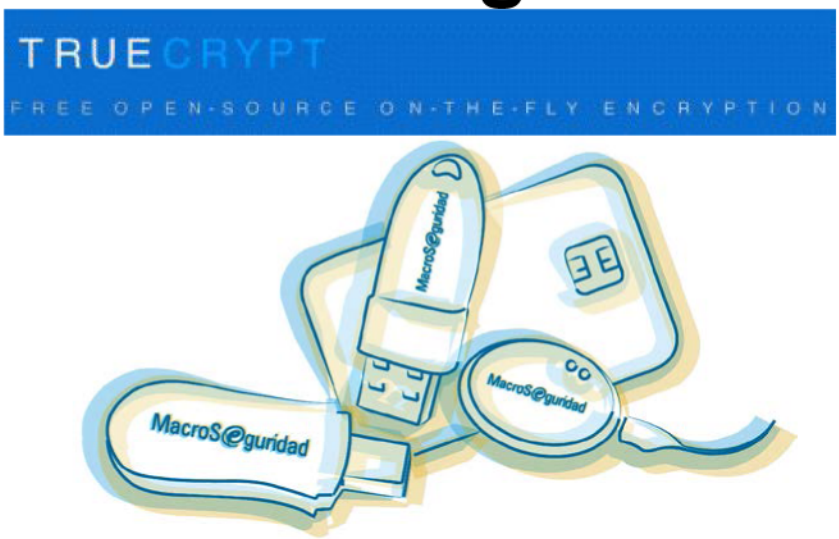
"Guía de integración de TrueCrypt con los Token USB de Macroseguridad"



Nombre del Partner	Truecrypt.org
Nombre de la Solución	Dispositivos Criptográficos de Macroseguridad (Tokens USB y Smartcards)
Fecha	10 de septiembre de 2015

Desarrollado por el Departamento de IT de MacroSeguridad y el Team de Integraciones

Revisiones:

Versión	Autor	Fecha	Comentarios
1.0	Pablo Lloveras	15-12-2009	Version preliminar
1.1	Alfredo Rodriguez	17-12-2009	1er revisión
1.2	Anabel Mirochnik	28-12-2009	2da revisión
1.3	Jessica Dragubitzky	11-02-2010	3era revisión
1.4	Pablo Lloveras	02-09-2010	Adicion explicación linux
1.5	Pablo Lloveras	13-07-2012	Actualización template
1.6	Pablo Lloveras	10-09-2015	Actualización contacto
1.7	Pablo Lloveras	10-09-2015	Actualización acuerdo de licencia

Tabla de Contenidos

A Acerca de Macroseguridad

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

Macroseguridad 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.

Los productos que MacroSeguridad.org distribuye incluyen: Smartcards (JavaCard, PKI Card), Lectoras de Smartcards (con conexión USB o interna, con características biométricas, contact y contactless, teclados con biometría y lectoras de smartcards), dispositivos Tokens USB para firma digital (otorgando portabilidad y transporte seguro de certificados digitales), generando no repudio en comercio electrónico, comunicaciones y Firma Digital. Los Tokens USB y las Smartcards brindan autenticación robusta y validación de usuarios en los accesos a la red (VPN, SSLVPN, Web Portal). La empresa también comercializa Tokens OTP (One-Time-Password), dispositivos generadores de números aleatorios para autenticación robusta de usuarios, software para single-sign-on y autenticación. Además, ofrecen soluciones de Time Stamping, Timbre Digital, Medios de pago diseñados para cumplir con los requerimientos y estandares de Payment Cards y EMV (PCI DSS) y HSM (hardware security module), equipos utilizados para el resguardo y generación de claves privadas. Asimismo ofrecen software para protección de booteo, soluciones de encripción de archivos y carpetas, logon seguro a la red, seguridad para SAP, autenticación robusta para PDA, teléfonos móviles, etc.

Macroseguridad 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), para la protección de desarrollos distribuidos en la red, que jerarquizan la venta de software vía Internet y evitan los mensajes de error en la descarga on line.

Macroseguridad 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.

Por último, Macroseguridad.org ofrece 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).

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

Para más información puede visitar www.MacroSeguridad.org

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.org

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

B.1 Redes Sociales de Contacto

Twitter: @macroseguridad

LinkedIn: www.linkedin.com/company/macroseguridad.org

WordPress: macroseguridad.wordpress.com

Youtube: www.youtube.com/Macroseguridad

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", y algo que conozco que es "la password del Token" y quien soy (ADN, Iris, Biometría, etc) brinda el tercer Factor de Autenticación.

2 Antes de Comenzar

2.1 Instalación del middleware del Dispositivo Criptográfico de Macroseguridad.org (Tokens USB / Smartcard)

Para poder utilizar un Token USB / SmartCard de Macroseguridad con **Truecrypt** deberá contar con un dispositivo criptográfico (Token USB o Smartcard) y tener **instalado el middleware del mismo**. De no ser así por favor instálelo y luego siga con esta guía.

Podrá obtener una guía de instalación del middleware en el siguiente vínculo:

www.macroseguridad.net/soporte/docs/guias_instalacion

El middleware del dispositivo criptográfico de Macroseguridad.org incluye todos los drivers necesarios para que su sistema detecte automáticamente el dispositivo (sea un Token USB o una Smartcard) y le permita descargar sus certificados directamente al mismo (para aprender cómo hacerlo haga click **aquí**), además contiene una importante herramienta para el uso del dispositivo, el *Administrador de Certificados de Macroseguridad*. Esta herramienta le permitirá cambiar el PIN que viene por defecto por otro que usted desee, cambiar el nombre del dispositivo para poder identificarlo con mayor facilidad, y poder exportar e importar certificados desde y hacia el dispositivo así como también eliminarlos.

2.2 Requisitos

- ✓ Truecrypt versión 6.3a o Superior.
- ✓ Middleware y herramientas del Token USB / Smartcards instaladas.
- ✓ Sistemas Operativos: Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows Server 2003, Windows Server 2008 , Windows Server 2012 o superior.
- ✓ Puerto USB habilitado o Lectora de SmartCards lista para funcionar.
- ✓ Un dispositivo criptográfico de Macroseguridad listo para usar.

Las pruebas desarrolladas en esta guía se han realizado bajo la plataforma **Windows XP SP3**, **Truecrypt 6** instalado junto con **Internet Explorer 8**.

3 ¿Qué es el TrueCrypt?

Truecrypt es una aplicación que le permite al usuario crear volúmenes virtuales encriptados los cuales pueden ser usados como si fueran unidades fisicas reales pero con la posibilidad de transportarlos fácilmente. Por otro lado tambien permite encriptar dispositivos y unidades fisicas tales como un disco duro o una memoria flash USB. Los procesos de encripción se realizan “On-the-fly” esto quiere decir que los procesos de encripción y desencripción se realizan en forma automática en un segundo plano sin intervención del usuario.

La información almacenada en un volumen cifrado puede ser leida (desencriptando los mismos) solo con la password/Keyfile.

Además de la password está la opción de utilizar un *keyfile*, es decir seleccionar uno de los miles de archivos que hay en el equipo como segunda contraseña. Si archivo y *password* coinciden, el volumen se monta y queda disponible como una unidad de disco estándar. Es importante tener presente que este archivo debe ser inmutable. Si su contenido cambia, TrueCrypt no lo reconocerá como el "archivo llave" correcto y negará el acceso al volumen cifrado.

Todo el sistema de archivos está codificado (por ejemplo, nombres de archivos, carpetas, el contenido de cada archivo, espacio libre, meta datos, etc.).

Los archivos se pueden copiar de un volumen de TrueCrypt montado igual que se copian desde cualquier disco normal (por ejemplo, arrastrar y soltar). Los archivos son automáticamente desencriptados on-the-fly, mientras que se está leyendo o copiando de un volumen encriptado por TrueCrypt. Del mismo modo, estos archivos que se escriben o copian en el volumen de TrueCrypt son automáticamente encriptados on-the-fly (antes de que se escriban en el disco virtual).

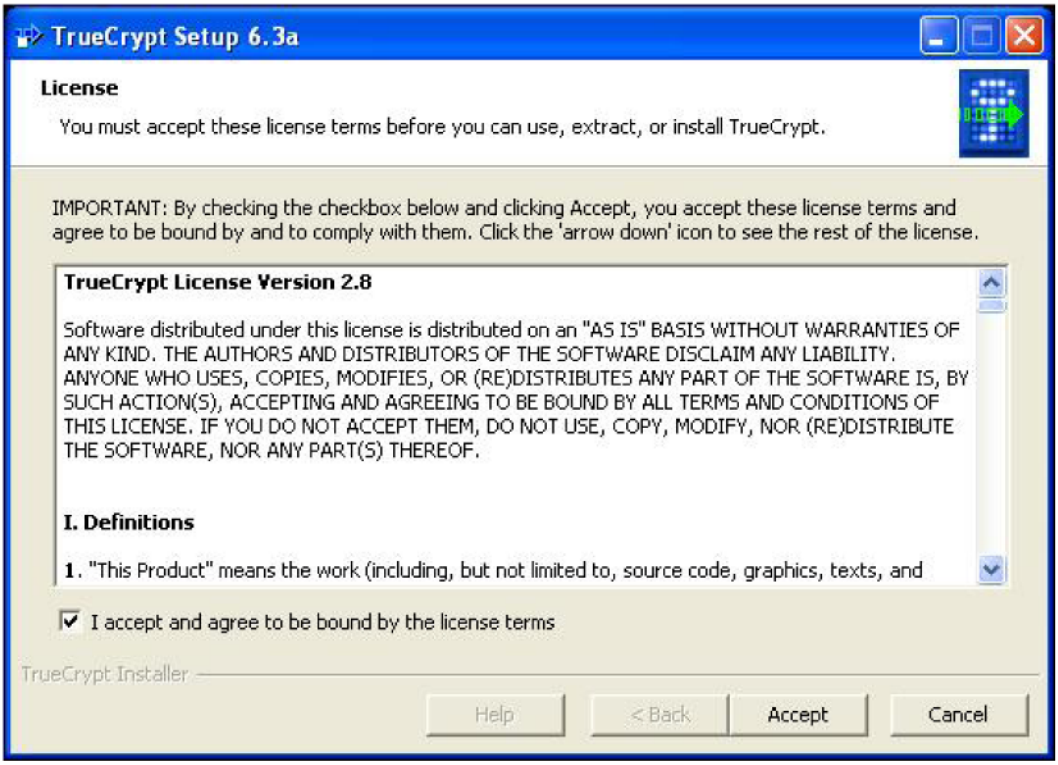
Luego de esta breve descripción lo invitamos a que continúe con la instalación.

4 Instalar el TrueCrypt

Ud. puede descargar el software de TrueCrypt desde **aquí**.

En este caso ejecutaremos el archivo "*TrueCrypt Setup 6.3a*" que acabamos de descargar, se le mostrará un mensaje que se encuentra firmado digitalmente.

Lea atentamente el contrato de licencia, si esta de acuerdo con el mismo haga click en "*Accept*" (tenga en cuenta de que si no lo acepta no podrá seguir con la instalación)

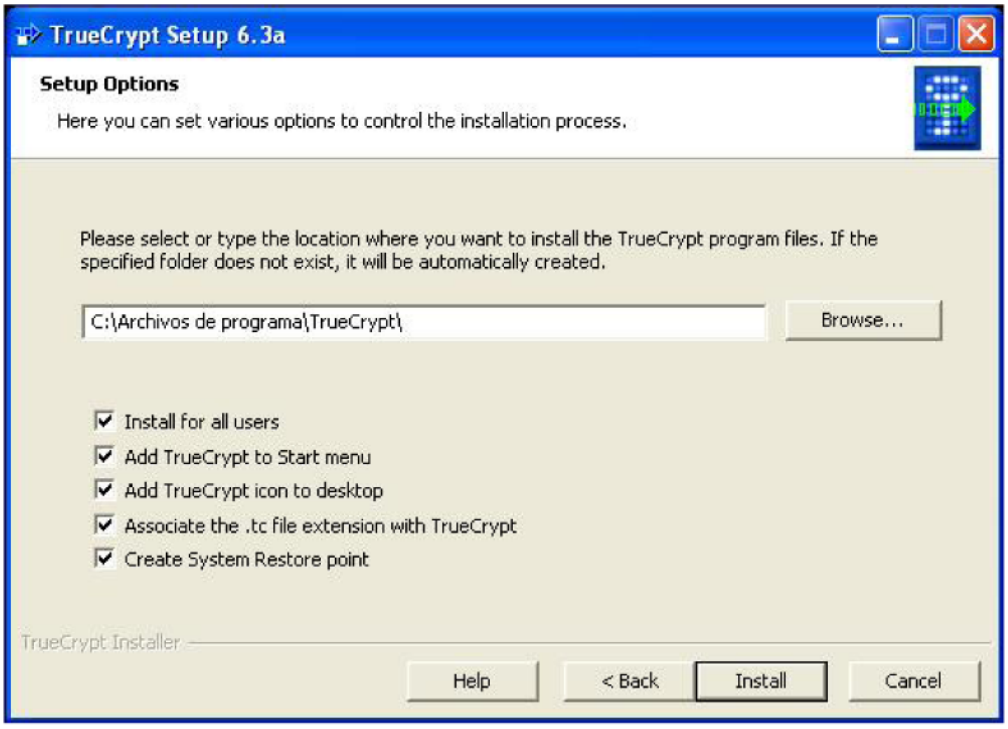


En la siguiente ventana le pregunta si desea instalar o extraer los archivos contenidos. Seleccione "*Install*" y luego haga click en "*Next*".

