface tendrá la siguiente apariencia:

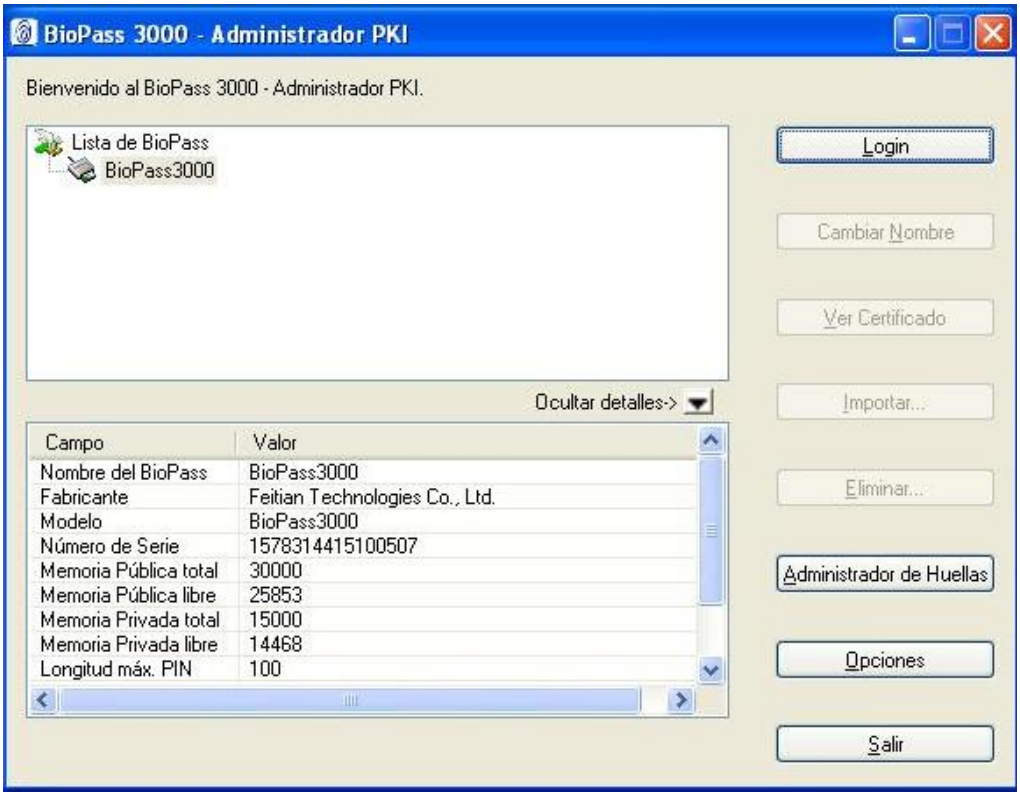


Figura 2.2. Interface luego de la Conexión del BioPass Token

2.3 Administrador de Huellas Dactilares

Haga click en el botón "*Administrador de Huellas*" para abrir la ventana del Administrador de Huellas Dactilares.

En la ventana, existen cinco opciones:

"Verificar",
"Registrar",
"Actualizar",
"Eliminar" y
"Salir".

La interface principal se muestra a continuación:

Figura 2.3. Ventana Administrador de Huellas

Cuando usted posiciona el puntero del mouse sobre cada botón, se mostrará al pie de la ventana una pequeña descripción acerca de la función que realiza ese botón en particular.

2.3.2 Verificando una Huella Dactilar

Usted debe registrar por lo menos una huella dactilar antes de realizar la verificación. Este procedimiento de verificación es la forma de acceder a los datos almacenados en forma segura en el dispositivo. El procedimiento de verificación se detalla a continuación:

Haga click en el botón "*Verificar*" de la ventana Administrador de Huellas Dactilares. Aparecerá la ventana "*Verificar Huella"*.

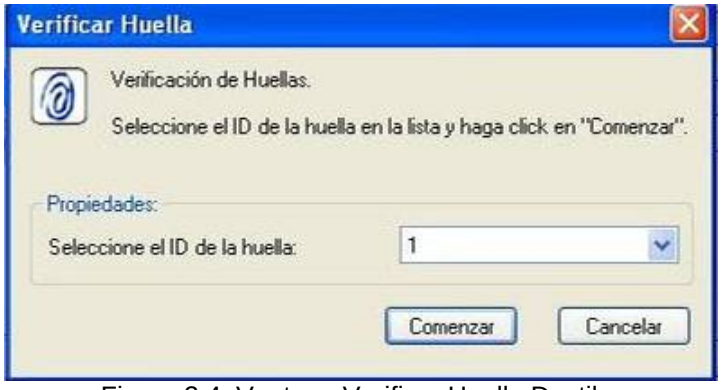


Figura 2.4. Ventana Verificar Huella Dactilar

Si usted todavía no registró ninguna huella dactilar, se le mostrará un mensaje informando que usted debe registrar por lo menos una huella dactilar para poder trabajar con la herramienta.

Figura 2.5. Ventana notificando que ninguna huella dactilar está registrada en el BioPass

Seleccione un ID en la lista (este ID es un número que es usado para asociar su huella con un identificador único, este puede luego ser usado para eliminar una huella dactilar en particular o volver a escanearla) y luego haga click en "*Comenzar*".

Cuando la ventana "*Verificar Huella*" aparezca, deberá deslizar su huella dactilar sobre el lector.

Figura 2.6. Ventana Verificar Huella Dactilar

Si usted ha realizado una verificación exitosa de una huella dactilar se desplegará una ventana como la que se muestra a continuación. Haga click en el botón “Aceptar” para poder loguearse al BioPass 3000 Token.

Figura 2.7. Verificación exitosa

2.3.3 Registrando Huellas Dactilares

Antes de registrar una nueva huella dactilar dentro del BioPass, debe autenticarse al dispositivo verificando alguna de sus huellas dactilares previamente registradas, o verificando la clave inicial del dispositivo (la misma es “**12345678**”) si aún no ha registrado ninguna.

El procedimiento para registrar una huella dactilar es el siguiente:

Haga click en el botón “*Registrar*” de la ventana del Administrador de Huellas Dactilares.

Si ésta fuese la primera vez que usted está registrando una huella dactilar, no tiene ninguna huella registrada, se le solicitará que se autentique con la "*password inicial*" del BioPass 3000 token USB que se provee de fabrica antes de registrar una huella.

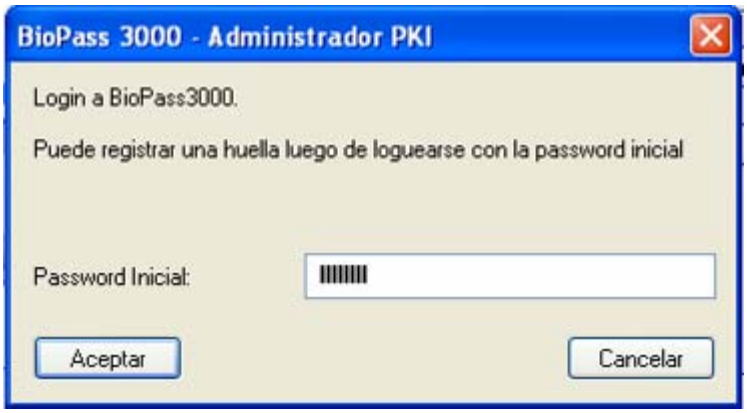


Figura 2.8. Ventana para ingresar la password inicial

Por defecto, esta password inicial es "**12345678**" y para continuar, usted debe digitar la contraseña inicial correctamente. Luego que una huella dactilar sea registrada con éxito, la contraseña inicial nunca más será válida, y usted deberá autenticarse únicamente con alguna de las huellas dactilares registradas en el dispositivo.

Luego de informar la password inicial correcta, haga clic en "*Aceptar*" para abrir la ventana "*Registrar Huella*" Dactilar. Si esta no fuese la primera vez que usted registra una huella, haciendo click en "*Registrar*" usted ira directamente a la ventana Registrar Huella Dactilar.

Figura 2.9. Ventana Registrar Huella Dactilar

Usted deberá seleccionar un ID (de los 8) disponible de la lista, como también especificar el nivel de comparación. El nivel puede ser alto, mediano o bajo. La verificación más estricta corresponde al nivel alto. El nivel de comparación de huella por defecto está configurado en el nivel medio de seguridad y escaneo (cumpliendo con el mecanismo para una robusta autenticación de usuarios).

Después, haga clic en "*Comenzar*". Se exhibirá la ventana Registrar Huella, esta ventana interactuará con usted para que sea posible la lectura de su huella dactilar.

Figura 2.10. Ventana – Registrar Huella

Para registrar su huella, deberá hacer tres lecturas exitosas (deslizamiento sobre el sensor). Debe utilizar la misma huella dactilar para realizar las 3 lecturas. Luego, se mostrará una ventana informando que su huella se ha registrado correctamente.

Para continuar haga clic en "*Aceptar*", finalizando el registro de su huella dactilar.

Figura 2.11. Ventana – Huella Registrada Correctamente

Usted puede registrar hasta 8 (ocho) huellas dactilares de esta misma forma.

2.3.4 Actualizando una Huella Dactilar

Usted puede modificar o actualizar las huelas dactilares ya registradas con el "*Administrador de Huellas*" del BioPass3000. Usted **DEBE** registrar por lo menos una huella dactilar y proceder a la verificación de esta huella o de la password inicial antes de actualizar la huella dactilar. Si no está autenticado, es decir, no verificó su huella ni la password inicial, se le mostrará la siguiente ventana:

Figura 2.12. Autenticación requerida

Haga clic en "*Actualizar Huella*" de la ventana del Administrador de Huellas. La ventana Actualizar Huella será exhibida.

Figura 2.13. Ventana Actualizar Huella

Si usted aún no registró ninguna huella dactilar, un mensaje será mostrado.

Este mensaje informará que usted necesita registrar primero una huella antes de poder realizar cualquier operación con el BioPass Token USB.

Figura 2.14. Ventana solicitando que el usuario registre primero una huella

Seleccione de la lista un ID de los disponibles. Cada ID representa una huella dactilar almacenada en el BioPass Token.

La huella que seleccione será la que actualizará con este proceso. Es decir, esa huella será eliminada del dispositivo y reemplazada por otra que Ud. enrolará en los siguientes pasos. Tenga en cuenta que la huella no esta asociada a un certificado digital en particular, las huellas dactilares son el mecanismo de autenticación que utiliza BioPass 3000 Token USB, y lo que marca la diferencia haciendo que esta solución sea única en su clase.

Luego haga click en “*Comenzar*”. Después se mostrará una ventana que le permitirá el registro de su huella a fin de que la logre actualizar.

Figura 2.15. Ventana Actualizar Huella

Para actualizar una huella, será necesario hacer tres lecturas bien efectuadas. Usted “**no**“ podrá usar huellas diferentes en este proceso.

Luego, haga click en “*Aceptar*” en la ventana de diálogo para completar la actualización.

Figura 2.16. Ventana de Diálogo – Actualización de huella exitosa

2.3.5 Eliminar una Huella

Usted también puede borrar huellas dactilares registradas. Para realizar esta tarea, antes es indispensable que verifique su huella para ganar acceso al dispositivo. Si no lo hace, es decir, no se autentica, se le mostrará una imagen como la de la Figura 2.12.

Haga click en "*Eliminar*" de la ventana del Administrador de Huellas. La ventana Eliminación de Huella será exhibida.