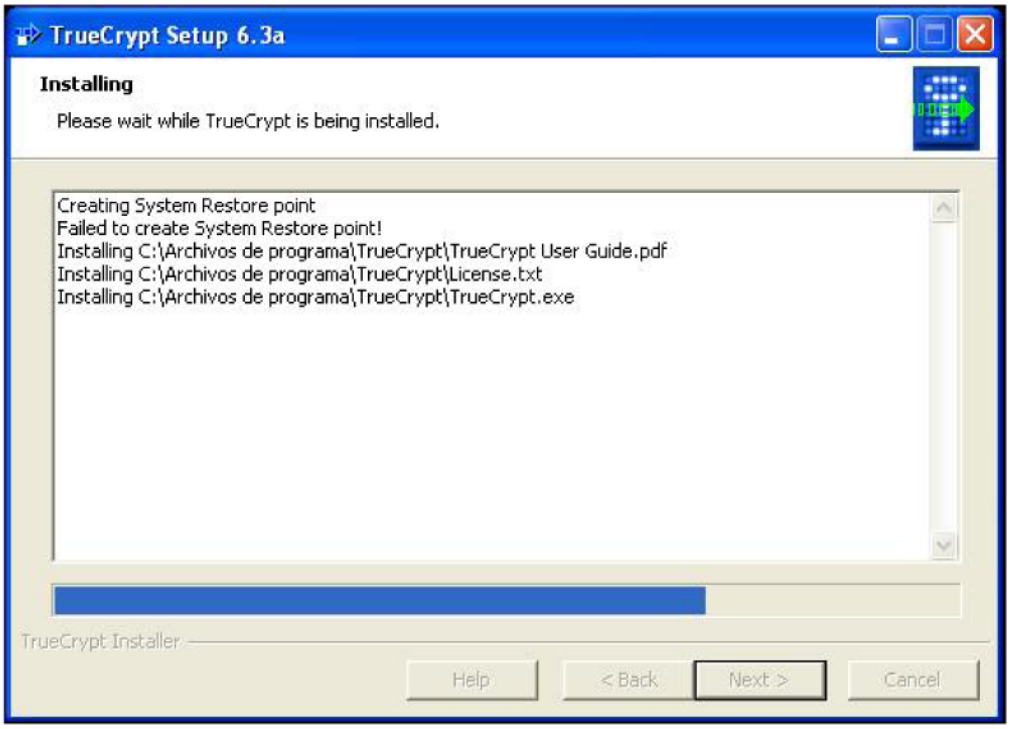
Ahora nos permitirá configurar los siguientes parámetros:

- Donde deseamos instalarlo
- Si lo desea instalar para todos los usuarios
- Si quiere crear un menú en el inicio
- Si quiere crear un acceso directo en el escritorio
- Si desea asociar la extensión ".tc" con el TrueCrypt
- Si quiere crear un punto de restauración del sistema.

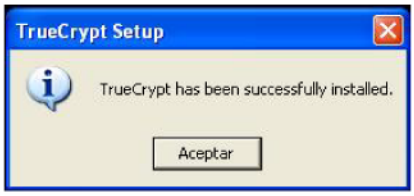
Seleccione las opciones que usted prefiera y haga click sobre "*Install*".

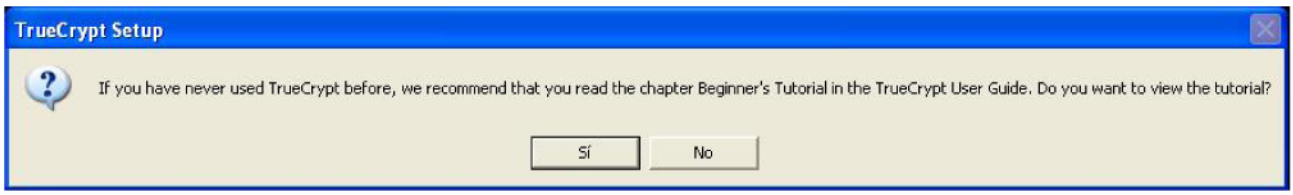


Luego el instalador procederá con la instalación del TrueCrypt en su PC.



Una vez finalizada la instalación se mostrará el siguiente mensaje informando que el programa se instaló satisfactoriamente. Se le ofrecerá leer un turorial (que se encuentra en inglés) de introducción en caso de ser la primera vez que utiliza este programa.

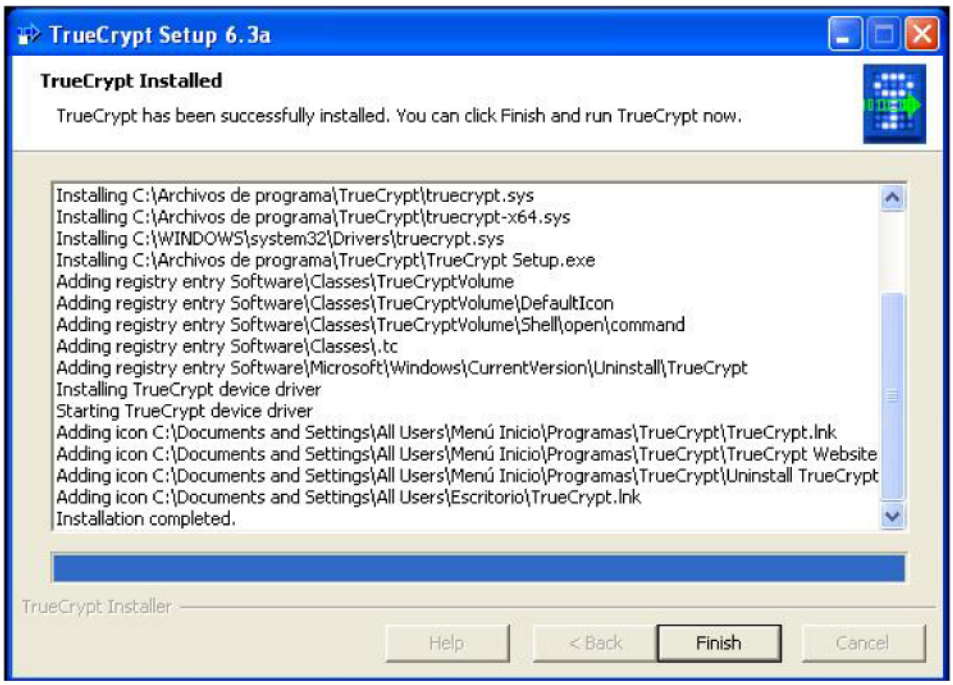




En caso de que usted quiera ver el tutorial seleccione lo opción "*Sí*". Inmediatamente se abrirá en el browser la página del manual del producto.

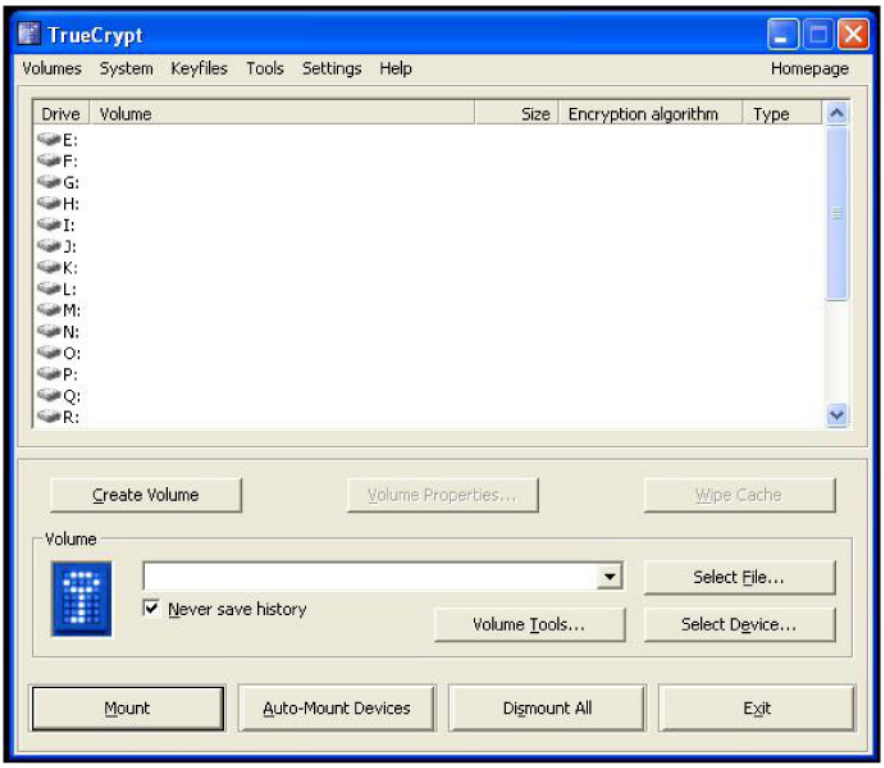
El programa se instaló correctamente, puede ejecutar TrueCrypt o reiniciar la PC.

Una vez que el programa se haya finalizado el proceso de instalación, haga click en "*Finish*" para cerrar el asistente de instalación.

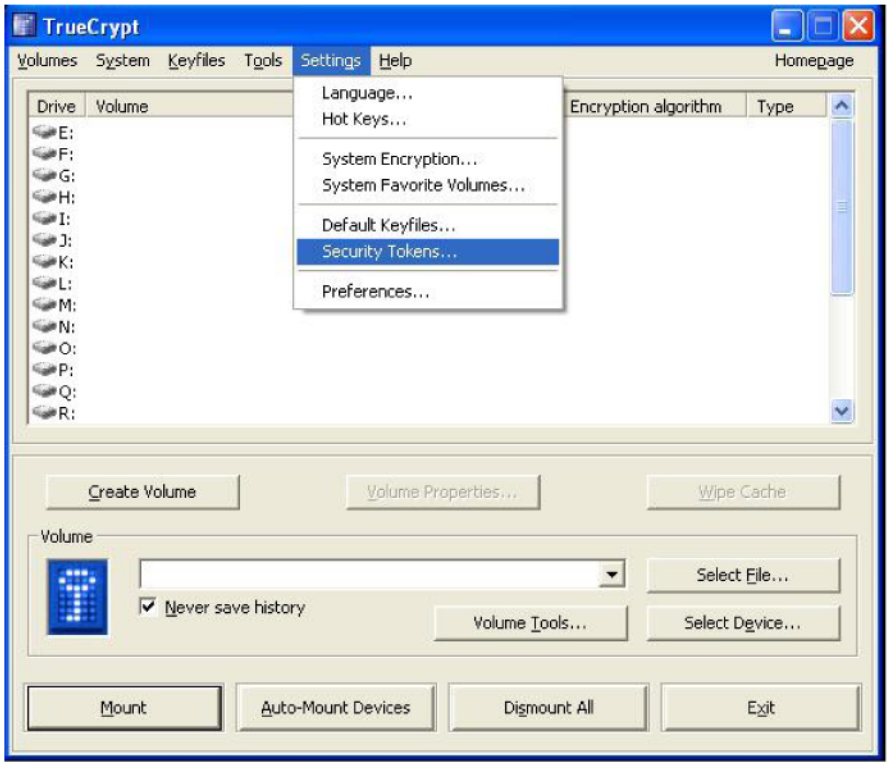


5 Como configurar un Dispositivo Criptográfico de Macroseguridad y la solución de TrueCrypt.org

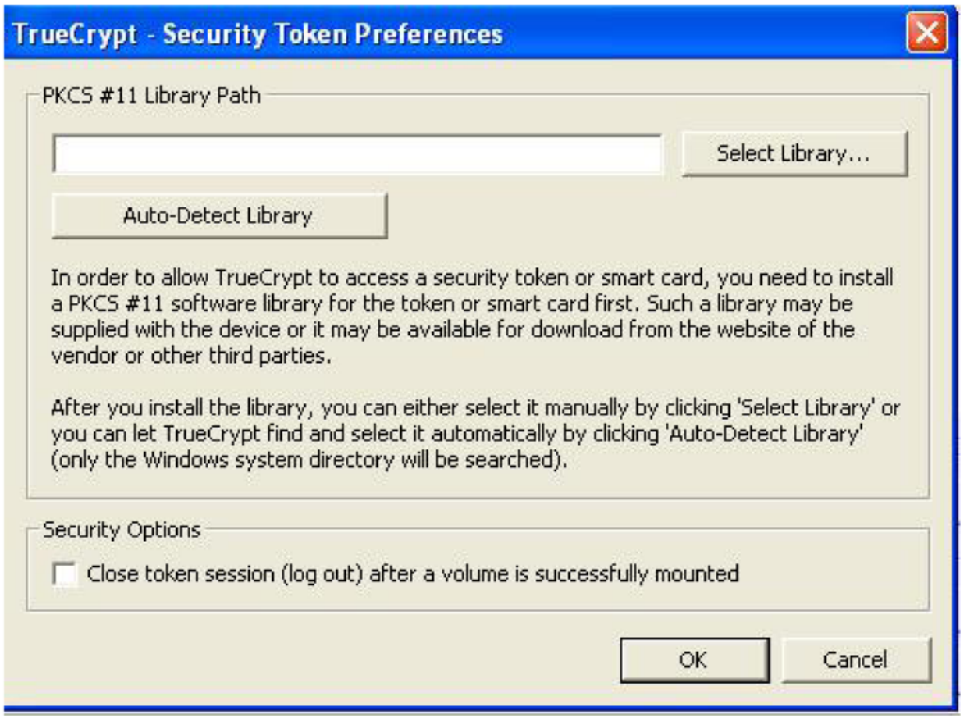
Por favor inicie el programa que se encuentra (por defecto) en *Inicio* > *Programas* > *TrueCrypt*



Haga click sobre "*Settings*" en el menú y luego sobre "*Security Tokens*"

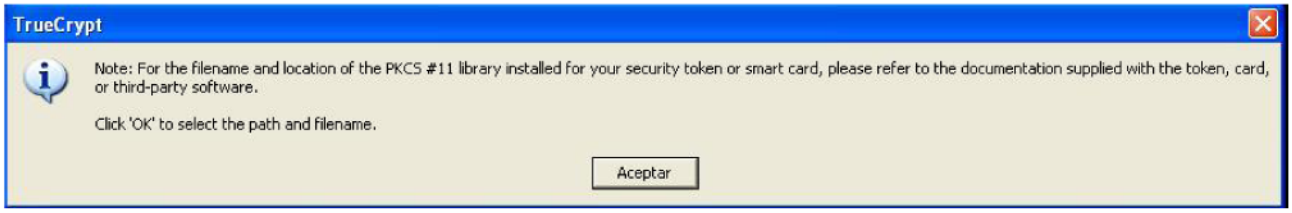


Se abrirá una ventana como la que se muestra a continuación.



Haga click sobre "*Select Library…*"

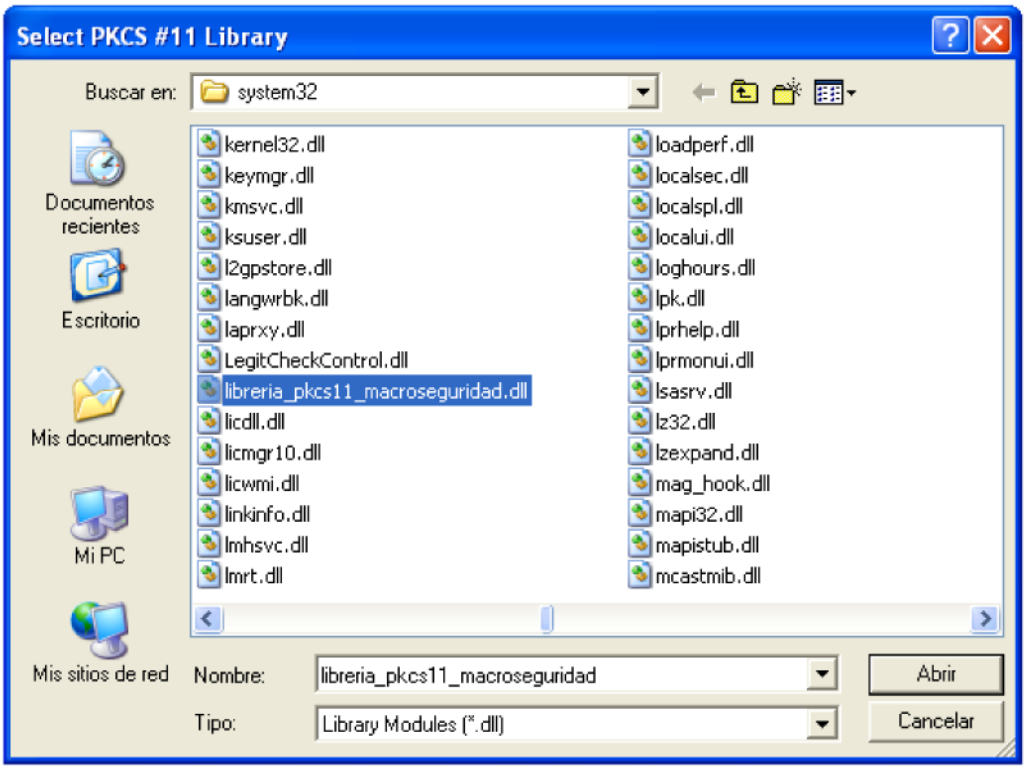
Se mostrará el siguiente mensaje. Haga click en "*Aceptar*" para continuar.



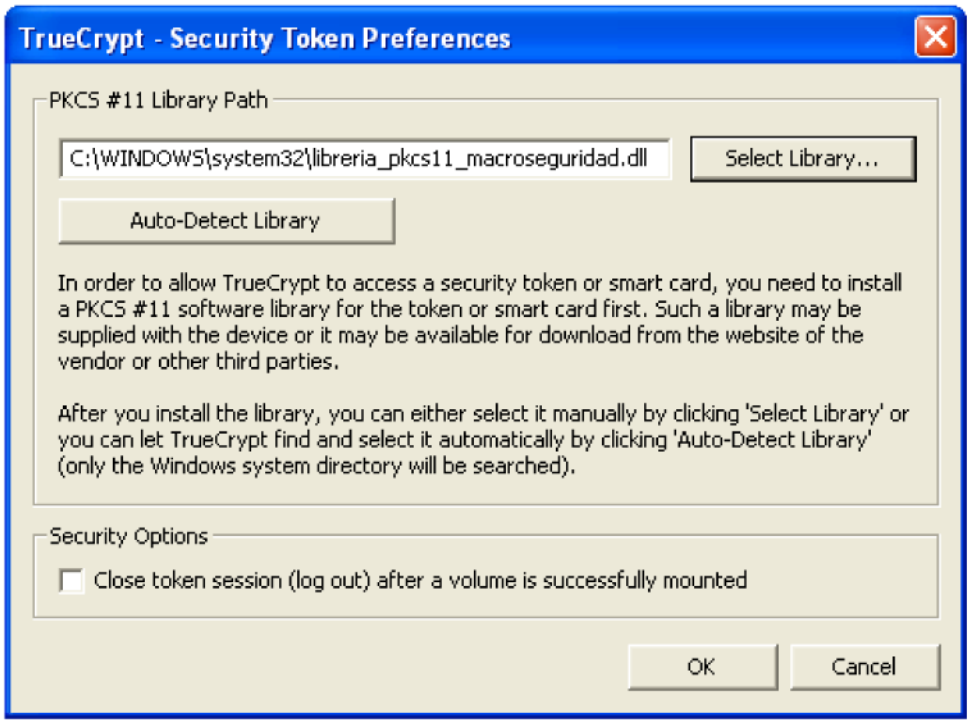
En este caso utilizaremos la libreria "*librería_pkcs11_macroseguridad.dll*" que se encuentra en la siguiente ubicación: [Unidad de Windows]:\Windows\system32\.

Refiérase al documento Compatibilidad_Token_USB_Macroseguridad-PKCS#11 para saber cual es la librería correspondiente a su Token USB / Smartcard (http://www.macroseguridad.net/soporte/docs/faqs_token.htm).

Seleccione la librería correspondiente y luego haga click en "Abrir"



Una vez que haya seleccionado la librería que soporta el estandar de PKCS#11 del Dispositivo Criptográfico de Macroseguridad, recomendamos activar el checkbox que se muestra en blanco en "*Security Options*" que refiere a "*close Token session (log out) after a volume is succesfully mounted*", para mayor seguridad. Esta opción cierra la sesion del Token USB / Smartcard luego de montada una unidad virtual de Truecrypt.



Luego haga click en "*OK*".

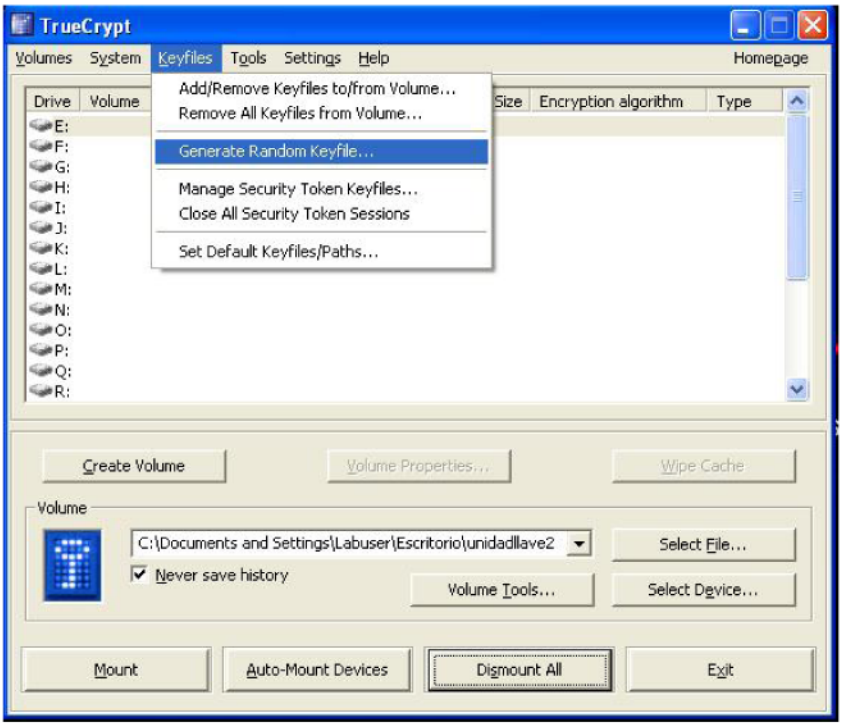
6 Integrar un Token USB / Smartcard de Macroseguridad mediante el uso de Keyfiles

6.1 ¿Qué es una Keyfile?

Para acceder a una unidad virtual, integrando un dispositivo criptográfico de Macroseguidad como un mecanismo de autenticación de doble factor, es necesario la utilización de una Keyfile (archivo de llave). Se puede usar una misma Keyfile para acceder a varias unidades, crear un Keyfile para cada una de esas unidades, usar varias Keyfiles (alojadas en distintos Tokens USB / Smartcard) para acceder a una unidad, etc. Existen múltiples opciones de trabajo junto con un Token USB / Smartcard de Macroseguridad.

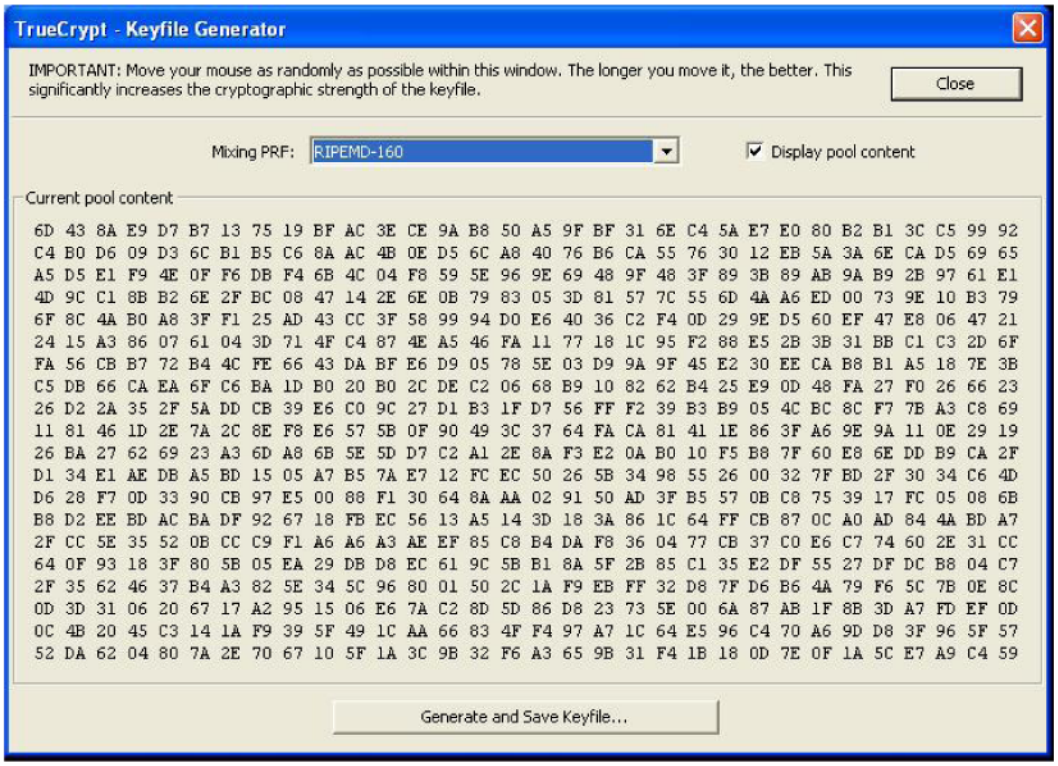
6.2 Utilizar un dispositivo criptográfico para crear y almacenar un keyfile en forma segura.

Para crear una Keyfile diríjase a la barra de herramientas y haga click sobre "*Keyfiles*" y luego en "*Generate Random Keyfiles*".