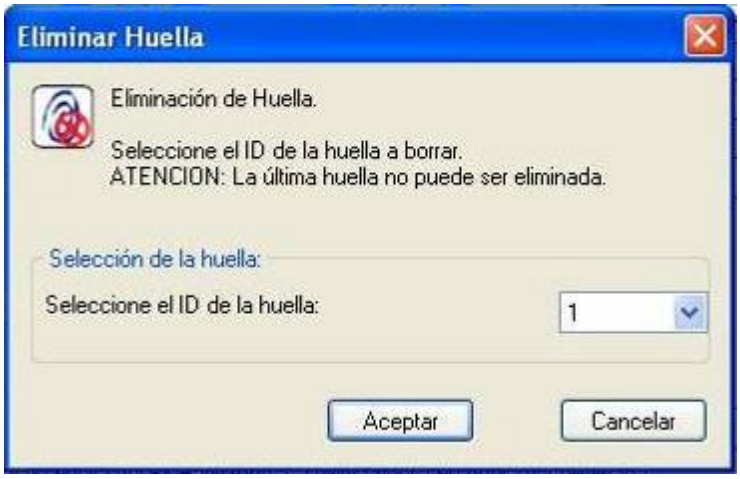


Figura 2.17. Ventana Eliminar Huella

Usted tendrá que seleccionar, a partir de la lista, el ID de una huella dactilar y luego hacer click en "*Aceptar*". Ni bien se concluye el proceso se mostrará la siguiente ventana:

Figura 2.18. Ventana – Eliminación de Huella

Haga click en "*Aceptar*" para finalizar la operación.

Figura 2.19. Mensaje: última huella no puede ser eliminada

2.3.6 Salir

Haga click en "*Salir*" de la ventana del Administrador de Huellas para salir y volver al menú principal de la herramienta.

2.3.7 Consideraciones Generales

- El BioPass3000 soporta la lectura secuencial de huella dactilar con deslizamiento hacia arriba o deslizamiento hacia abajo.
  Puede realizar la lectura de su huella de la forma que a Ud más le convenga. Sin embargo, usted debe conocer que al registrar una huella de atrás para adelante, usted siempre tendrá que obedecer este sentido cuando vaya a realizar la verificación correspondiente para ganar acceso en el dispositivo, por ej. para firmar un correo o abrir una VPN.
- Como consejo, le recomendamos la lectura de su huella siempre en la misma dirección (es decir en el mismo sentido), esto evitará que usted tenga dificultades en la verificación en función del sentido de la lectura, caracterizando así una falla en la lectura de su huella.
- Usted debe proceder a la lectura de su huella de forma ni muy rápida ni muy lenta. Una velocidad adecuada es cercana a la mitad de un segundo. Usted podrá verificar la velocidad de lectura a través de la herramienta (FingerPrint Tour).
  Lo invitamos a que practique con el Finger Print Tour ubicado en Inicio / Programas / Macroseguridad.org / BioPass
  Si la velocidad fuese inapropiada, usted no obtendrá un resultado "favorable" de la imagen exhibida en la pantalla. Si la imagen es clara y completa toda el área del display, usted logró obtener una velocidad y presión adecuada para realizar el registro de su huella.
- No registre sus huellas con los dedos húmedos, engrasados, manchados o temblorosos. De lo contrario, la verificación estará predestinada al fracaso.

2.4 Login al BioPass Token

Haga click en "*Login*" de la ventana principal del Administrador. Luego se mostrará la ventana para realizar la lectura (escaneo) de la huella dactilar:

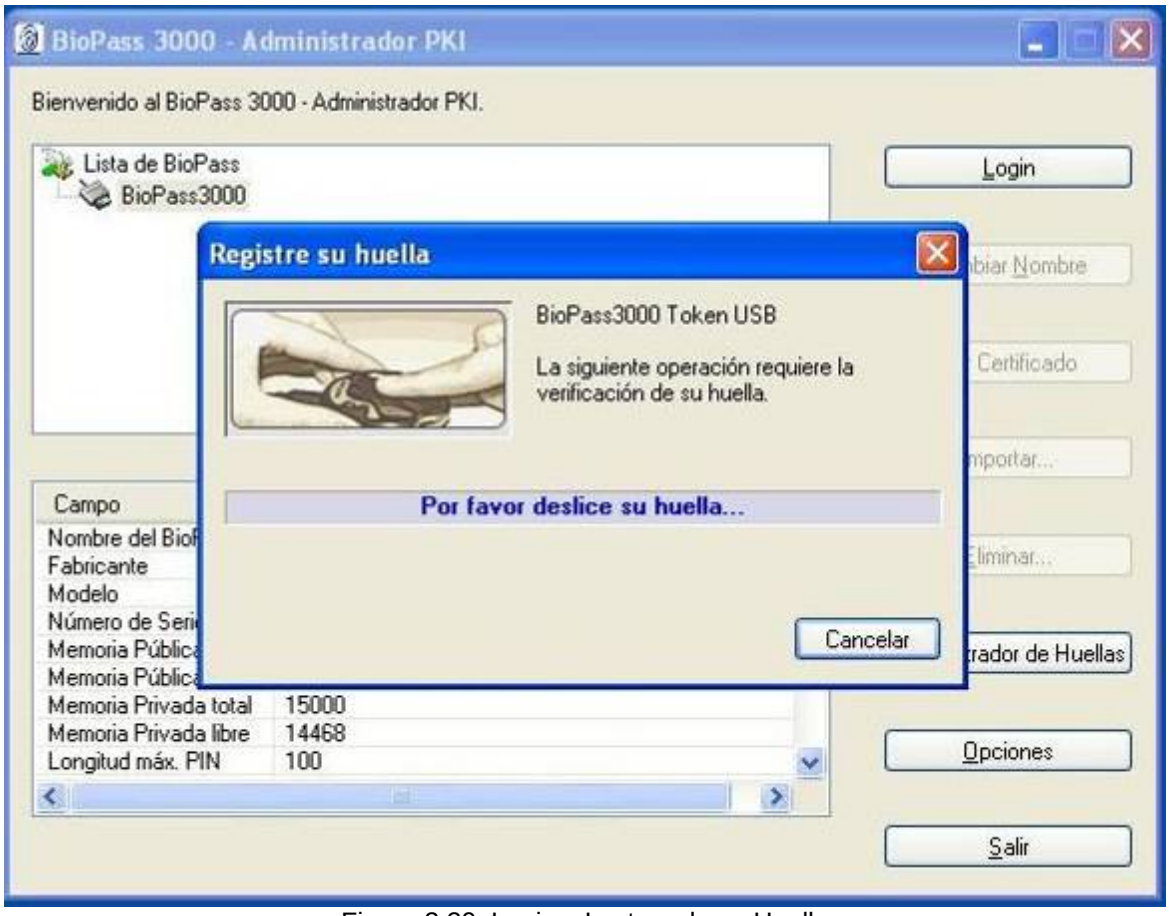


Figura 2.20. Login y Lectura de su Huella

Si usted aún no registró ninguna huella, tendrá que informar la password inicial para autenticarse al BioPass3000.

Haciendo click en "*Login*", se exhibirá una ventana que hará la verificación de la password inicial (recuerde que está password es por defecto "**12345678**").

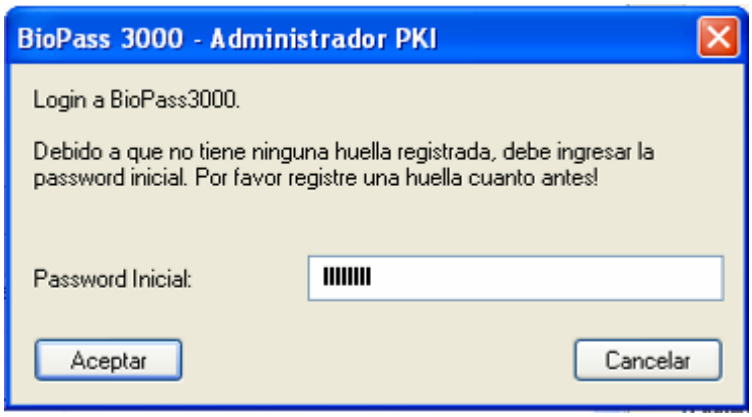


Figura 2.21. Ventana – Login con la Password Inicial

Luego de haber realizado la verificación de la huella o de la password inicial con éxito, la próxima ventana se mostrará, el nombre del BioPass Token en la parte superior de la ventana. Para visualizar un ítem, haga click sobre el mismo. Los detalles del ítem serán exhibidos en la parte inferior de la ventana. Si usted desea ocultar los detalles, basta con hacer click en el botón "*Ocultar Detalles*".

Luego del Login (autenticación), usted podrá ver no solo los datos públicos sino también los datos privados que están almacenados en su BioPass3000.

Observe que el botón "*Login*" cambió a "*Logout*". Usted puede hacer click en "*Logout*" para salir de forma segura.

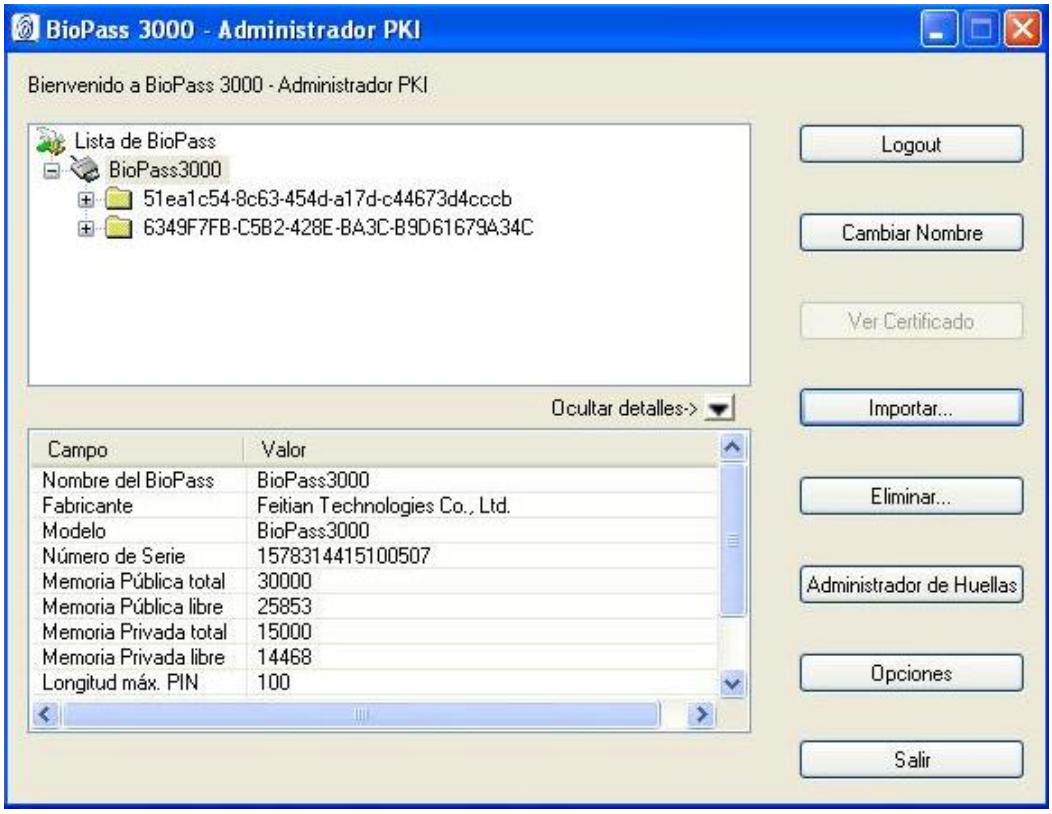


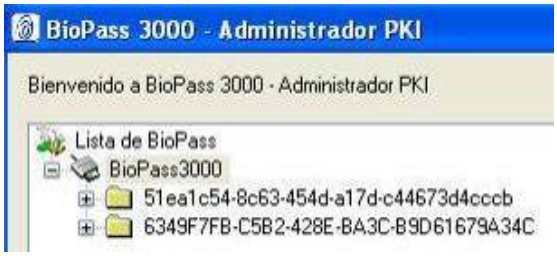
Figura 2.22. Interface luego del Login

2.5 Administrador de Certificados

Una vez que usted está autenticado (logueado) al "*Administrador del BioPass3000*", podrá realizar otras operaciones, tales como ver informaciones sobre el certificado, importar y eliminar datos o certificados.

2.5.1 Visualizando la Información del Certificado

Haga click en "**+**" situado al lado izquierdo del contenedor o, si prefiere, un doble click sobre el icono para exhibir el contenido del contenedor del BioPass Token. Los nombres de los contenedores que Ud. ve en la interface son generados automáticamente por la CA o por el middleware del BioPass.



De la misma forma, haga click en "**+**" situado a izquierda del ícono del certificado, o si prefiere doble click sobre este ícono para mostrar el par de claves (pública y privada).

Observe que en este momento el botón "*Ver Certificado*" quedará activo.

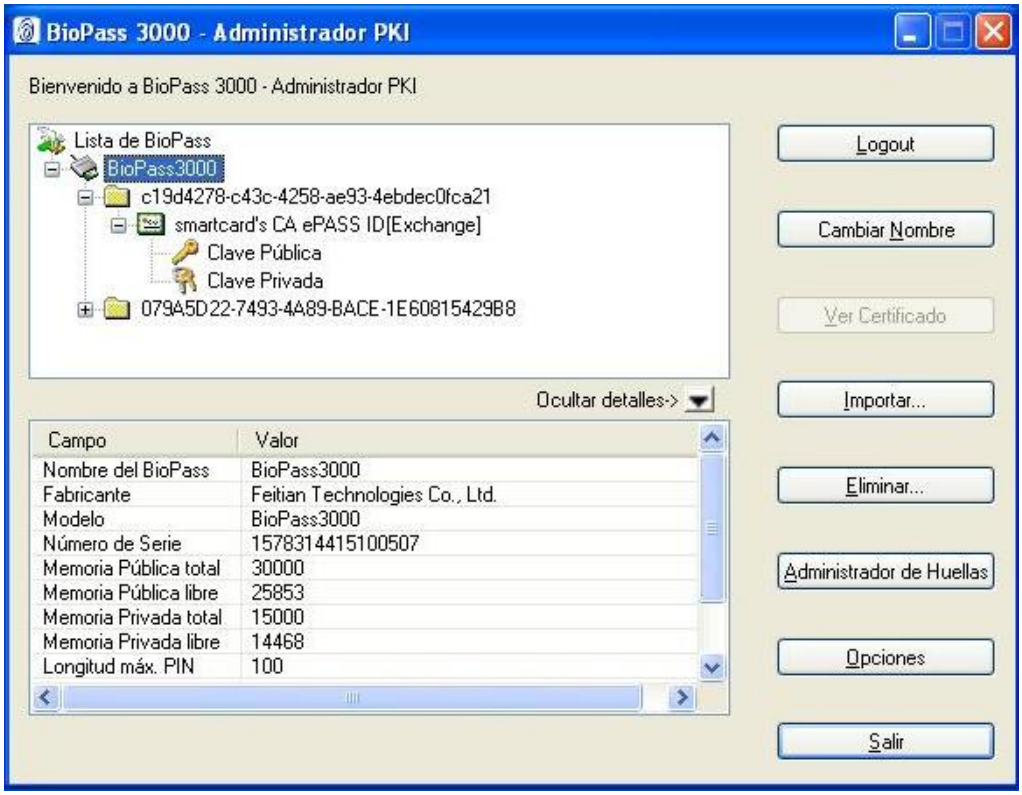


Figura 2.23. Ver Certificado

Haga click en el botón "*Ver Certificado*".

Luego la ventana Ver Certificado será exhibida. Usted podrá seleccionar las solapas "*General*", "*Detalles*" o "*Ruta de Certificación*" para visualizar la información del certificado.

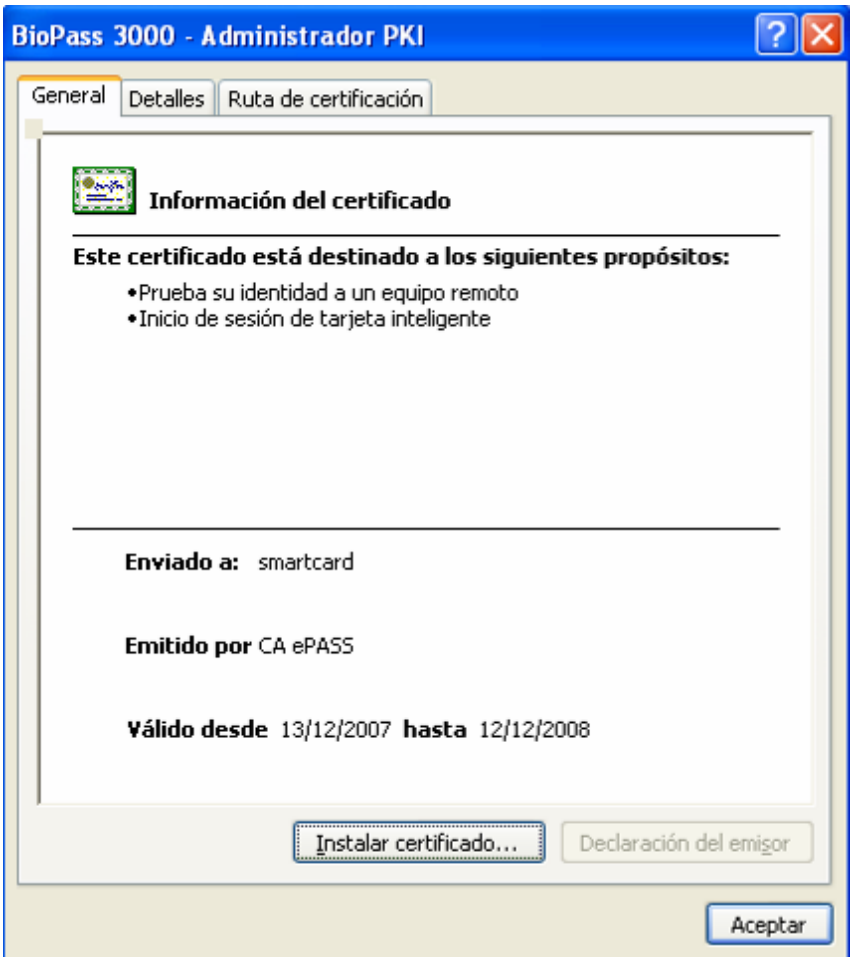


Figura 2.24. Ventana Ver Certificado

2.5.2 Importando Certificados al BioPass

Actualmente, los siguientes tipos de archivos de certificados son soportados por BioPass3000 Token USB:

- P7B,
- CER,
- P12
- y PFX

Los archivos de certificados P7B y CER no contienen el par de claves criptográficas. PFX es un tipo de archivo definido para almacenar un certificado y su par de claves asociadas (tanto la clave publica como la clave privada). P12 es el sucesor del formato PFX.

Importando un archivo de Certificado .PFX / .P12

Haga click en “Importar” de la ventana principal del “*BioPass 3000 - Administrador PKI*”. A continuación se exhibirá una nueva ventana, en ella haga click en “*Examinar*” y seleccione la ruta de acceso al archivo PFX del certificado que usted desea importar.

Si este archivo de certificado estuviese protegido por una password, ingrésela en el campo “*Password de Archivo*”. Usted podrá crear un nuevo contenedor para almacenar el certificado que esta siendo importado o si prefiere hacer uso de un contenedor ya existente.

Como un certificado contiene una clave pública y una clave privada, el mismo puede ser usado para intercambio o firma. Luego de especificar el propósito de uso del certificado, por favor haga click en “*Aceptar*” para importar el certificado.

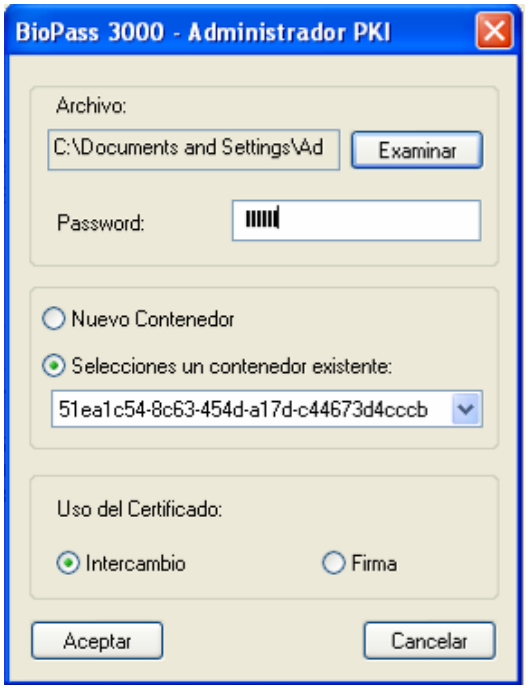


Figura 2.25. Importando un Certificado a partir de un archivo PFX

Importando un archivo de Certificado .CER / .P7B

Haga click en "*Importar*" de la ventana principal del Administrador. Luego será mostrada una nueva ventana, haga click en "*Examinar*" seleccione la ruta de acceso al archivo CER que usted desea importar.

Usted podrá crear un nuevo contenedor para almacenar el certificado que está siendo importado o si prefiere hacer uso de un contenedor ya existente.

Dado que el archivo de certificado CER no contiene el par de claves criptográfico (solo contiene la clave pública), solo puede ser usado para intercambio de claves, pero no para encripción o firma ya que estas operaciones requieren la utilización de la clave privada asociada al certificado.

Usted no puede seleccionar ninguna opción en el área Uso del Certificado. Haga click en Aceptar para importar el certificado.

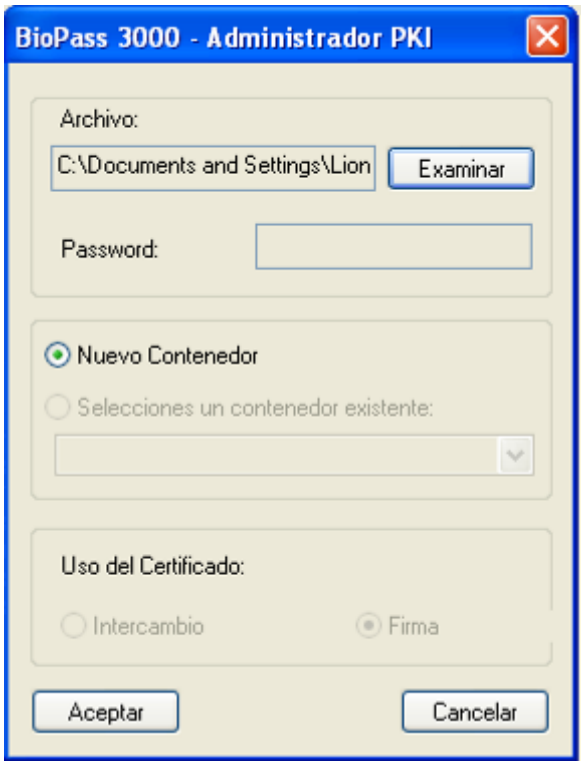


Figura 2.26. Importando un certificado a partir de un archivo CER

2.5.3 Eliminando Certificados

A partir de la estructura de opciones de la ventana principal del Administrador, seleccione el certificado que usted desea eliminar.