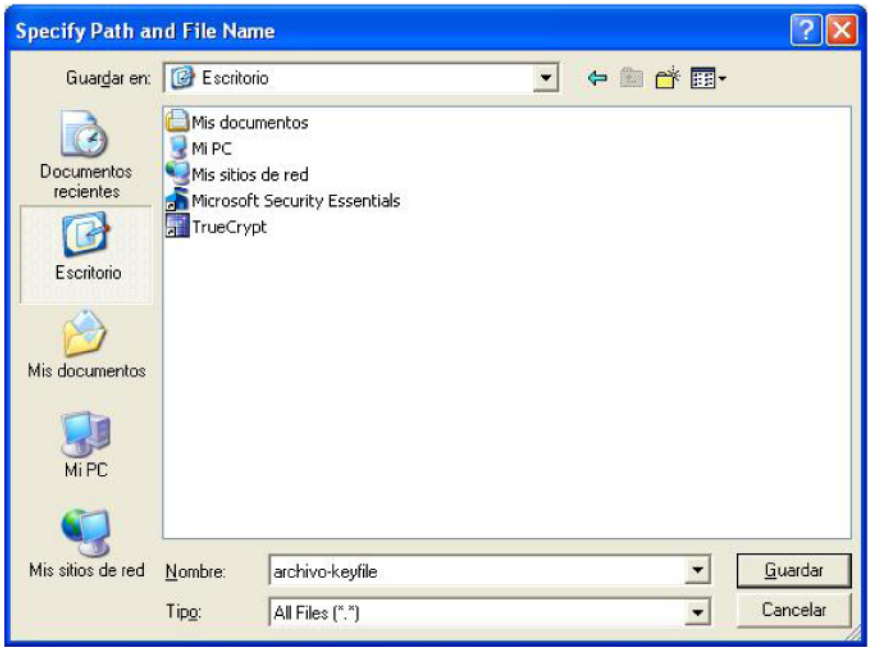
A continuación se muestra e informa como se generarán valores aleatorios para ser utilizados por el Truecrypt al momento de encriptar (optamos por los valores aleatorios del algoritmo "*RIPEMD-160*") y luego presionaremos "*Generate and Save Keyfiles*"

Existen otros algoritmos que pueden ser seleccionados, dependiendo de las preferencias de cada uno de los integradores que configuren el Truecrypt.



Podemos especificar donde guardar el keyfile y definir el nombre del mismo para tal fin (se recomienda que, después del almacenamiento de la clave en el Token USB / Smartcard (keyfile) y hecho un backup en un lugar seguro, se elimine del lugar que primeramente se había guardado).

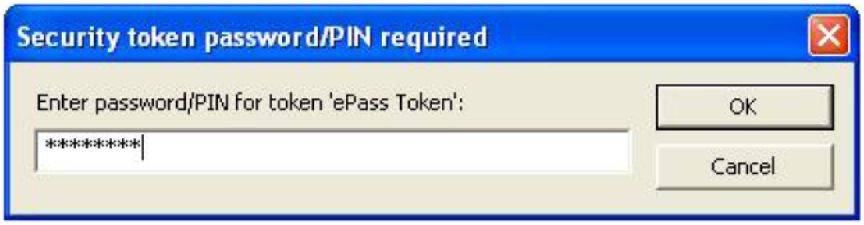
En este caso se ha optado por "*archivo-keyfile*" como nombre para el Keyfile. Note que la misma puede tener o no extensión.



Una vez terminado el proceso, haga click en "*Aceptar*" y vuelva a la ventana principal (haciendo click sobre "*close*").

Haga click sobre la barra de herramienta de Truecrypt en *Keyfiles > Manage Security Tokens Keyfiles.*

TrueCrypt le solicitará que se autentique al Token USB / Smartcard, en caso de que la sesión del mismo haya expirado (usted puede establecer la duración de la sesión mediante el parametro "*PIN Time Out*" de la herramienta de formateo.



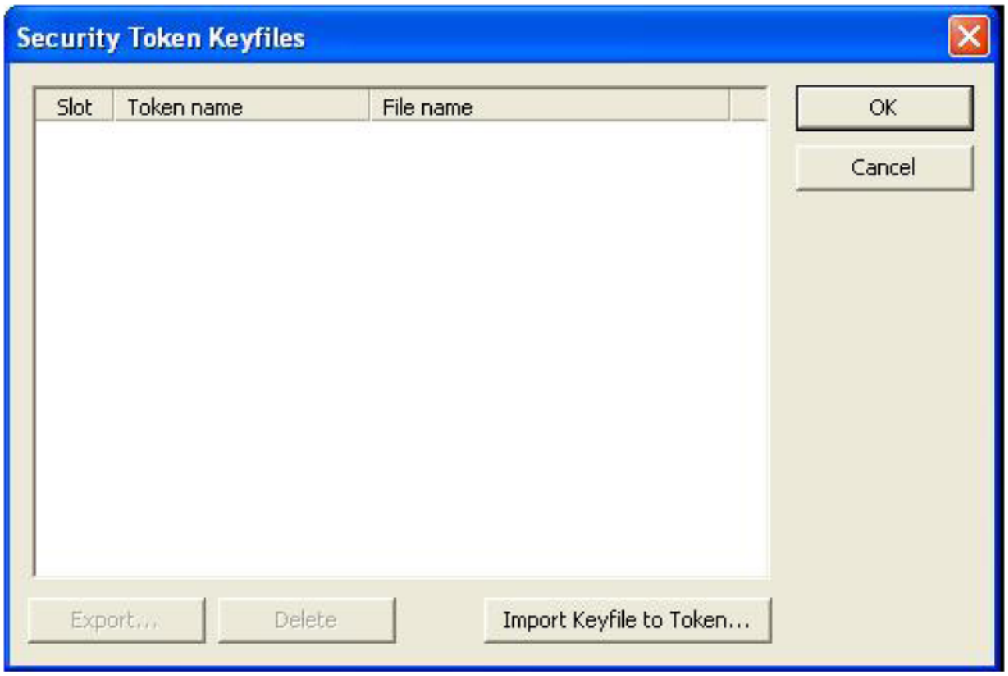
Si usted ingresa un PIN (o passowrd del Dispositivo Criptográfico de Macroseguridad) no válido, no le permitirá acceder a las Keyfiles a través del manager del TrueCrypt.

Al ingresar un PIN no valido la siguiente advertencia se mostrará.

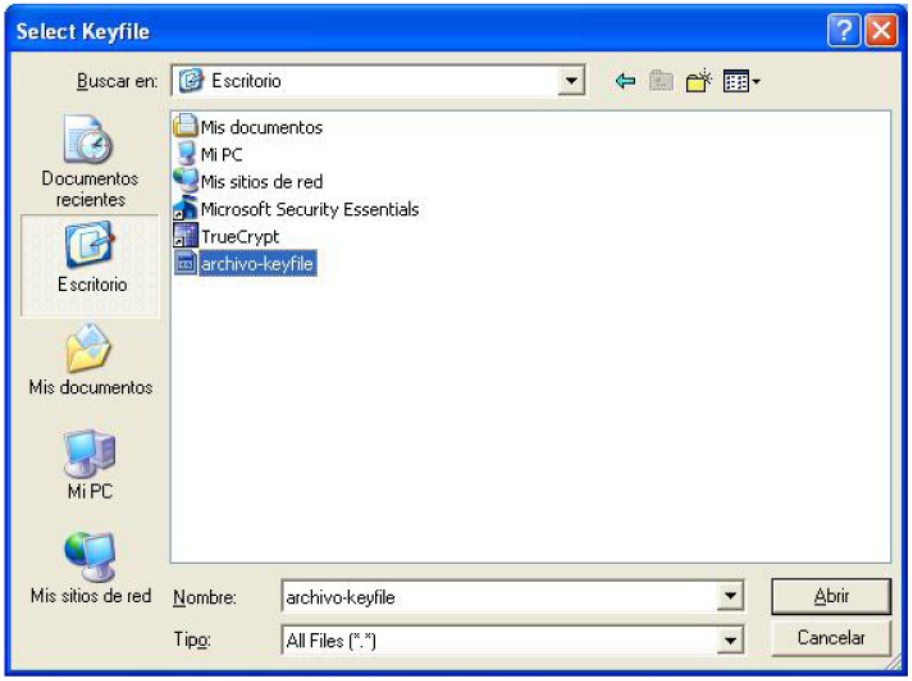
En caso de que usted agote la cantidad de reintentos permitidos, truecrypt le informará que el PIN de Usuario del Token USB / Smartcard se ha bloqueado.

Contacte al administrador de su red para poder desbloquearlo o refiérase a la guía de Formateo de su dispositivo. La cantidad de re-intentos establecida de fabrica es de diez intentos para el PIN de usuario y tres intentos para el SO PIN (Password del Administrador). **Tenga en cuenta que algunos dispositivos no permiten realizar un formateo del dispositivo si el SO PIN se encuentra bloqueado.**

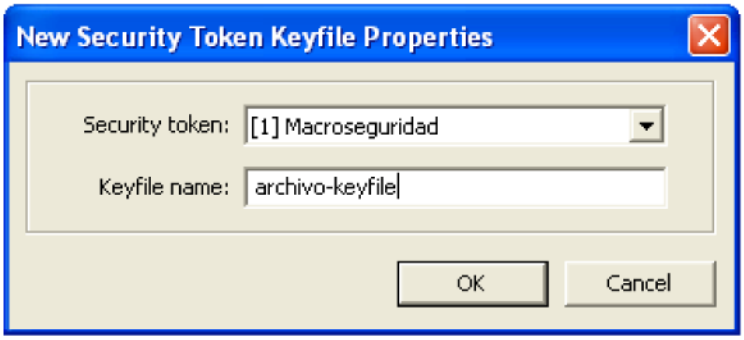
Luego se mostrará la siguiente ventana.



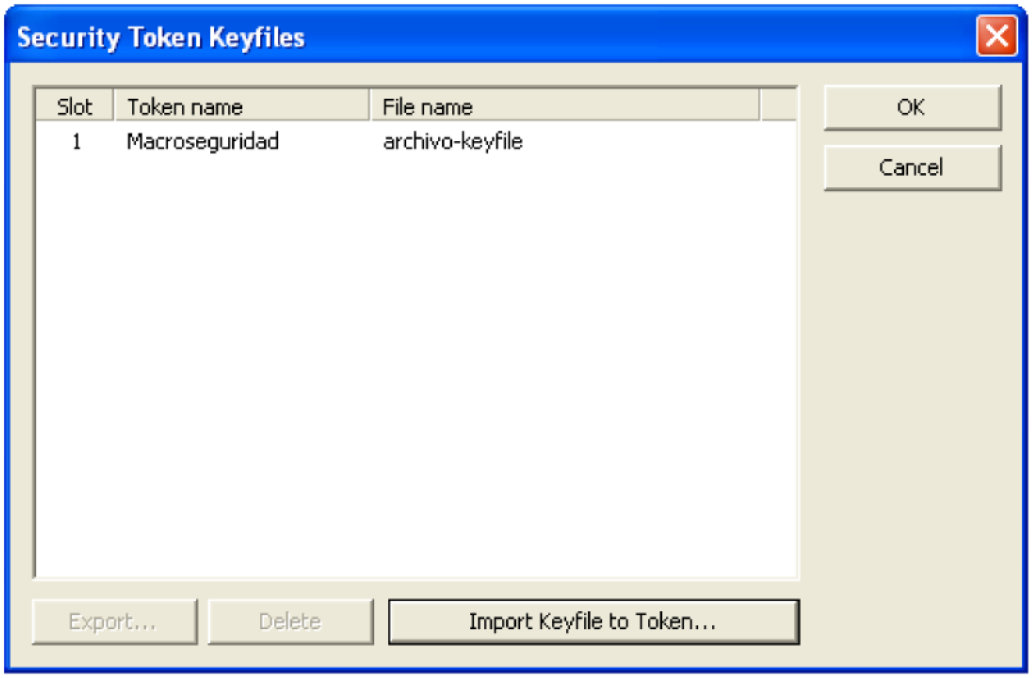
Para importar el archivo que anteriormente habiamos definido como llave a ser utilizada en los procesos de encriptación haga click sobre "*Import Keyfile to Token*".



Seleccione el archivo Keyfile (creado por Ud. en pasos anteriores) y haga click en "*Abrir*". Se mostará una ventana en la cual usted puede definir un nuevo nombre más descriptivo a ser utlizado por el manager (truecrypt). Le permite importar el keyfile y a su vez Ud. podra guardar el keyfile en más de un token / smartcard (si desease importar el mismo keyfile para que lo utilice mas de un usuario.) y le permitira también elegir el dispositivo criptográfico en el cual el usuario desea importar la llave.



Haga click en "*Ok*" y volverá a mostrarse la ventana anterior con la nueva llave dentro del dispositivo criptográfico de Macroseguridad.



Haga click en "*OK*" para volver a la ventana principal.

Si no una hay una política robusta de "*PIN Time Out*" por parte del administrador se recomienda siempre cerrar la sesión del Token/Smartcard.

Con el objeto de evitar puertas traseras en los sistemas, recomendamos armar una política para recupero de los Keyfiles, por ej. involucrando a más de un departamento "administración" + "marketing" + "recursos humanos". Reiteramos como se ha sugerido previamente, eliminar la Keyfile que esta almacenada en la PC una vez que fue almacenada en el Token USB / Smartcard de Macroseguridad.

En caso de querer hacer un backup de la clave (lo recomendamos), desde el manager del TrueCrypt, se podrá exportar.

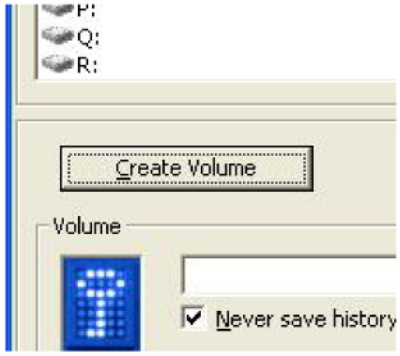
7 Integrar un Token USB / Smartcard con un archivo contenedor encriptado ("*Encrypted File Container*")

7.1 ¿Qué es un "Encrypted File Container"?