Después haga click en “Eliminar”. La siguiente ventana será exhibida.

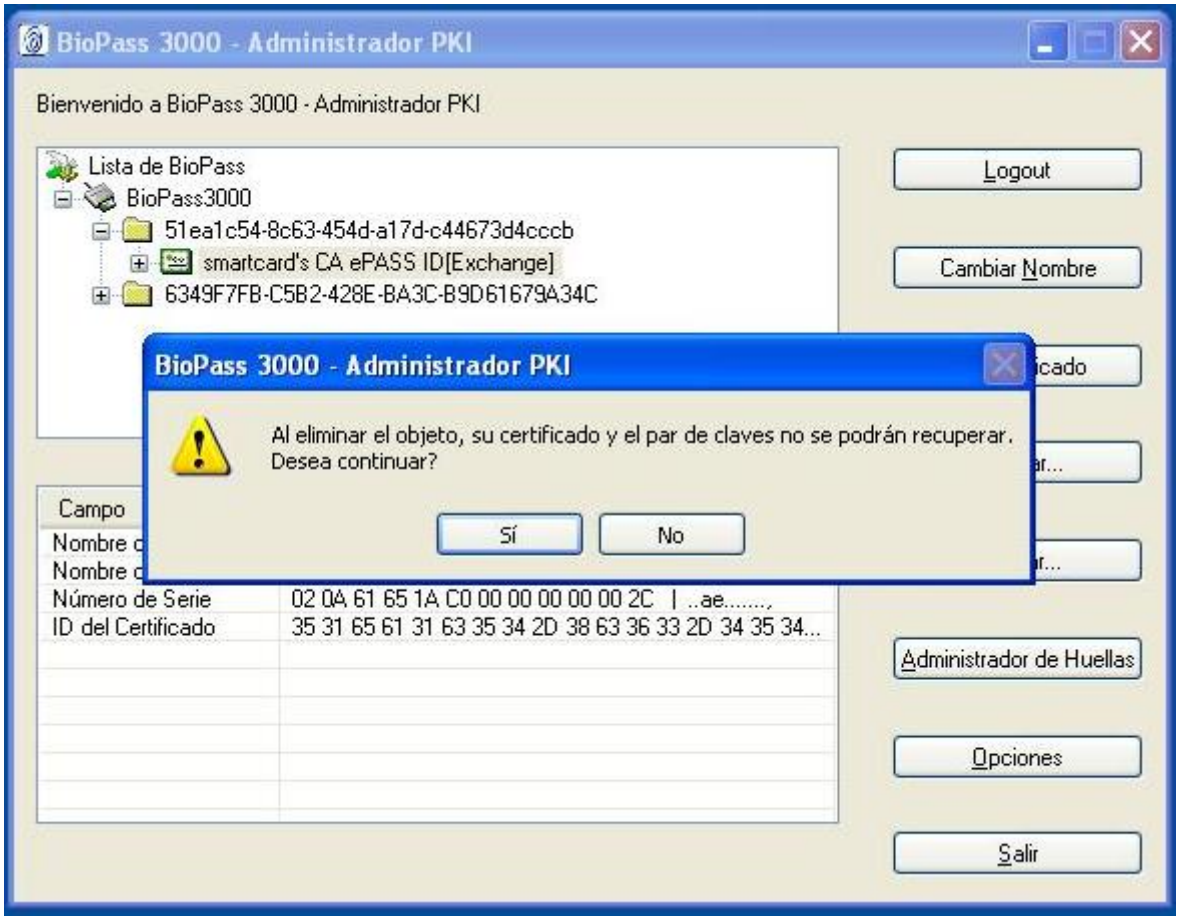


Figura 2.27. Eliminando un Certificado

Haga click en “*Si*” para confirmar la operación de eliminar. Los datos y la clave privada del certificado eliminado no podrán recuperarse:

2.6 Opciones del BioPass

Haga click en “Opciones” de la ventana principal del “*BioPass 3000 – Administrador PKI*”. Luego se exhibirá la ventana Opciones. Usted podrá definir el “*Windows SmartCard Logon*” (Logon al dominio del windows) y “*Visitar sitio web al conectar un BioPass 3000*”.

Si usted elige la opción "*Activar Windows SmartCard Logon con BioPass 3000*", usted podrá usar su BioPass3000 para autenticarse de la misma forma que con una smartcard, sin embargo es necesario tener un certificado digital emitido para ser utilizado con esta finalidad. Otra información importante es que, la funcionalidad de smartcard logon es soportada solo por los sistemas operativos Windows2000, Windows XP, Windows VISTA y versiones mas recientes de este sistema operativo, siempre y cuando exista tambien un controlador de dominio. Si usted elige la opción "*Visitar sitio web al conectar el BioPass3000*" e informar un website, usted podrá visitar automáticamente este site la próxima vez que usted conecte el Token a su PC. Para finalizar, haga click en "*Aceptar*".

Figura 2.28. Opciones Avanzadas

2.7 Cambiar el Nombre del Token

Generalmente, un dispositivo criptográfico es identificado por el número serial, pero este número es muy difícil de memorizar. Para facilitar la identificación de su dispositivo criptográfico, usted puede definir un nombre para él.

Para cambiar el nombre del Token siga las siguientes instrucciones:

Haga click en "*Cambiar nombre*" de la ventana principal del Administrador. Se mostrará una ventana como la que sigue:

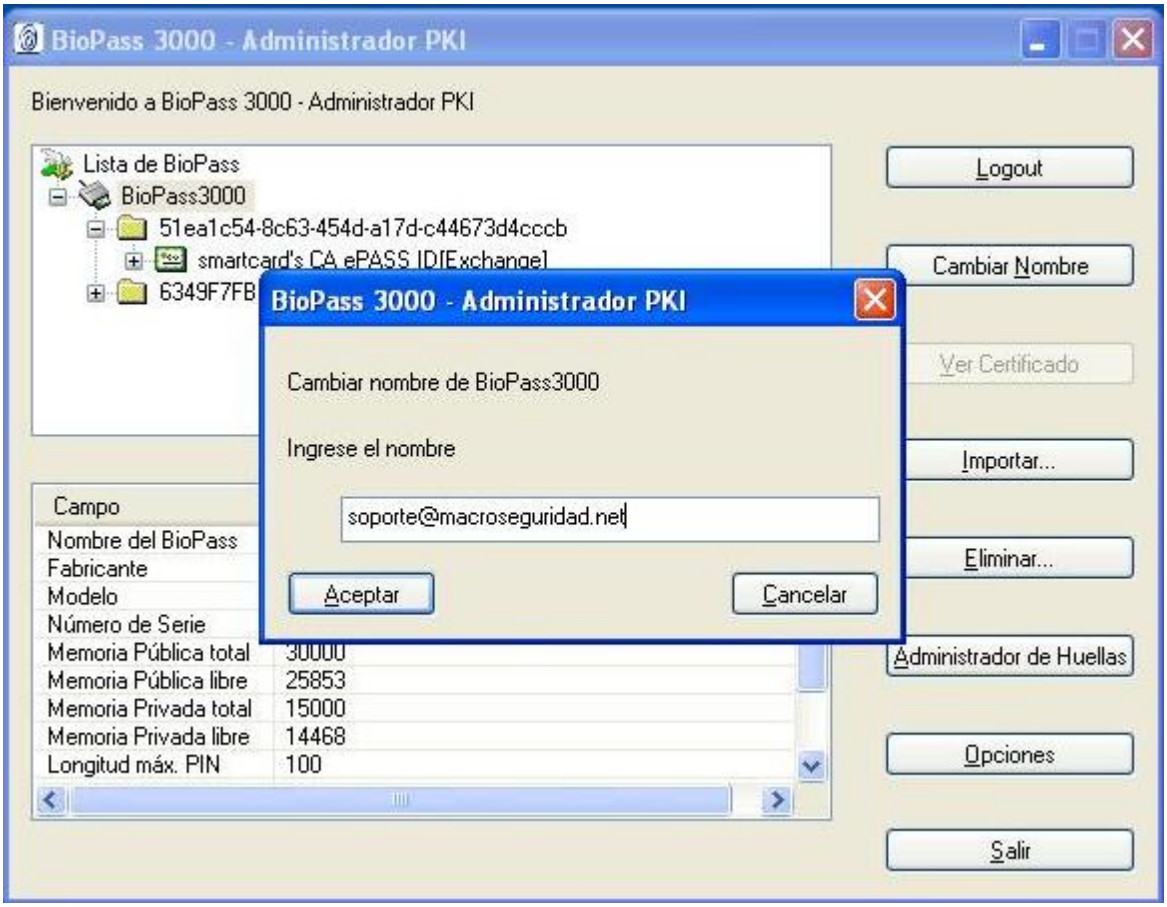


Figura 2.29. Cambiar nombre del BioPass Token

Ingrese un nuevo nombre para el Token en la ventana de diálogo y haga click en "*Aceptar*".

3 Fingerprint Tour

Este capítulo presenta la herramienta "*Fingerprint Tour*" que le enseñará a realizar una lectura de su huella dactilar en forma correcta.

Para iniciar esta herramienta haga click en "Menú Inicio" → "Programas" → "Macroseguridad.org" → "BioPass 3000" → "Fingerprint Tour".

Este capítulo abordará los siguientes tópicos:

- Interface
- Uso
- Una introducción sobre tipo de imágenes de huellas

3.1 Interface

La ventana principal de Herramientas FingerPrint Tour está dividida en cuatro áreas: Área de Muestra de la Huella, Área de Controles, Área de Estado y Área de Ejemplos.

Área		**Descripción**
Área de Muestra de Huella		Muestra la imagen de una huella que fue leída por el sensor
Control	Escanear	Haga click en “Escanear” para leer una huella.
	Ayuda	Haga click en “Ayuda” para obtener ayuda.
	Salir	Haga click en “Salir” para cerrar el programa.
Estado		Muestra el estado actual del dispositivo
Ejemplos		Muestra ejemplos comunes de huellas para comparar

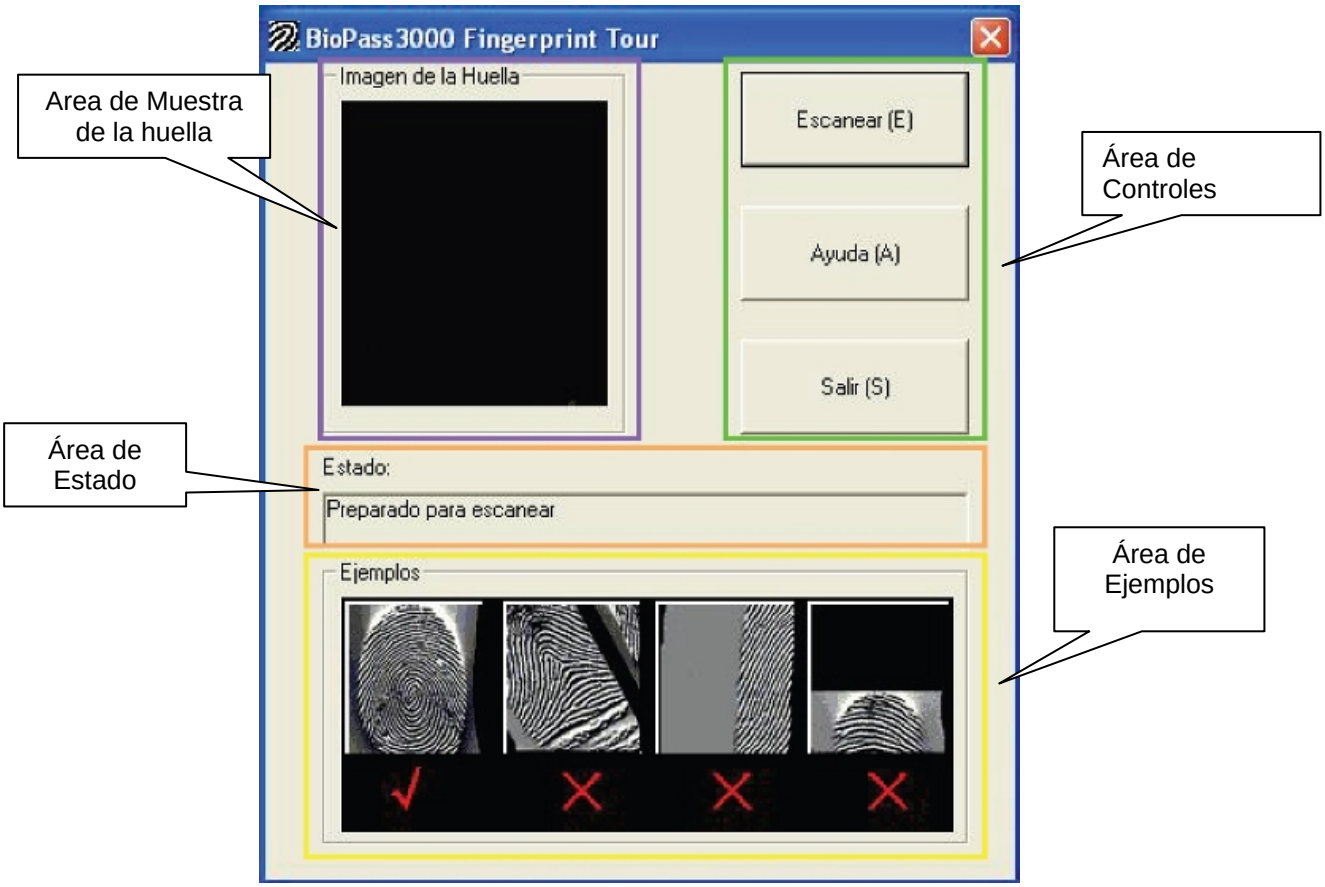


Figura 3.1. Ventana Principal

3.2 Uso del FingerPrint Tour

Luego de conectar un BioPass 3000 token, inicie la herramienta "*Fingerprint Tour*". Haga click en "*Escanear*" en el Área de Controles, y luego deslice su dedo sobre el sensor del dispositivo criptográfico.

El Área de Muestra de la Huella creara de forma automática la imagen de su huella. A través de comparación con las imágenes del Área de Ejemplos, usted podrá ver si el modo como su dedo fue deslizado proporcionó una lectura correcta.

3.3 Introducción sobre Imágenes de Huellas

3.3.1 Imágenes de Huellas Aplicables

Para obtener una alta calidad de imagen en su huella, se deben tener en cuenta los siguientes puntos:

- El punto central de la huella está localizado en el área central de la imagen
- La imagen de la huella está centralizada
- La imagen debe ser clara y no debe tener interferencias
- La textura debe estar limpia y completa
- La imagen debe completar toda el área de lectura
- Alto contraste

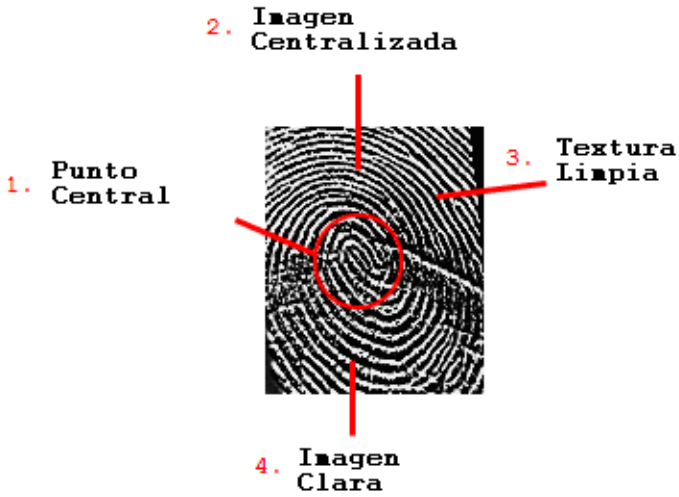


Figura 3.2. Imagen de una huella digital adecuada

Las siguientes imágenes son ejemplos de huellas adecuadas:

Figura 3.3. Ejemplo 1

Figura 3.4. Ejemplo 2

3.3.2 Imágenes de Huellas Inapropiadas

Como el sensor del producto funciona a través de diferencia de temperatura entre el inicio y el fin de la lectura de una huella, en algunos momentos la calidad de la huella obtenida puede quedar un poco distorsionada debido a las siguientes razones:

El dedo puede estar húmedo. La imagen obtenida queda oscura y con poco contraste.

Figura 3.5. Dedo Húmedo

La piel del dedo está dañada o parcialmente descamada. Alguna parte de la imagen no quedará muy clara.

Figura 3.6. Piel del dedo dañado o parcialmente descamada

El dedo tiene una cicatriz o cicatrices. Existe una o mas marcas en la imagen.

Figura 3.7. Cicatrices

El dedo está severamente gastado. La mayor parte de la imagen no es clara. La imagen no presenta una calidad buena 3D.

Figura 3.8. Dedo severamente gastado

Una entrada incorrecta puede llevar a una falla en el reconocimiento. Usted debe observar las siguientes formas para hacer la lectura de su huella dactilar:

El dedo es deslizado fuera (o parcialmente) del área del sensor.

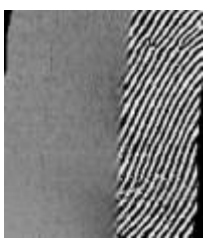


Figura 3.9. Lectura parcial de la huella

El dedo estaba muy inclinado cuando fue realizada la lectura.

Figura 3.10. Inclinado

El dedo se deslizó de forma muy rápida sobre el sensor durante la lectura.

Figura 3.11. Muy Rápido

El dedo no tuvo contacto total con el sensor durante la lectura.

Figura 3.12. Sin Contacto Total con el Sensor

La huella en si esta dañada

Figura 3.13. Huella Dañada

4 Usando el BioPass Token

Este capítulo tratará de los siguientes tópicos:

- Como conectar el BioPass 3000 Token a PC
- Visión General del Producto
- Como agarrar el BioPass 3000
- Como deslizar su huella sobre el lector
- Ejemplos de Uso

4.1 Como conectar el Token a la PC

Se utiliza el puerto USB Mini para conectar el BioPass3000, mientras que el puerto USB estándar es utilizado para conectarlo a la PC.

Vea la siguiente imagen:

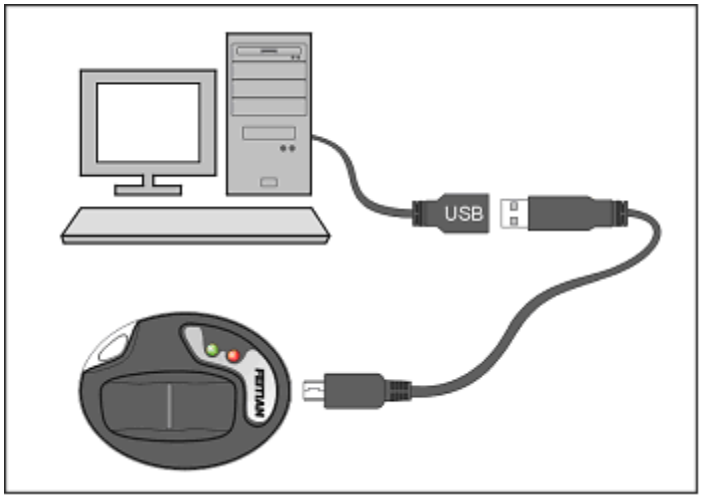


Figura 4.1. Método de Conexión

4.2 Visión General del Producto

Se muestra a continuación una visión general del producto.

Figura 4.2. Visualización del Producto

[1] Mini USB

El BioPass 3000 está equipado con un puerto Mini USB y lo acompaña un cable de conexión. Una de las extremidades del cable se conecta al Token y la otra extremidad puede ser conectada directamente al puerto USB de su PC o a otro cable extensor USB. El BioPass3000 es un producto con bajo consumo de energía. Se alimenta a través del puerto USB y no necesita de ninguna fuente de energía externa.

[2] [3] LED

El BioPass 3000 Token USB posee dos LEDs indicadores que exhiben el estado del funcionamiento.

Rojo	Encendido	Inactivo
	Apagado	Procesando
Verde	Encendido	En espera para leer huellas
	Apagado	Lectura finalizada

[4] Sensor

[5] Key Hole (espacio destinado para colocar el dispositivo criptográfico es su propio llavero).

4.3 Como manipular el BioPass Token

Usted podrá maniobrar su BioPass Token sin importar la forma, mientras sea posible hacer la lectura de su huella. Le mostraremos a continuación dos métodos:

Figura 4.3. Método 1

Figura 4.4. Figura 5.4 Método 2

4.4 Como deslizar la huella sobre lector

La huella debe ser deslizada de una punta a la otra como se muestra en la imagen a continuación.

La huella dactilar DEBE tener contacto total con el sensor.

Figura 4.5. Ejemplo 1

Figura 4.6. Ejemplo 2

4.5 Generación de Certificados On Board

BioPass 3000 Token permite la generación del par de claves dentro del propio hardware del dispositivo. Esto, sumado a su capacidad de realizar operaciones con estas claves utilizando el procesador criptográfico interno, asegura que las claves privadas nunca sean exportadas ni leídas por ninguna aplicación externa.

Toda operación de firma o encripción es realizada con el hardware de BioPass 3000, sin posibilidad de extraer la clave privada.

Para generar el par de claves dentro del Token USB solo deberá seleccionar el motor criptográfico de BioPass, llamado "***EnterSafe BioPass3000 CSP V1.0***".

El BioPass soporta la generación onboard de claves RSA de 2048 / 1024 y 512 bits para lo cual utiliza un RNG (Randon Number Generation) conocido también como generador de números aleatorios, pudiendo generar dentro del mismo dispositivo 9 certificados digitales. La solución provee un procesador de 32 bits, que es 4 veces superior a los otros tokens del mercado que solo proveen un procesador de 8 bits. Un certificado de 1024bits es generado en tan solo en 2 segundos.