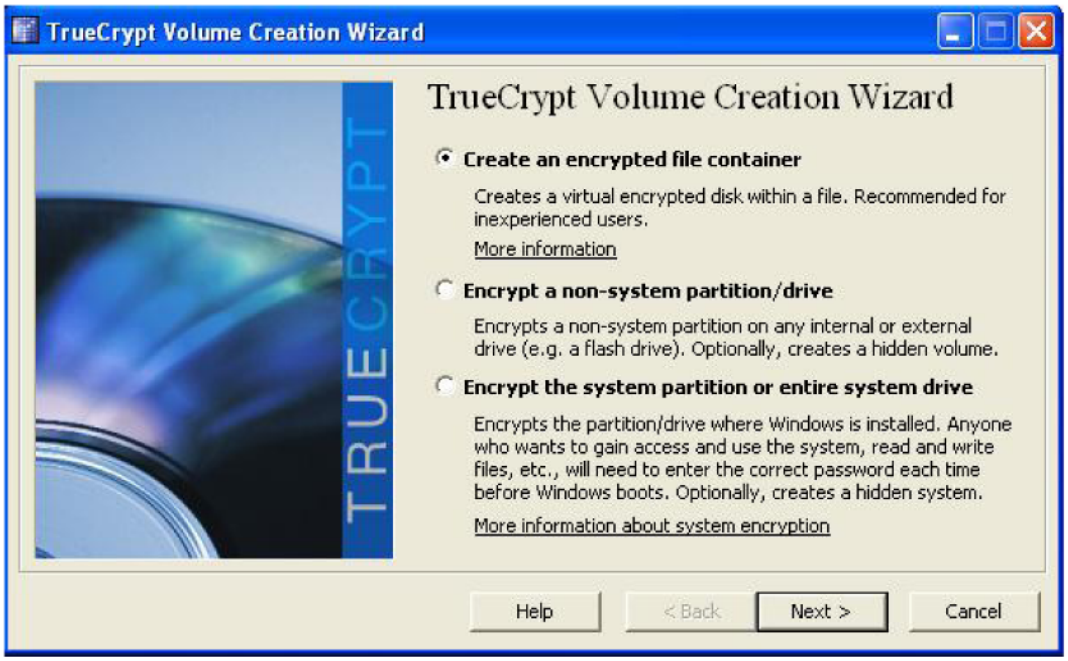
Es un archivo el cual TrueCrypt puede montar como una unidad de disco, con su identificación respectiva, según el sistema operativo utilizado. El contenido de ese archivo tiene su propio sistema de archivos y todo lo necesario para operar como una unidad común de almacenamiento. Lo que se grabe en esa unidad virtual se encriptando utilizando la tecnología y potencia de cifrado que el usuario seleccione. Cuando se "monta" la unidad a través de TrueCrypt, se pide la contraseña (Keyfile almacenada dentro del Token USB / Smartcard) que el usuario escogió al momento de crear este archivo.

7.2 Crear un "Encrypted File Container"

Haga click sobre "*Create Volume*".



Se abrirá una ventana como la siguiente.



Seleccione la primer opción "*Create an encrypted file container*" y haga click en "*Next*".

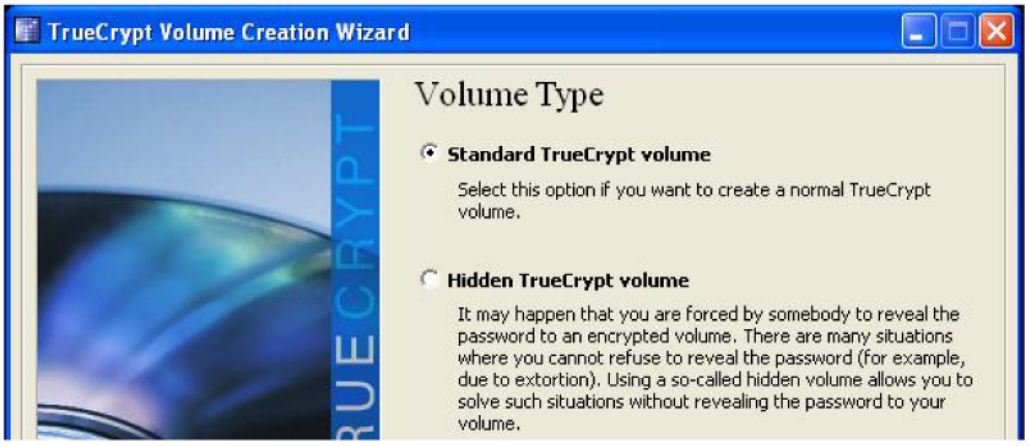
Luego nos permite elegir que tipo de volumen queremos crear.

1. La primera opción es un "*Standard TrueCrypt Volume*" y la segunda un "*Hidden TrueCrypt volumen*".

2. La segunda opción permite al usuario crear un sistema de volumenes con una unidad "oculta" donde se puede guardar información sensible la cual debe ser resguardada, y otra "visible" para el almacenamiento de información menos importante.

Ambos volúmenes se encriptan de la misma manera pero la diferencia radica en que si a un usuario lo obligan a desencriptar su unidad por la fuerza, el mismo puede descriptar el volumen "visible" engañando así al perpetrador y resguardando la información importante.

En esta guía se detallará como crear un volumen estandar. Para ello seleccione "*Standard TrueCrypt Volume*", luego haga click en "*Next*".



En la siguiente ventana haga click en "*Select file…*". Deberá seleccionar el nombre y la ubicación del archivo que luego será montado como una unidad virtual (será reconocido como un disco rigido o unidad de red). Para terminar haga click sobre "*Guardar*". Volverá a la pantalla anterior. Haga click en "*Next*".

Seleccione el Algoritmo que desea utilizar para la Encripción. Se recomienda la utilización del Algoritmo "*AES*" por ser el más rápido y confiable (si desea hacer una prueba de velocidad de los diferentes algoritmos haga click en "*Benchmark*"). Luego haga click en "*Next*" para continuar.

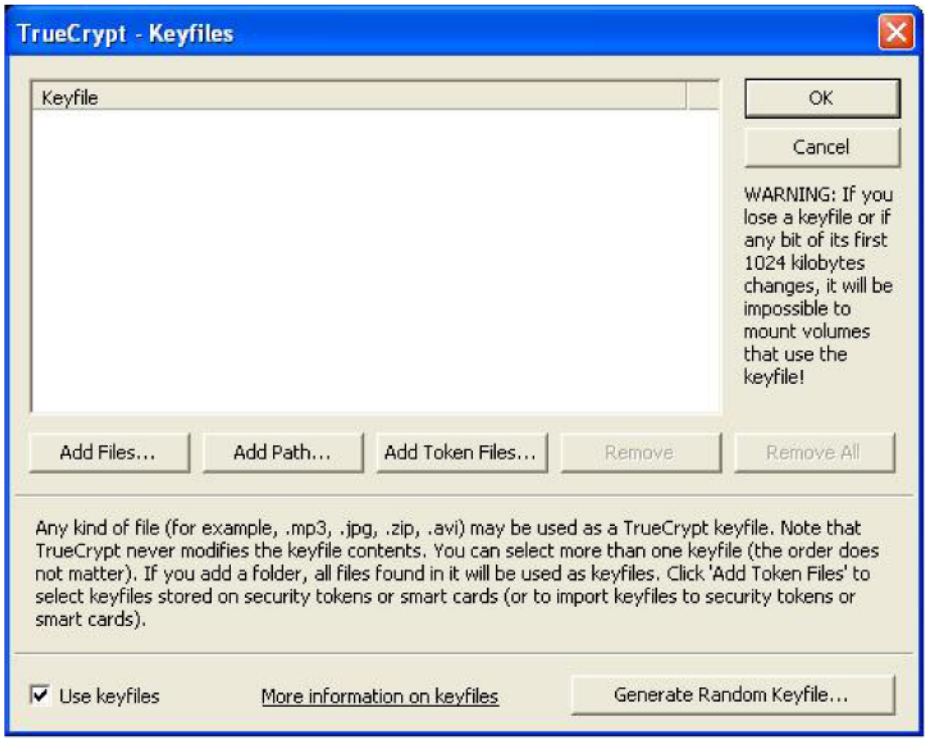
Luego deberá seleccionar el tamaño que tendrá el volumen.

Una vez configurado el tamaño deberá establecer la forma de autentificación del volumen, utilizaremos un Keyfile que fue almacenado dentro de un Dispositivo Criptográfico de Macroseguridad como se mostró en pasos anteriores. Es la mejor opción ya que

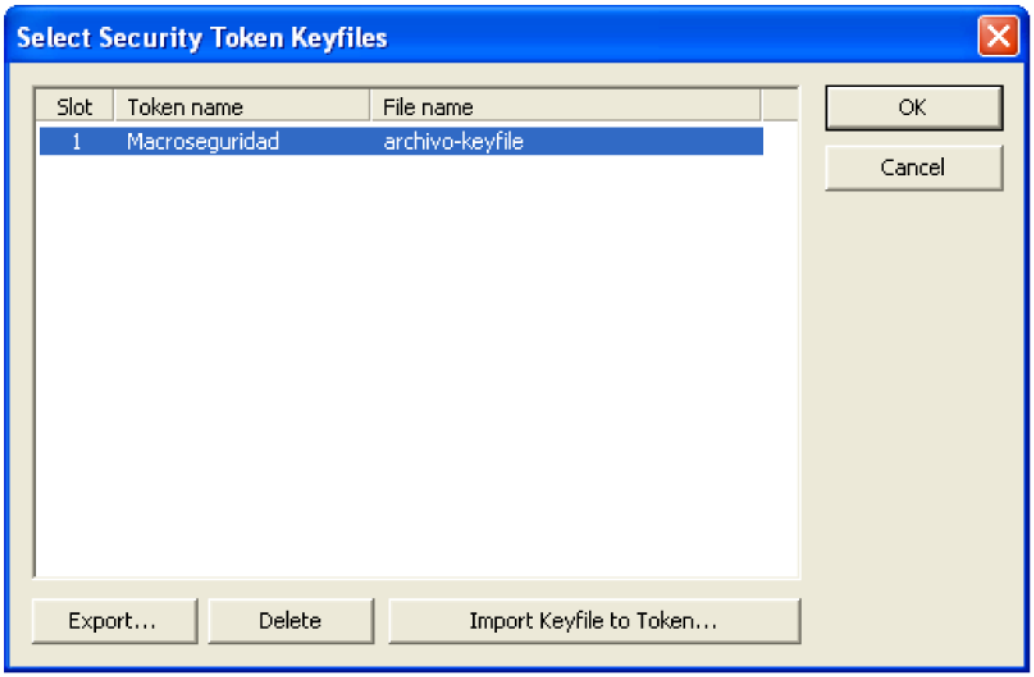
gracias a los robustos estándares de Macroseguridad, el Keyfile permacerá segura y solo el usuario podrá acceder a la información del volumen.

Seleccione el checkbox "*Use Keyfiles".* Luego haga click sobre "*Keyfiles..*"

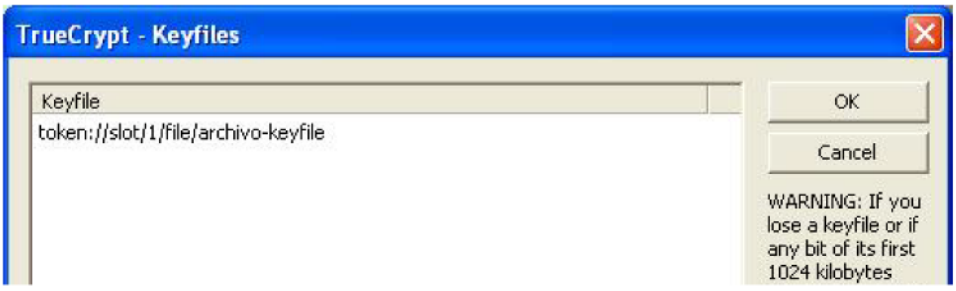
La siguiente ventana se abrirá, permitiendo adicionar keyfiles almacenados en dispositivos criptográficos como son los de Macroseguridad. Haga click sobre "*Add Token Files*". (En caso que por el "*PIN Time Out*" la sesión del Token haya expirado, o no haya iniciado nunca sesión, se le solicitará al usuario que se autentique al mismo).



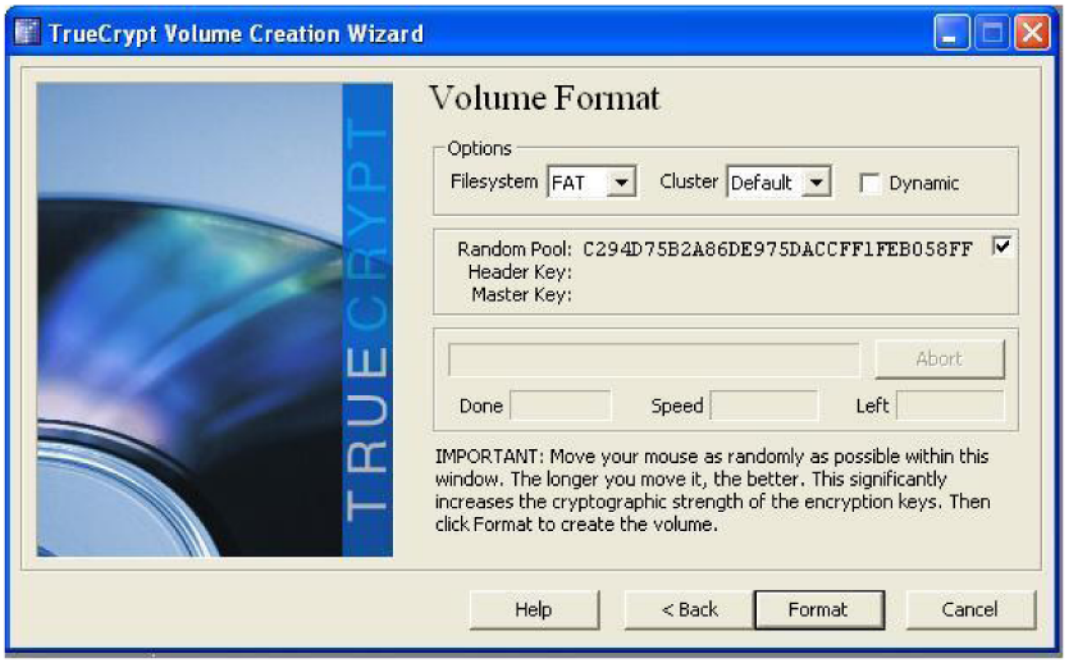
Luego se mostrará la siguiente ventana:



Seleccione el archivo Keyfile a utilizar y luego haga click en "*OK*". También tiene la posibilidad de importar un nuevo keyfile al Token USB / Smartcard. La Keyfile se mostrará listada. Haga click en "*OK*" para volver al asistente de creación.