Por ejemplo, la siguiente imagen es tomada del sitio www.pki.gov.ar, el cual provee certificados de verificación de existencia de cuenta de correo en forma gratuita para los ciudadanos. Para más información sobre la solicitud de certificados o sobre la utilización de los mismos con aplicaciones como Outlook, clientes VPN, etc., refiérase a

http://www.macroseguridad.net/download/epass/guias_PKI.htm

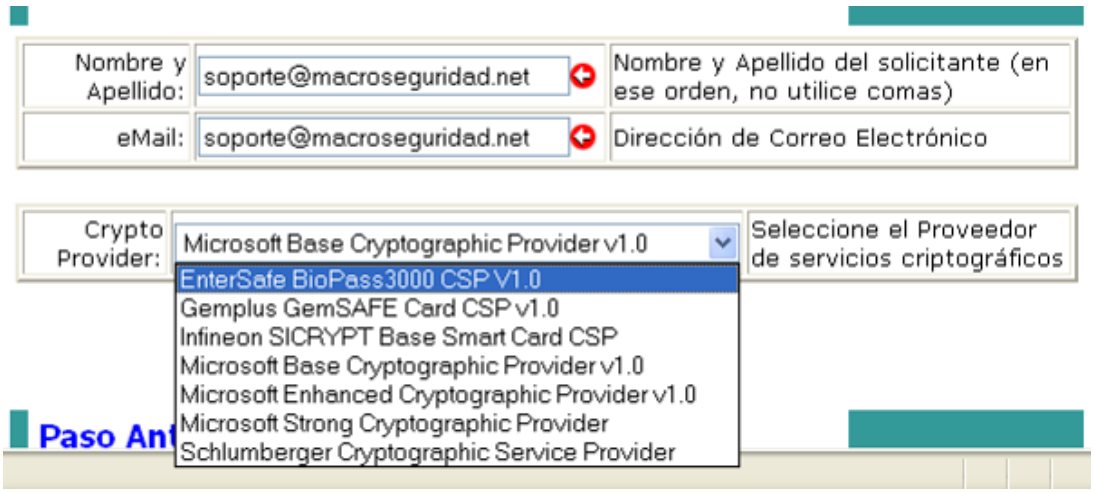


Figura 4.7. Selección del motor criptográfico (CSP) de BioPass

Luego, podrá utilizar el certificado generado en cualquier aplicación compatible con CAPI (Outlook, Outlook Express, Internet Explorer, Office, Adobe Acrobat, Checkpoint VPN Client, y muchas otras) o PKCS#11 (Firefox, Thunderbird, Netscape Navigator, PGP, OpenVPN, y muchas más).

4.5.2 Configuración de Aplicaciones CAPI

La mayoría de las aplicaciones compatibles con el estándar CAPI para comunicación con dispositivos criptográficos, no requieren ningún tipo de configuración adicional. Los certificados almacenados en el BioPass Token USB serán listados como si estuvieran almacenados en el repositorio local de Windows.

La única salvedad, es que al hacer uso de la clave privada de ese certificado, Ud. deberá autenticarse al dispositivo, deslizando su huella dactilar por el sensor.

La siguiente es una imagen que muestra la integración de **BioPass con Microsoft Outlook Express**.

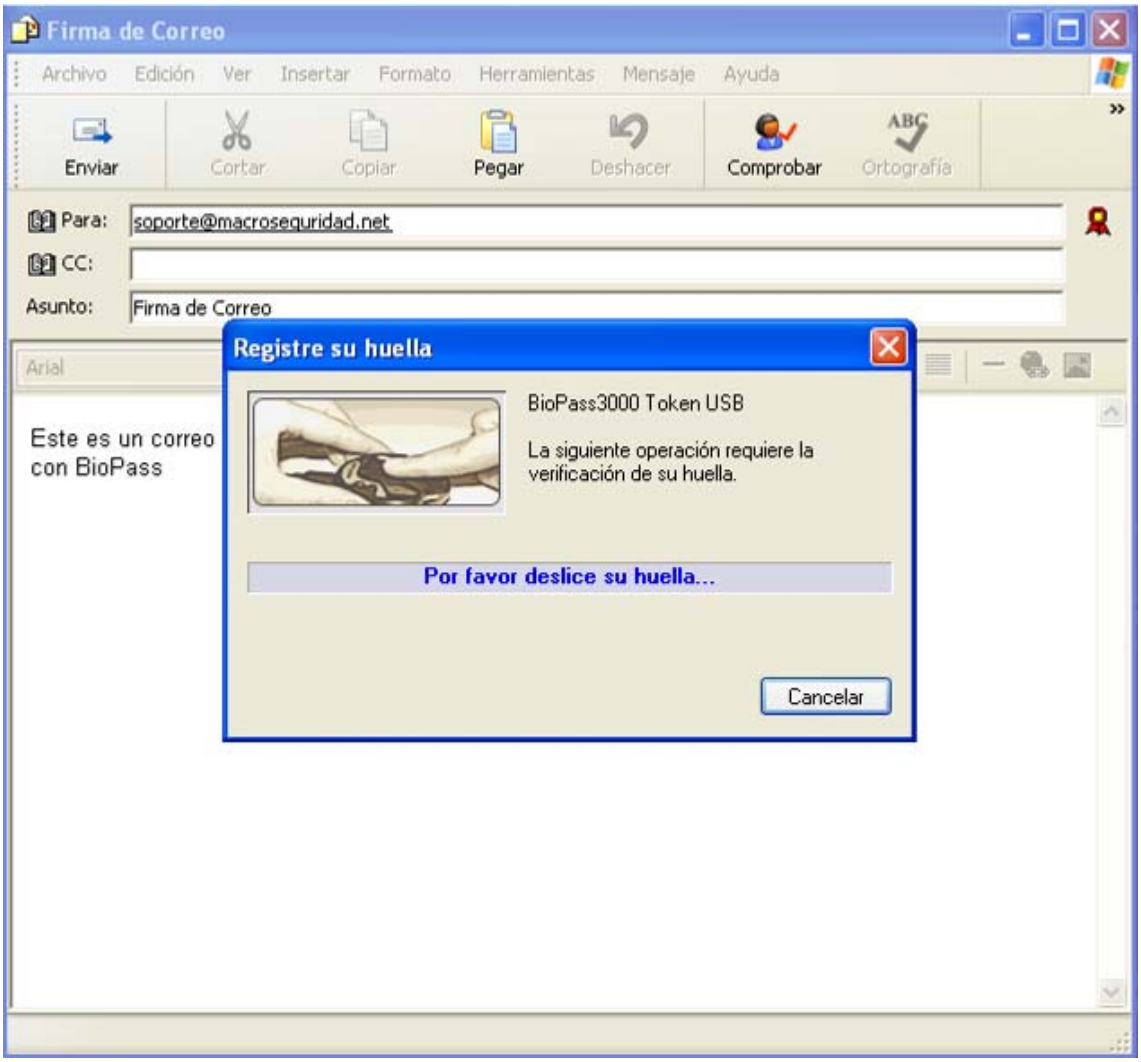


Figura 4.8. Autenticación al BioPass en aplicaciones CAPI.

4.5.3 Configuración de Aplicaciones PKCS#11

Al contrario que las aplicaciones que utilizan CAPI, éstas requieren una preconfiguración para reconocer los dispositivos criptográficos como BioPass u otro tipo de smartcard. Hay que especificar cual es la librería provista por el fabricante para trabajar con el estándar. En el caso de BioPass3000 en sistemas operativos Windows, esta dll es "*es1b3k.dll*", ubicada en el directorio *system32* de *Windows.*

Una vez hecho esto, la aplicación estará configurada para trabajar con los dispositivos BioPass, como se muestra en la siguiente imagen (la aplicación es un Mozilla Firefox, generando un certificado desde la CA de www.pki.gov.ar)

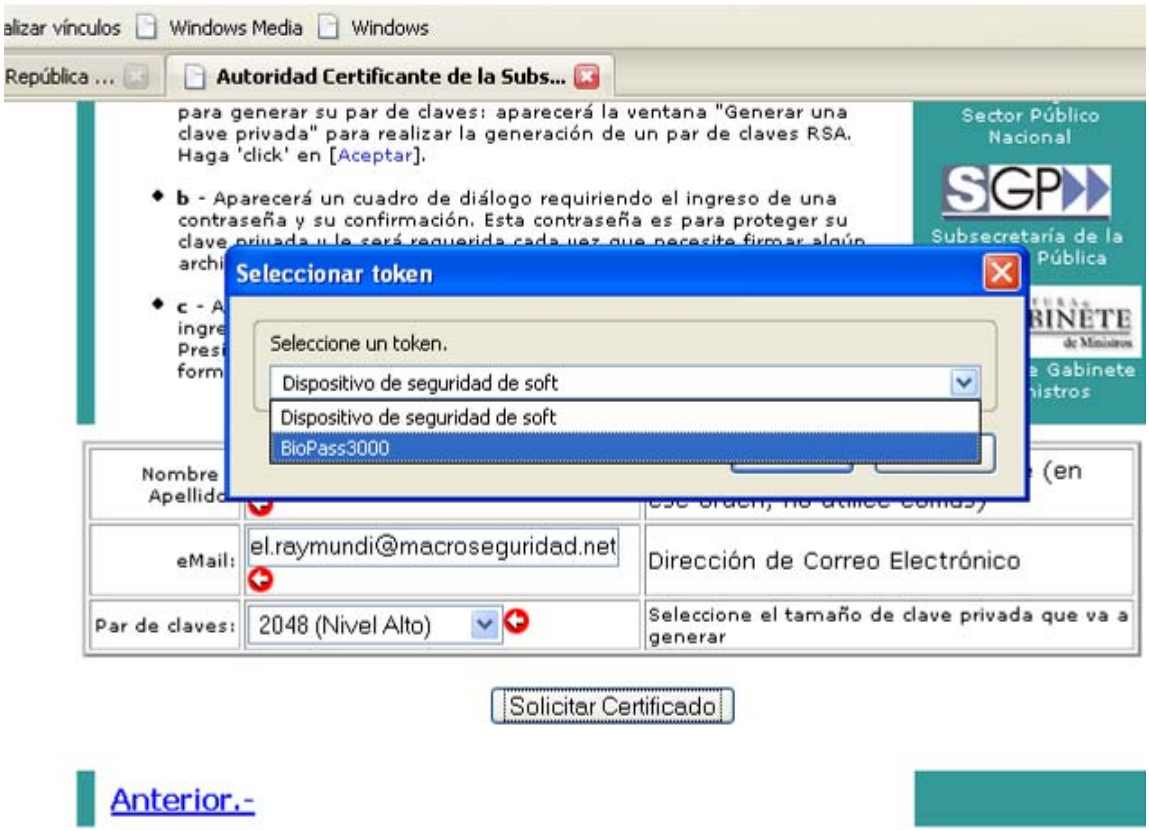


Figura 4.9. BioPass3000 compatible con el estándar PKCS#11

Es posible que la aplicación compatible con PKCS#11 requiera que ingrese una password, debido a que el estándar debe aplicarse a cualquier tipo de dispositivos criptográficos, incluyendo aquellos que no cuentan con la seguridad de BioPass3000 y autenticación biométrica.

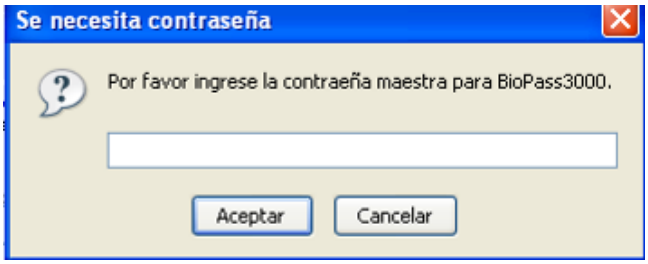


Figura 4.10. Autenticación al BioPass en aplicaciones PKCS#11

Puede hacer click en *Aceptar* y automáticamente se mostrará la ventana de login correspondiente a BioPass, para que se autentique a través de su huella dactilar.

Figura 4.11. Autenticación biométrica de BioPass en aplicaciones PKCS#11

Una vez autenticado, la aplicación continuará trabajando normalmente.