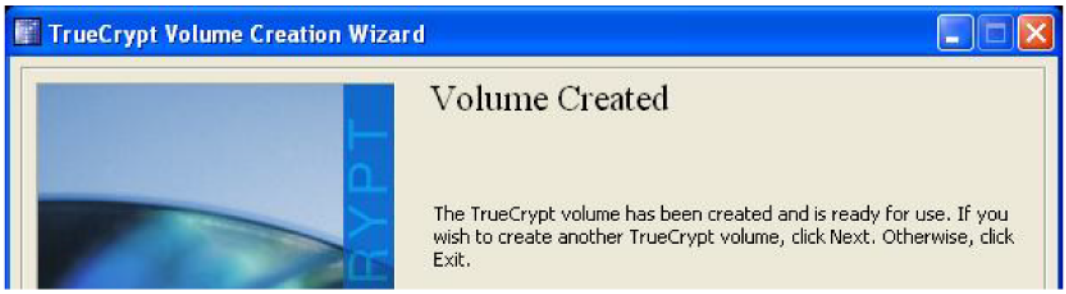


En la siguiente ventana se mostrarán los parámetros del volumen a crear, seleccione sus preferencias y luego haga click en "*Format*"



Al finalizar la creación se le notificará que la misma fue exitosa.:

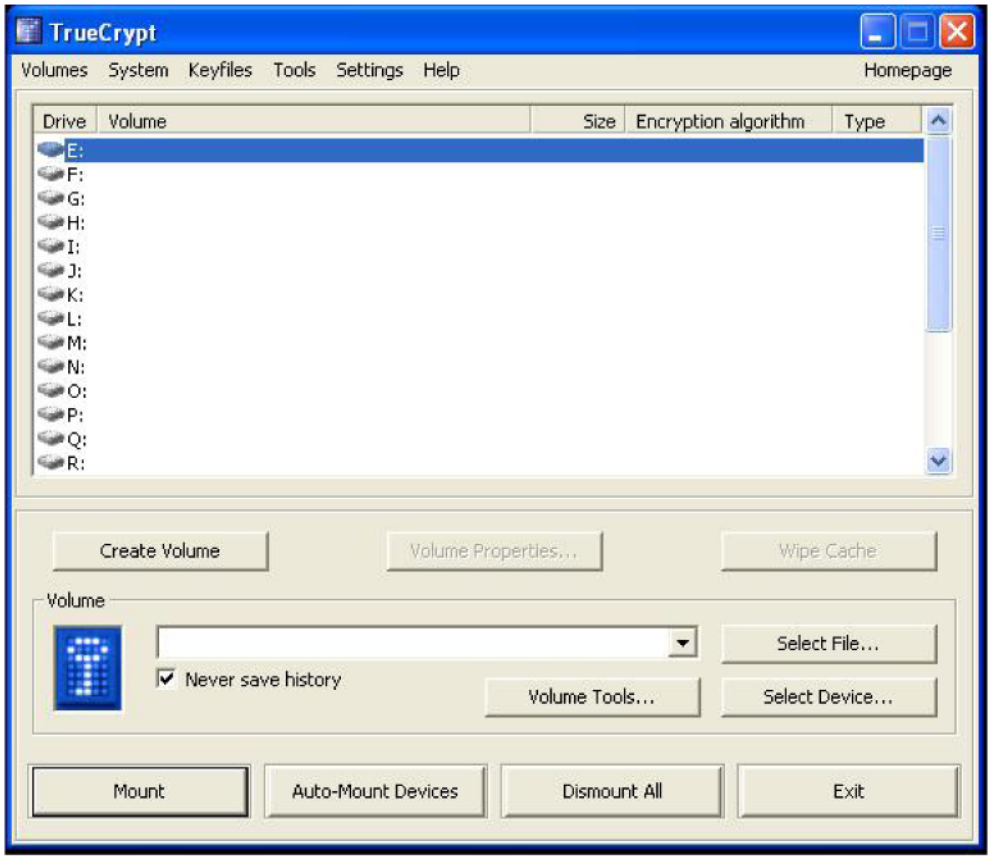
Luego de hacer click en “Aceptar” la siguiente ventana se abrirá:



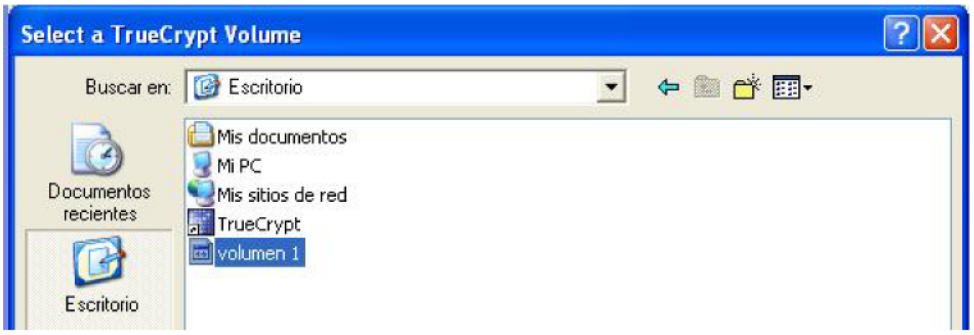
Haga click sobre “*Next*” en caso de querer crear otro volumen o “*Exit*” para salir.

7.3 Como montar un "*Encrypted File Container*" *con* un Keyfile almacenado en Dispositivo Criptográfico de Macroseguridad

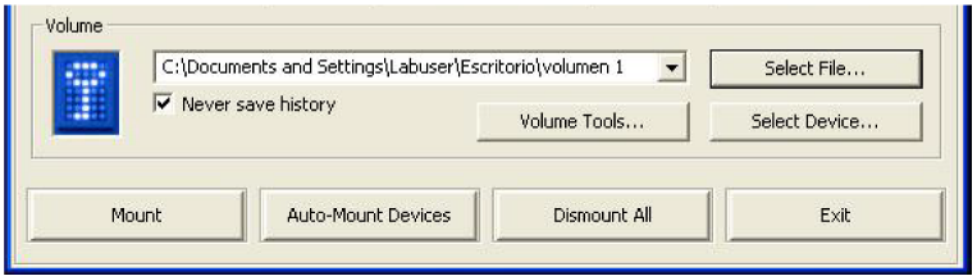
Inicie la aplicación TrueCrypt. Seleccione una letra disponible de la lista (por ejemplo en este caso "E:") y haga click sobre "*Select File*". Se mostrarán únicamente la letras no tomadas por dispositivos presentes en la PC (Por ejemplo un disco duro o una lectora).



En la siguiente ventana debemos localizar y seleccionar el archivo contenedor que deseemos montar.



Haga click en "*Abrir*". Se mostrará nuevamente la ventana anterior. Note que ahora en la parte inferior se encuentra la ruta al volumen a ser montado.

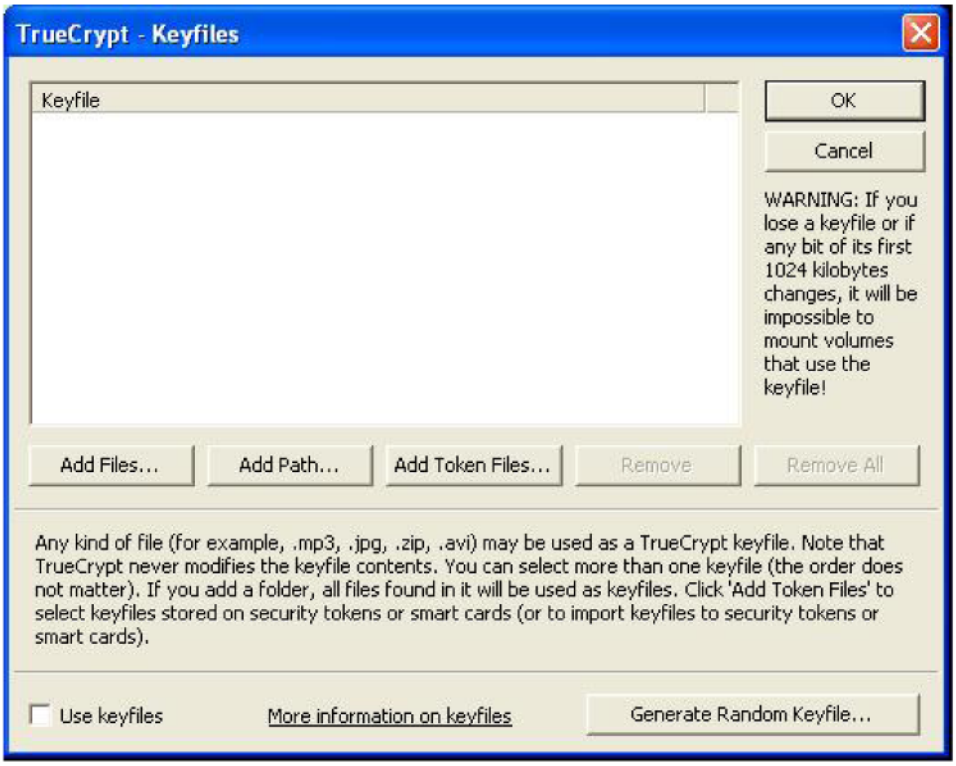


Ahora haga click en "*Mount*" para cargar el volumen seleccionado.

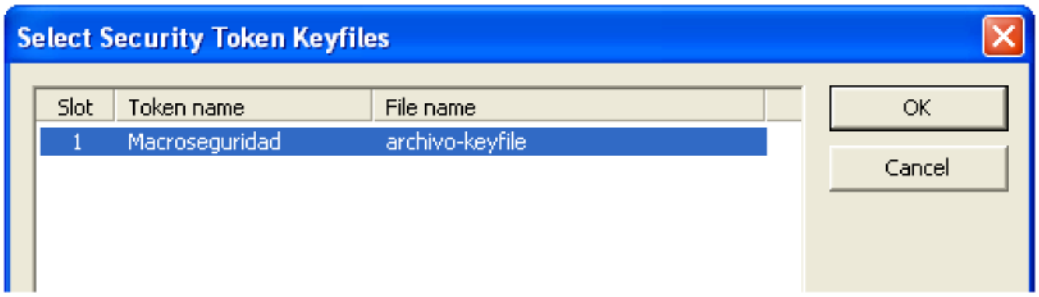
La siguiente ventana le solicitará que seleccione el mecanismo de autenticación del volumen.

El volumen se encuentra protegido por un keyfile y el mismo se encuentra almacenada/s en un Token USB / Smartcard para obtener la mayor seguridad y confiabilidad que brindan las robustas características de los mismo. Haga click en "*Keyfiles*".

Luego haga click en "*Add Token Files*" (si el "*PIN Time Out*" del dispositivo criptográfico ha expirado, o no se ha iniciado la sesión, se le requerirá al usuario que se autentique frente al mismo).



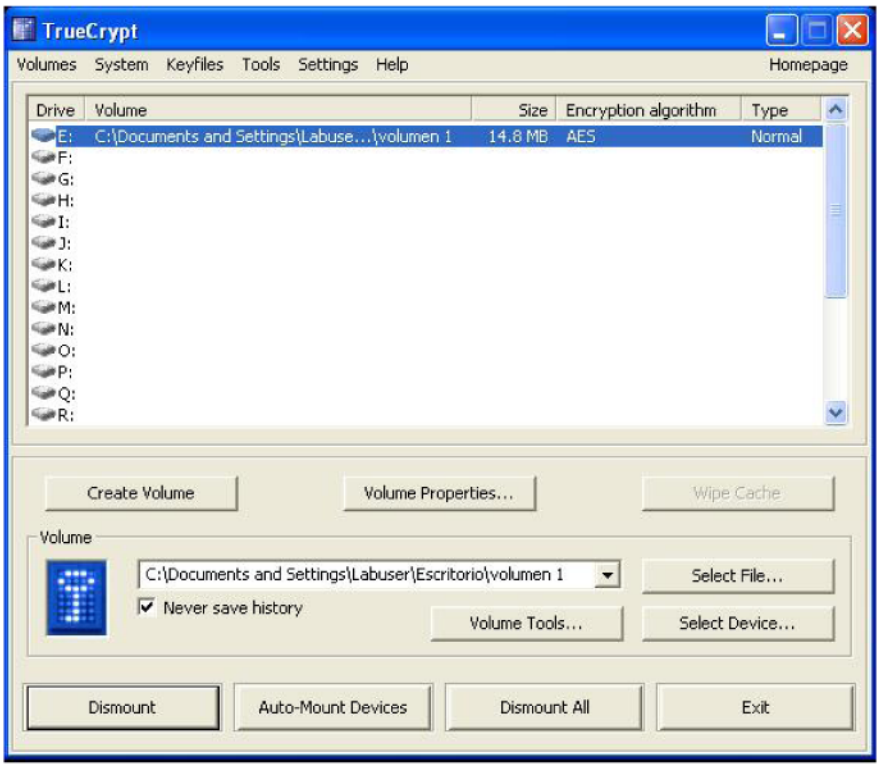
Ahora seleccione la llave que desea utilizar y luego haga click sobre *"OK"*.



(En caso de que se requiera seleccionar mas llaves se deberá repetir el paso anterior)

Luego haga click en "*OK*" y en la siguiente ventana haga click en "*OK*".

Como se muestra en las dos imágenes siguientes el dispositivo quedará montado correctamente.



Los Keyfiles se pueden establecer como predeterminadas. Esto quiere decir que el TrueCrypt automáticamente (si su ubicación esta disponible) las utilizará en todos los procesos de autenticación.

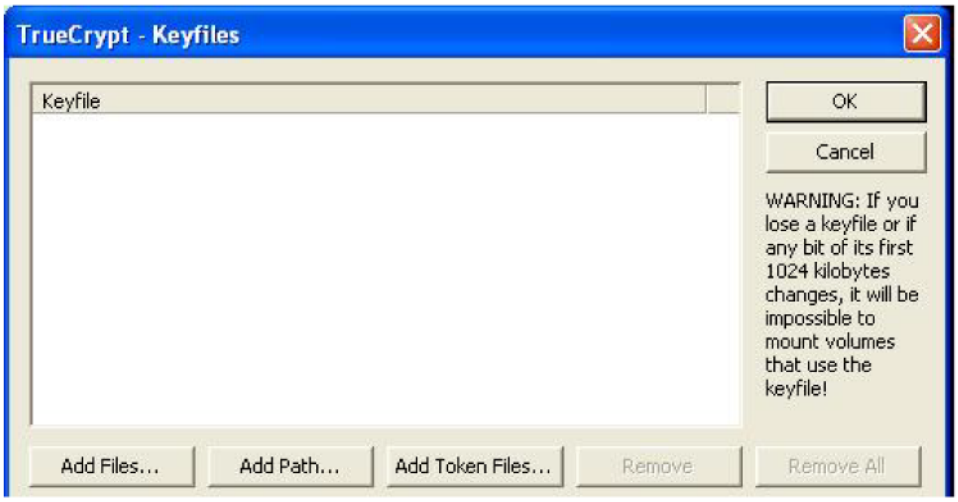
Si el o los Keyfiles que sirven para autenticarse ante un volumen estan establecidas como predeterminadas el usuario solo deberá hacer click sobre "*Mount*" para que se monte la unidad virtual (el proceso se ejecutará de manera automática).

En caso contrario, si requiere utilizar otro Keyfile también deberá hacer click en "*Mount*" pero se le desplegará una ventana de selección de password/keyfile y deberá seleccionar solamente la Keyfile restante.

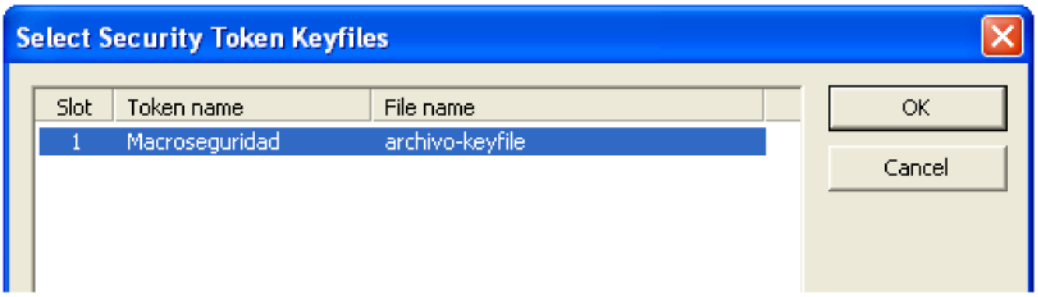
Nota: La opción de auto-mount devices es solo para montar dispositivos como son las memoria flash

Para esto haga click, en la barra de herramientas, sobre "*Keyfiles*" y luego en "*Set Default Keyfiles/Paths…*"

Ahora haga click donde dice "*Add Token Files*" (En caso de que la sesión del token haya expirado por una política de "*PIN Time Out*", o no haya iniciado sesión, se le requerirá al usuario que se autentique frente al Token USB / Smartcard).



El usuario deberá seleccionar el keyfile a establecer por defecto.



Se mostrará una advertencia, haga click en "*Sí*".

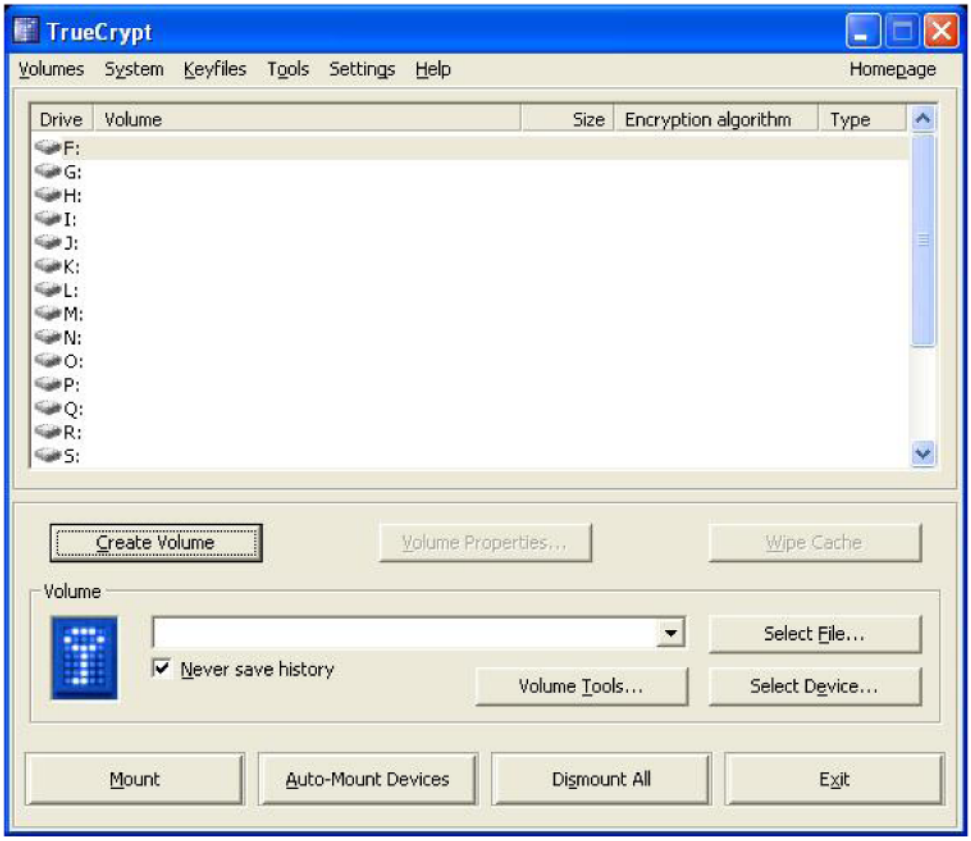
Ahora cuando quiera montar el volumen solo deberá hacer click sobre "*Mount*" y se montara automáticamente mediante la Keyfile almacenada en el Dispositivo Criptográfico de Macroseguirdad.

.

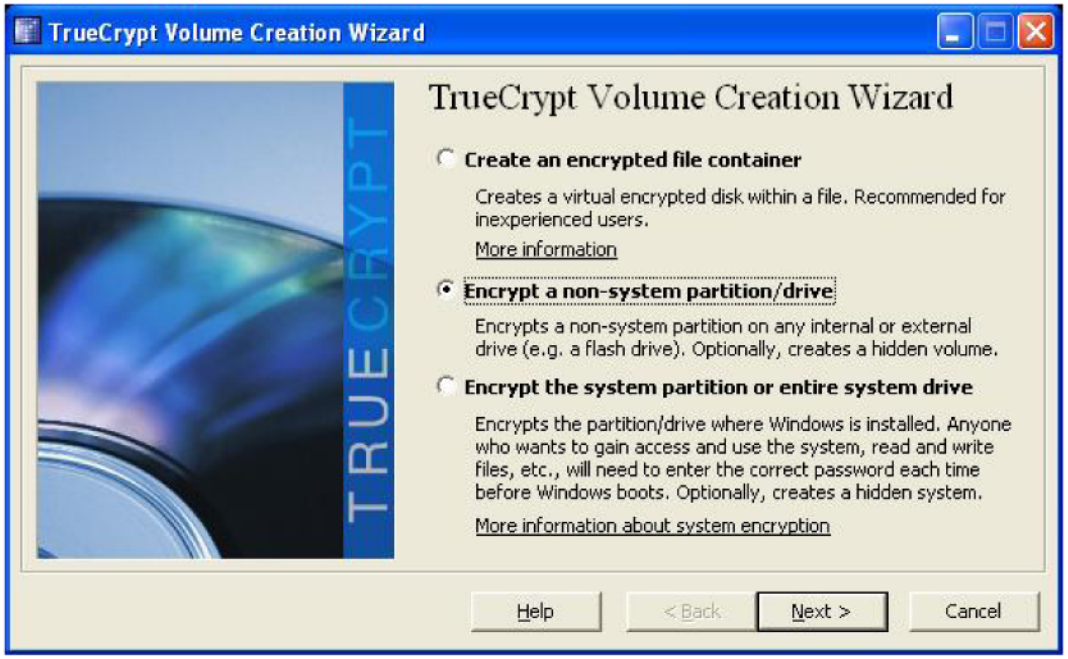
8 Integrar un Dispositivo Criptográfico para encriptar una partición o dispositivo.

8.1 Encriptar una partición ajena al sistema (*non-system partition*) o un dispositivo de almacenamiento masivo.

Haga click sobre "*Create Volume*"

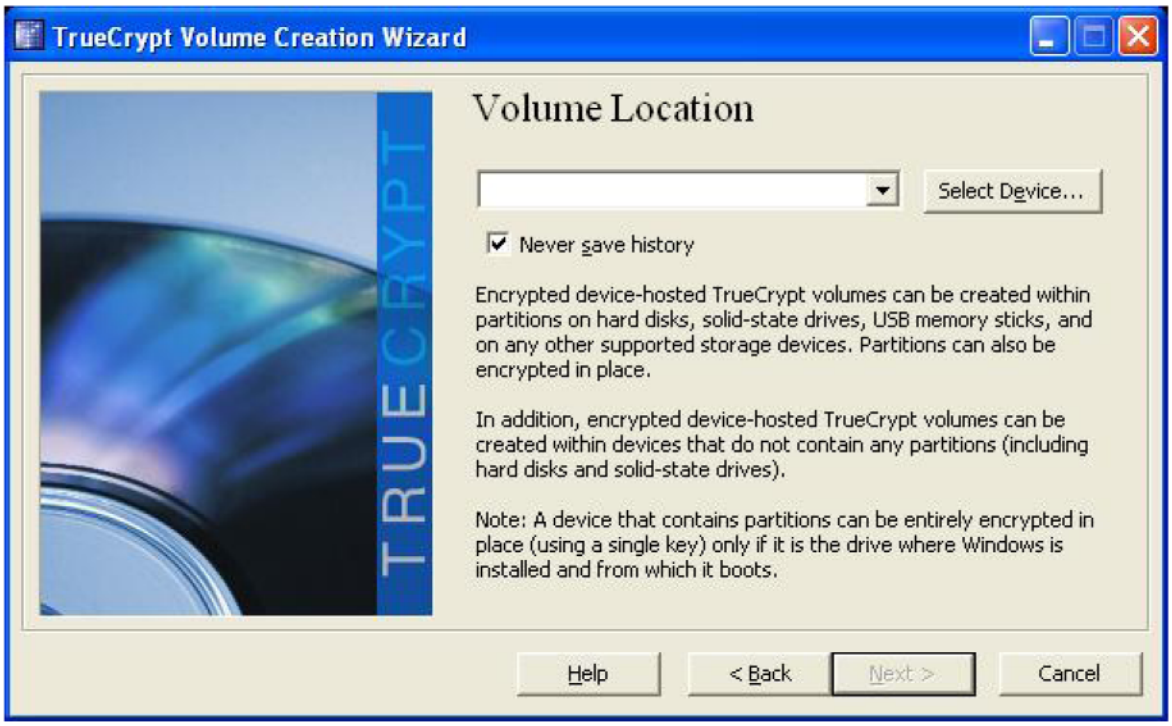


A continuación haga click sobre "*Encrypt a non-system partition/drive*" y luego en "*Next*".