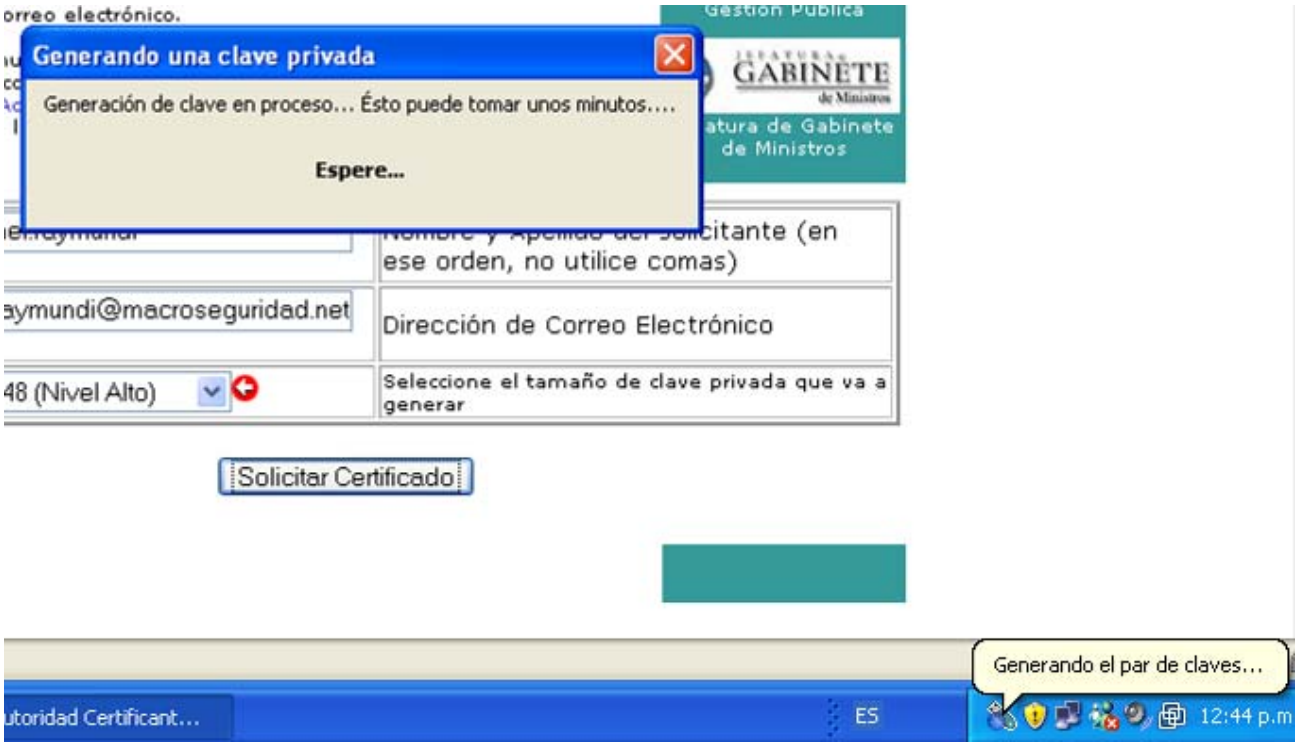


Figura 4.12. Aplicaciones compatibles con PKCS#11

5 La herramienta de Formateo

La herramienta de formateo de BioPass Token USB le permitirá inicializar la funcionalidad para PKI, además de formatear a bajo nivel el dispositivo (restaurando el estado de fábrica), permite eliminar todas las huellas dactilares almacenadas previamente, así como el contenido de la memoria del BioPass Token (claves públicas, privadas, certificados o passwords).

5.1 ¿Para que sirve?

La herramienta de Formateo restaura el estado de fábrica del BioPass 3000 Token USB, dejándolo como si recién llegara a sus manos desde su proveedor.

Esto involucra la inicialización para operaciones PKI, la eliminación de las huellas dactilares y de los datos almacenados (claves, certificados, passwords, etc.)

Si el BioPass perteneciera a un usuario que abandonó o fue despedido de la institución o empresa, y se desea reutilizar el dispositivo, debe utilizarse esta herramienta para eliminar las huellas que éste usuario dejó registradas. Nuevamente, recuerde que al formatear el BioPass, la información que este contenía será completamente eliminada (no pueden recuperarse los certificados y sus claves que fueron generadas dentro del BioPass 3000 Token), por lo cual esta herramienta no representa ningún riesgo en cuanto a la seguridad de la empresa. Es decir, las claves e información crítica solo pueden accederse por el usuario legítimo que utiliza sus huellas para poder autenticarse al dispositivo.

5.2 Modo de uso

Puede acceder a la herramienta de formateo desde Inicio -> Programas -> MacroSeguridad.org -> BioPass -> Formateador, o bien haciendo doble click en el archivo Formateador.exe, ubicado en la carpeta {Instalación SDK BioPass}\Tools\.

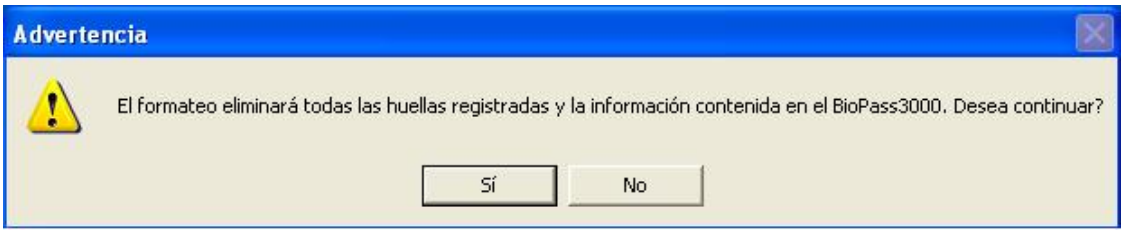
Al iniciar la aplicación se verá una ventana como la siguiente:

Figura 5.1. Opciones de formateo

En la pantalla anterior puede ingresar el Nombre del BioPass Token USB (el mismo puede ser cambiado más adelante, utilizando la herramienta de administración).

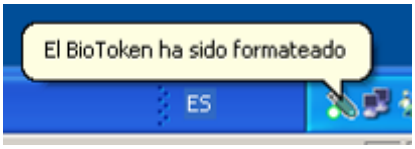
Una vez seleccionadas sus opciones, conecte un BioPass y haga click en el botón Formatear.

Se mostrará una advertencia como la que se ve a continuación



Haga click en Si para continuar y formatear el dispositivo conectado.

El icono del BioPass mostrado en el system tray de la PC comenzará a titilar  mostrará mensajes sobre el proceso de inicialización.



Una vez finalizado el mismo, la ventana principal de la herramienta mostrará el mensaje de "*Formateo exitoso*".

Ud. puede ahora desconectar el BioPass y comenzar a utilizarlo como si recién llegara de la fábrica.

6 Apéndices

6.1 Apéndice 1: Preguntas Comunes

1. **¿Por qué mi BioPass Token no puede ser reconocido por el sistema operativo y se desplegó la ventana de Nuevo Hardware fue Encontrado?**

   En este caso, parece que el driver no está instalado o no fue instalado con éxito. Por favor, verifique si la instalación del middleware del BioPass3000 finalizo correctamente antes de haber conectado su token BioPass3000 a la PC. Si este problema persiste, por favor desinstale el middleware del BioPass3000, reinicie su PC, luego del inicio del sistema, ejecute el archivo instalador del Middleware de BioPass3000 sin conectar el dispositivo hasta que el procedimiento de instalación haya finalizado y Ud. haya reiniciado su PC.

2. **Porque recibo una alerta de software**

   Puede existir la posibilidad de que Ud. posea una versión antigua del middleware del BioPass3000 y que la misma no se encuentre firmada digitalmente por

Microsoft. Simplemente contacte a nuestro soporte en:

www.macroseguridad.net/soporte/ePass

Windows VISTA

3. ¿Cómo puedo registrar mi huella dactilar?

Por favor, consulte las instrucciones de la **Sección 3.3.2** de este manual.

4. ¿Qué es la Password Inicial? ¿Para qué se utiliza?

Cuando el Token es usado con propósitos de seguridad, como por ejemplo, una solicitud de certificado, firma de documentación, etc., el usuario DEBE ser autenticado antes de usar el dispositivo. El mismo concepto se aplica para el BioPass3000, el usuario DEBE verificar su huella con la que está registrada y almacenada en forma segura dentro del BioPass. Cuando usted adquiere el BioPass3000 del fabricante, este no contiene ninguna huella, para facilitar el proceso a los usuarios y proteger el Token, se provee una password inicial de 8 caracteres “12345678”.

Usted deberá ingresar esta password para activar su Token y substituirla por su huella. La password Inicial podrá ser obtenida de su reseller o distribuidor oficial de Macroseguridad.org. Una vez que usted registró su huella, la Password Inicial quedara inválida.

5. ¿Por qué no consigo registrar mi huella con éxito, o hacer la verificación en forma correcta?

Por favor, consulte el punto ***2.3.3 Registrando Huellas Dactilares***

6. ¿Por qué no consigo hacer el smartcard logon?

Por favor, consulte aplicaciones CAPI para que el BioPass3000 realice el smartcard logon. Para lograrlo, se deben cumplir los siguientes requisitos:

a) Su PC debe estar como parte de un dominio;
b) Usted DEBE tener registrada una huella;
c) Tener almacenado en el Token por lo menos un certificado digital para smartcard logon;
d) Usted DEBE haber elegido la opción soporte smartcard logon.
Usando la Password Inicial no será posible hacer un smartcard logon.

7. ¿Por qué tengo problemas con la conexión del Token?

Verifique si el cable USB está debidamente conectado al puerto USB o al mini puerto USB. La mala conexión puede ser el origen del problema, verifique también que estén habilitados el uso de los puertos USB

6.2 Apéndice 2 Términos y Abreviaciones

Firma Digital: Resultado de aplicar el uso de los certificados digitales por ej. para la firma de un correo electrónico, una transformación criptográfica de datos, que cuando se implementa apropiadamente, provee los siguientes servicios de seguridad:

Autenticación de origen,

Integridad de datos y

No repudio.

Atribución de claves (key establishment): Proceso que posibilita atribuir una clave simétrica para uso criptográfico a los participantes legítimos de una sesión de comunicación. La atribución de claves puede ser realizada por medio de dos técnicas: “Negociación de Claves” o “Transferencia de Claves”.

Autoridad Certificadora o Autoridad de Certificación (AC de sus siglas en ingles Certificate Authority): Entidad idónea que cumples con una serie de normas, politicas y procedimientos de certificación y esta autorizada a emitir, renovar y cancelar certificados digitales. Es responsable por la administración de las claves públicas de cada uno de las personas.

Autoridad de Registro (AR): Es una entidad operacionalmente vinculada a determinada Autoridad Certificadora, la misma esta habilitada y es responsable por la confirmación de la identidad de cada uno de las personas o entidades que pueden solicitar un certificado.

BioPass3000: Token USB portátil, que se conforma por un sensor de huellas dactilares, un módulo de reconocimiento, una smarcard (sin necesidad de una lectora externa) y un puerto USB. Se garantiza y proporciona una autenticación univoca al dispositivo a través del uso de la biometría, a diferencia de la autenticación a través de una simple password.

Certificado Digital: Documento electrónico firmado digitalmente por una autoridad certificadora, y que contiene diversos datos sobre el titular, el emisor. La función principal del certificado digital es vincular una persona o una entidad a una clave pública.

Dicho en otras palabras el certificado digital no es ni más ni menos que nuestro documento de identidad para el mundo electrónico que estamos comenzando a transitar.

Clave criptográfica: Código o parámetro usado en conjunto con un algoritmo criptográfico, determinando las siguientes operaciones:

- Transformación de datos en texto claro para un formato cifrado y vice-versa;
- Generación on board de Firma digital;
- Verificación de una firma digita;
- Generación de un código de autenticación; o
- Un acuerdo para intercambio de un secreto compartido.

Clave Criptográfica en texto claro: representa una clave criptográfica no cifrada.

Clave secreta: Clave criptográfica, usada con un algoritmo criptográfico de clave secreta, que está únicamente asociada a una o más entidades y no debería tornarse pública.

Código de Autenticación: corresponde a un verificador de integridad criptográfica que es comúnmente referenciado como MAC (Message Authentication Code).

Co-firma: La co-firma (o sign) es aquella generada independiente de las otras firmas.

Contra-firma: La contra-firma (o countersign) es aquella realizada sobre una firma ya existente. En la especificación PKCS#7, la contra-firma es adicionada en forma de un atributo no autenticado (countersignature attribute) en el bloque de informaciones (signerInfo) relacionado a la firma ya existente.

Elemento de Dato: Corresponde a un ítem de información para el cual son definidos un nombre, una descripción de contenido lógico, un formato y una codificación [ISO/IEC 7816-4].

Entidad usuaria externa: Un individuo o proceso que realiza acceso a un módulo criptográfico independientemente del papel asumido.

ePass3000: Dispositivo criptográfico portátil integrado con una smartcard y puerto USB.

Una de las ventajas de este dispositivo por sobre las smartcards es que provee un procesador de 32bits, genera claves de 512 / 1024 y 2048bits, provee una memoria de 64Kb, con soporte para aplicaciones PKI y posee todo el software, manuales y guías en castellano, con licenciamiento perpetuo y actualizaciones sin cargo.

ePass2000: Es una smartcard en formato USB, con certificación FIPS 140-2 Level2, genera claves RSA1024bits, cuenta con 32kb de memoria y posee todo el software, manuales y guías en castellano, con licenciamiento perpetuo y actualizaciones sin cargo.

ePassNG: Es la denominación de la nueva generación del software de la línea de productos ePass Token (middleware). Este nuevo middleware soporta todas las series de los productos ePass. De fácil actualización con nuevo soporte de hardware, y soporte para aplicaciones PKI.

FIPS (Federal Information Processing Standards): corresponde a estándares y certificaciones desarrollados y publicados por el NIST (National Institute of Standards and Technology) para uso de sistemas en el ámbito de gobierno federal de Estados Unidos. El NIST desarrolla los estándares y certificaciones FIPS, cuando hay requisitos obligatorios del gobierno federal, tales como, seguridad e interoperabilidad, y no hay estándares o soluciones industriales aceptables.

Firmware: Programas y componentes de datos de un módulo que están almacenados en hardware (ROM, PROM, EPROM, EEPROM o FLASH, por ejemplo) y no pueden ser dinámicamente escritos o modificados durante la ejecución.

Frontera criptográfica (cryptographic boundary): La frontera criptográfica es un perímetro explícitamente definido que establece los límites físicos de un módulo criptográfico.

Hardware: Parte o equipamiento físico usado para procesar programas y datos.

Identificador de Registro: Valor asociado a un registro que puede ser usado para referenciar aquel registro. Diversos registros podrían tener el mismo identificador dentro de un EF [ISO/IEC 7816-4].

Integridad: propiedad que determina que la información que han sido escrita o los datos transmitidos NO han sido modificados o eliminados de una manera no autorizada e indetectable.

Interface: representa un punto lógico de entrada y salida de datos, que provee acceso a los servicios disponibles por los módulos criptográficos.

Interface CryptoAPI: Interface de operación de criptografía desarrollada por Microsoft, denominada también Microsoft CryptoAPI o MS CAPI. Esta interface ofrece al dispositivo criptográfico independencia o implementación de encapsulado de algoritmos criptográficos, permitiendo a los desarrolladores una fácil utilización de estos algoritmos en sus aplicaciones desarrolladas sobre la plataforma Microsoft integrando la utilización de la plataforma PKI (certificados digitales a través de CAPICOM), incluyendo criptografía de datos, verificación de certificados y firma digital en la plataforma Windows.

Middleware: Software que es usado para dar soporte criptográfico a un token (sea usb o smartcard) en algún sistema operativo y le interactuar con una aplicación concreta (como por ej. firmar digitalmente en Firefox).

Módulo criptográfico (cryptographic module): Conjunto de hardware, software y/o Firmware que implementa funciones o procesos criptográficos, incluyendo algoritmos criptográficos y de generación de claves.

Módulo criptográfico de chip único (Single-chip Cryptographic Module): representa una materialización física en la cual un chip único de circuito integrado (Integrated Circuit Chip - ICC) podría ser usado como dispositivo independiente (standalone), o podría estar embutido dentro de un producto (material de área delimitada), que está o no físicamente protegido. Por ejemplo, las Smartcards incluyen módulos criptográficos de chip único.

Negociación de claves (key agreement): Protocolo que posibilita atribuir una clave simétrica a los participantes legítimos en función de valores secretos definidos por cada uno de los participantes, de forma que ninguno de los participantes pueda predeterminar el valor de la clave. En este método, la clave no es transferida, ni siquiera de forma cifrada. Un ejemplo clásico de esta clase de protocolo es el algoritmo Diffie-Hellman.

Número de Identificación Personal (Personal Identification Number - PIN): un código alfanumérico o password usada para autenticar una identidad.

Número de Registro: Número secuencial atribuido a cada registro, que sirve para identificar únicamente el registro dentro de su EF [ISO/IEC 7816-4].

Oficial de seguridad: una entidad o proceso que actúa como tal, realizando funciones criptográficas de administración (llamado también Security Officer) para el reseteo de passwords en las smartcards y tokens usb.

Parámetros críticos de seguridad (PCS): Representan informaciones sensibles y relacionadas a la seguridad, tales como, claves criptográficas privadas, claves simétricas de carácter secreto, claves de sesión y datos de autenticación (passwords y PIN, por ejemplo), cuya divulgación o modificación puede comprometer la seguridad de un módulo criptográfico.

PC/SC: especificación para integración de smartcards en sistemas de computación (Personal Computer / Smart Card)

PKCS#11: estándar utilizado como interface para invocar operaciones criptográficas en hardware y es utilizado para proveer soporte a los tokens.

Registro: Cadena (string) de bytes que puede ser dirigida como un todo por la smartcard y referenciada por un número de registro o por un identificador de registro [ISO/IEC 7816-4].

Password: una cadena de caracteres (letras, números y otros símbolos) usada para autenticar una identidad o para verificar autorizaciones de acceso.

Password Inicial: password provista con el equipo por defecto para la utilización antes del registro de la primera huella. Esta password queda inválida luego del registro de la primera huella dactilar en el BioPass 3000 Token.

Software: Programas y componentes de datos usualmente almacenados en medios que pueden ser borrados (disco rígido, por ejemplo), los cuales pueden ser dinámicamente escritos y modificados durante la ejecución.

Token: Nombre genérico utilizado para identificar a todos los dispositivos criptográficos, tales como smartcards, dispositivos que poseen características y funcionalidades de almacenamiento de certificados y generación on-board de las claves privadas de los certificados, etc.

Token USB: Dispositivo criptográfico con conector USB, portátil y de fácil uso que brinda un doble factor de autenticación.

TSP (Token Service Provider): Conjunto de hardware abstracto presente en el framework **ePassNG**. Este conjunto de interfaces comunes de entrada y salida para todos los tipos de dispositivos. El diseño puede proveer una determinada expansión contra las diferencias de hardware.

Transporte de claves (key transport): Protocolo que posibilita que una clave simétrica sea transferida a los participantes legítimos. En este método, la clave es definida por una de las entidades y transferida a las demás.

Unidad de Dato: El menor conjunto de bits que puede ser referenciado de forma no ambigua [ISO/IEC 7816-4].

Usuario: un individuo o proceso que actúa como tal con la intención de obtener acceso a un módulo criptográfico para ejecutar servicios.

6.3 Apéndice 3 Lista de Acrónimos

AES Advanced Encryption Standard

AFIP Administración Federal de Ingresos Públicos

ANSES Administración Nacional de la Seguridad Social

APDU Application Protocol Data Unit

API Application Programming Interface

ATR Answer To Reset

CBC Cipher Block Chaining

CE Consumer electronics

CFCA China Financial Certificate Authority

CLK Clock

DES Data Encryption Standard

DF Dedicated File

EEPROM Electrically Erasable Programmable Read-Only Memory

EF Elementary File

FCC Federal Communications Commission

FIPS Federal Information Processing Standards

GND Ground

ICC Integrated Circuit Chip

ICP Infra-Estrutura de Chaves Públicas

ICP-Brasil Infra-Estrutura de Chaves Públicas Brasileira

IEC International Electrotechnical Commission

IKE Internet key exchange

IN Instrução Normativa

IPSec Internet Protocol Security

I/O Input/Output

ISO Internation Organization for Standardization

ITL Information Technology Laboratory

ITI Instituto Nacional de Tecnologia da Informação

IV Initialization Vector

JCE Java Cryptography Extension

LCR Lista de Certificados Revogados

LEA Laboratório de Ensaios e Auditoria

LSITEC Laboratório de Sistemas Integráveis Tecnológico

MAC Message Authentication Code

MF Master File

MSCAPI Microsoft Crypto API

NIST National Institute of Standards and Technology

OPSEC Operations security

PC Personal Computer

PCS Parâmetros Críticos de Segurança

PIN Personal Identification Number

PPS Protocol and Parameters Selection

PUK PIN Unlock Key

RFU Reserved for Future Use

RNG Random Number Generator

RSA Rivest Shamir and Adleman

RST Reset

SHA Secure Hash Algorithm

SO Sistema Operacional

SP Service Provider

SSL Secure Sockets Layer

TLV Tag Length Value

TSP Token Service Provider

TTL Time To Live

USB Universal Serial Bus

VPP Variable Supply Voltage

Contactos

MacroSeguridad Latino América – Headquarter

Dirección	Av. Raul Sacalabrini Ortiz 2356 Piso 7 “A” , Capital Federal, Buenos Aires, Republica Argentina.
Teléfono	+54-11-4833-9354 4833-5760
Fax	+54-11-4831-6538
E-mail	soporte@macroseguridad.net
Web Site	www.macroseguridad.org o www.macroseguridad.net

MacroSeguridad Latino America - Chile

Dirección	Av. Scalabrini Ortiz 2356 Piso 7 A (CP1425) Capital Federal – Republica Argentina
Telefono	+54-11-4833-9354
Fax	+54-11-4833-5760
E-mail	soporte@macroseguridad.cl
Web Site	www.macroseguridad.cl

MacroSeguridad Latino América – Brasil - Pronova Soluções Inteligentes

Dirección	Av. das Américas 500, bloco 4 (entrada A), Sala 302. Barra da Tijuca. Rio de Janeiro – RJ. CEP 22.640-100. Brasil.
Telefono	+55-21-24913688
Fax	+55-21-24913688 (ramal 103)
E-mail	suporte@pronova.com.br ou sac@pronova.com.br
Web Site	www.pronova.com.br ou www.lojapronova.com.br

Feitian Technologies Inc., Ltd. (Fabricante)

Dirección	3Fl., No.5 Building, Jimen Hotel, Xueyuan Road, Haidian District, Beijing, 100088, República Popular da China
Telefono	+86-10-62360800 e +86-10-62360900
Fax	+86-10-82070027
Web site	www.FTsafe.com