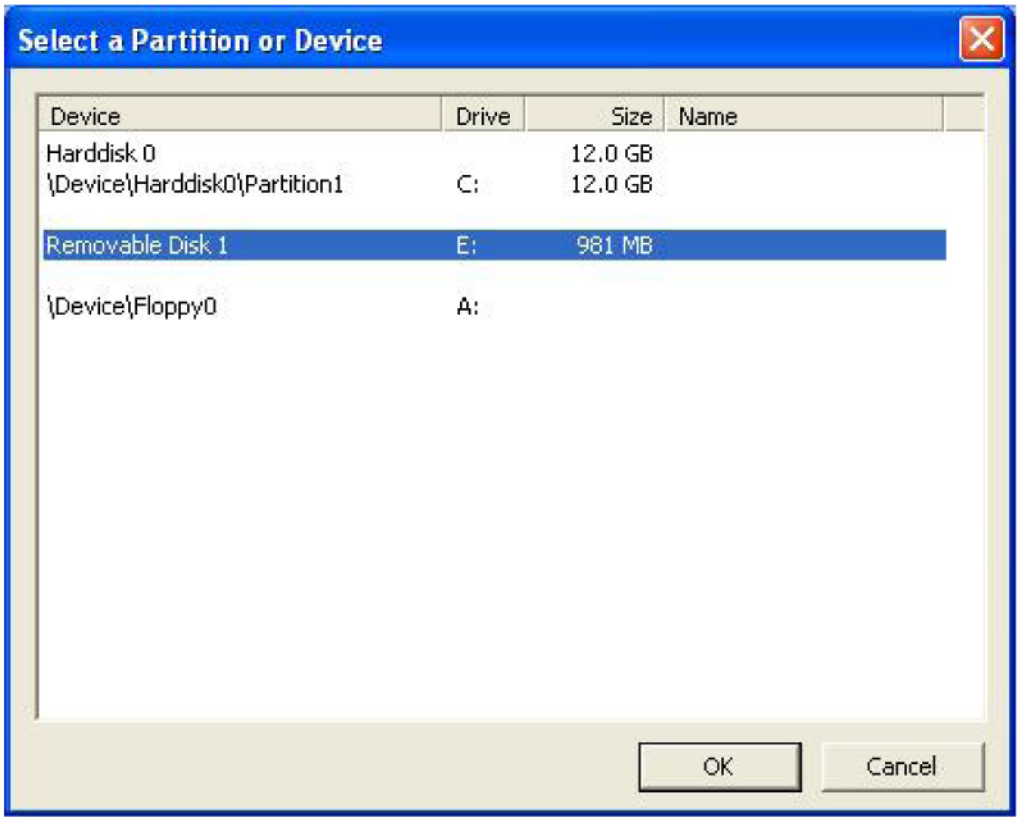
En la siguiente ventana seleccione el tipo de volumen que desea crear, en este caso seleccionaremos "*Standard TrueCrypt volumen*". Luego haga click en "*Next*".

Ahora seleccione haciendo click en "*Select Device…*" la partición o dispositivo que desea encriptar.



Una vez que la partición/dispositivo ha sido encriptado la única forma de desencriptarlo es el formateo del mismo. Se recomienda realizar la encriptación en una partición o dispositivo sin contenido.

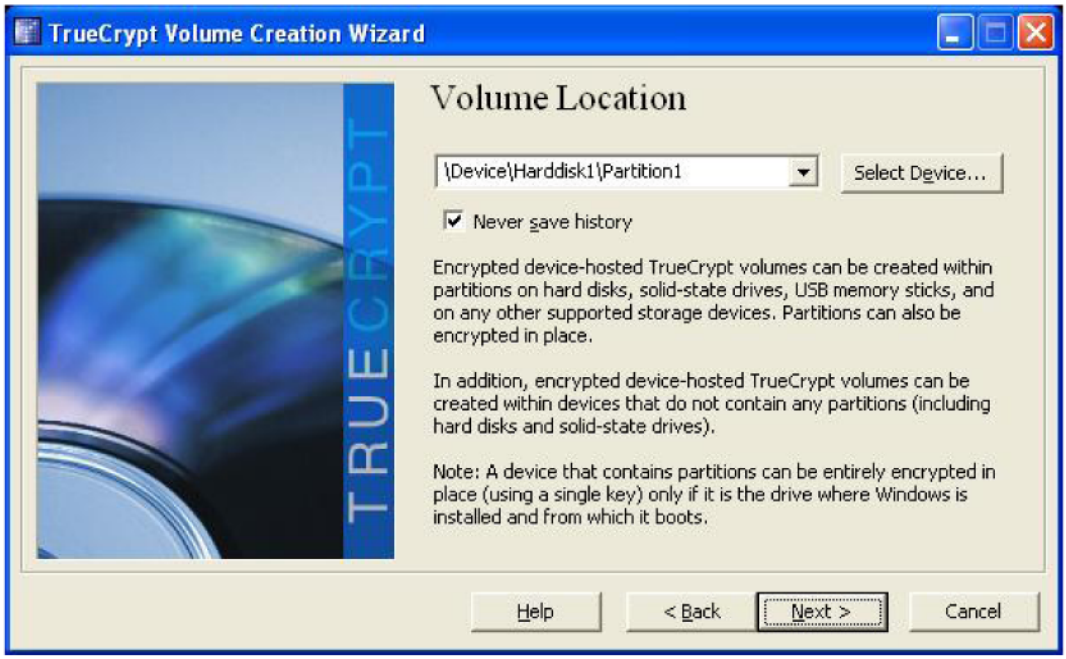
A modo de ejemplo en esta guia utilizaremos una memoria Flash USB. Luego haga click en "*OK*".



El siguiente mensaje de advertencia se mostrará:

(En el mismo se advierten los riesgos de encriptar un dispositivo. Luego de leerlo haga click en "*Sí*" en caso de querer continuar o "*No*" en caso contrario, al seleccionar "*No*" se cancela la encripción.)

Para continuar haga click en "*Sí*" y luego en "*Next*" para avanzar con el proceso de encripción.

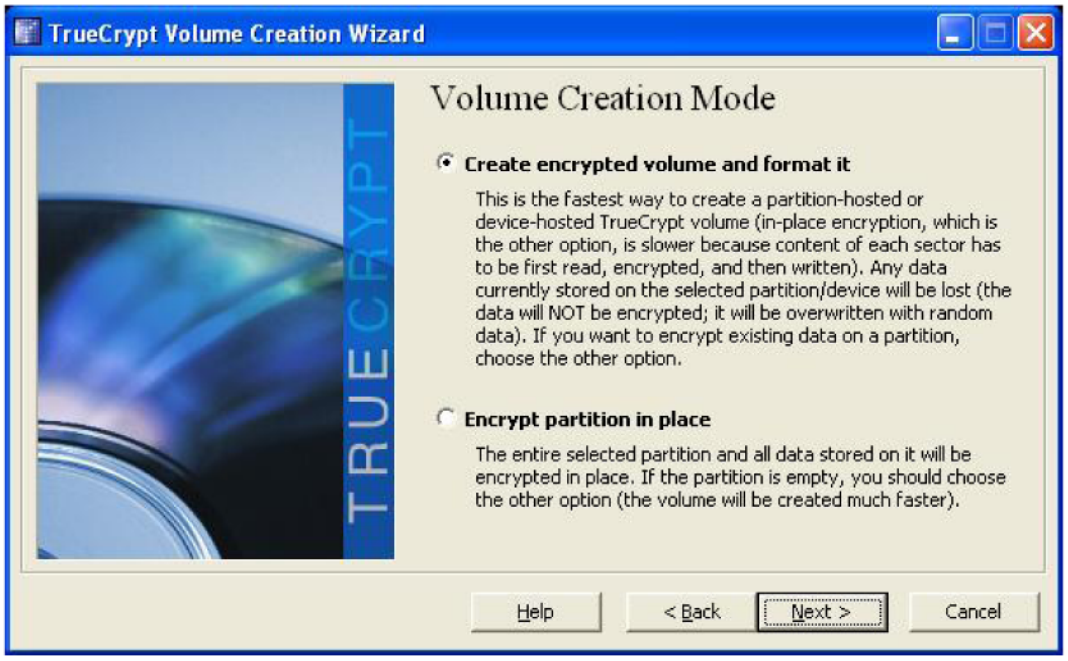


Preguntará si prefiere que se formatee previamente la partición/dispositivo y luego pase a encriptarse o que se encripte el dispositivo con toda la información que el mismo pueda contener.

La segunda opción es más lenta que la primera y para poder utilizarla es necesario poseer como sistema operativo Windows Vista o superior.

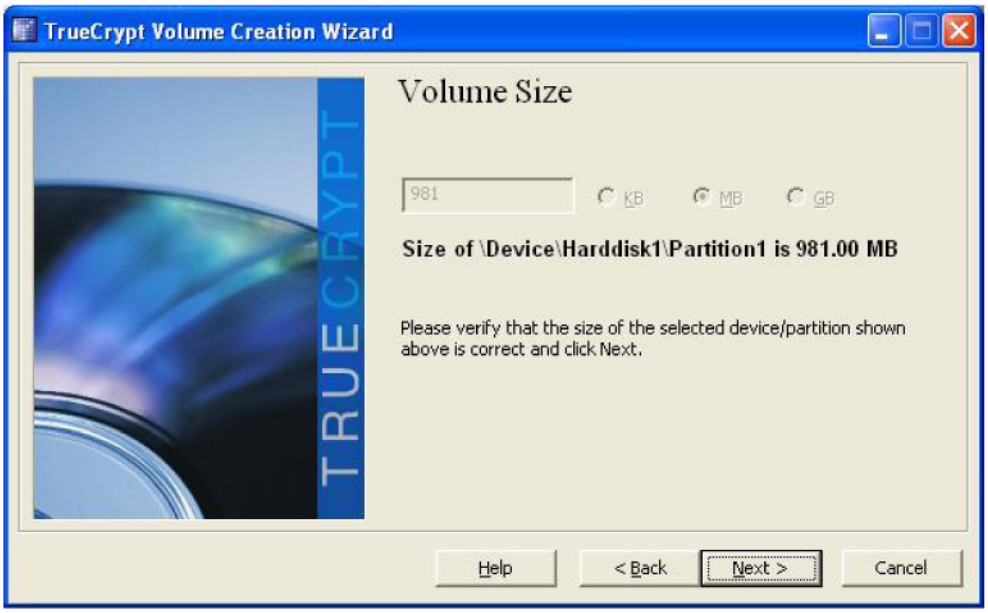
En el ejemplo que se usa en esta guia se utiliza la primer opción.

Luego haga click en "*Next*".



A continuación le requerirá que seleccione el Algoritmo de Encripción y de Hash. (En el ejemplo se utilizan los Algoritmos por defecto por ser los más eficientes). Haga click en "*Next*" para continuar.

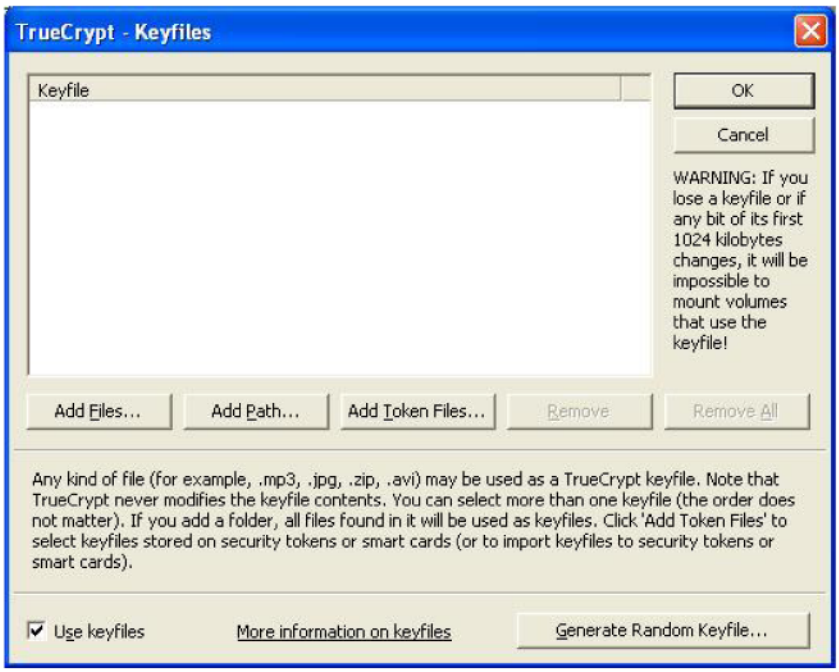
Luego en la siguiente ventana le mostrará al usuario el tamaño del volumen a encriptar. Verifique que los datos sean los correctos. Si lo son haga click en "*Next*" para continuar.



Ahora deberá seleccionar el Keyfile que usted tiene almacenado en su Dispositivo Criptográfico de Macroseguridad, con todos los beneficios de seguridad que este le brinda, como clave para la unidad que esta siendo encriptada.

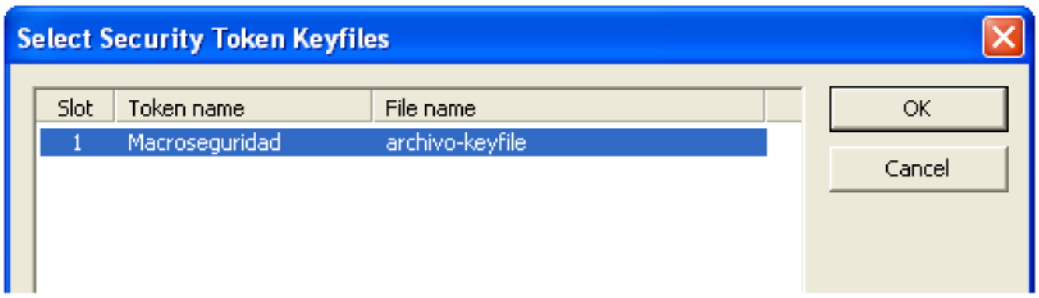
Para lograr esto haga click sobre el checkbox "*Use Keyfiles*" y luego sobre "*Keyfiles…*".

A continuación haga click sobre "*Add Token Files…*":



En caso de que usted no se haya autentificado al Token USB / Smartcard o que la sesión del mismo haya expirado usted deberá escribir el PIN del dispositivo para acceder a la información contenida en el mismo.

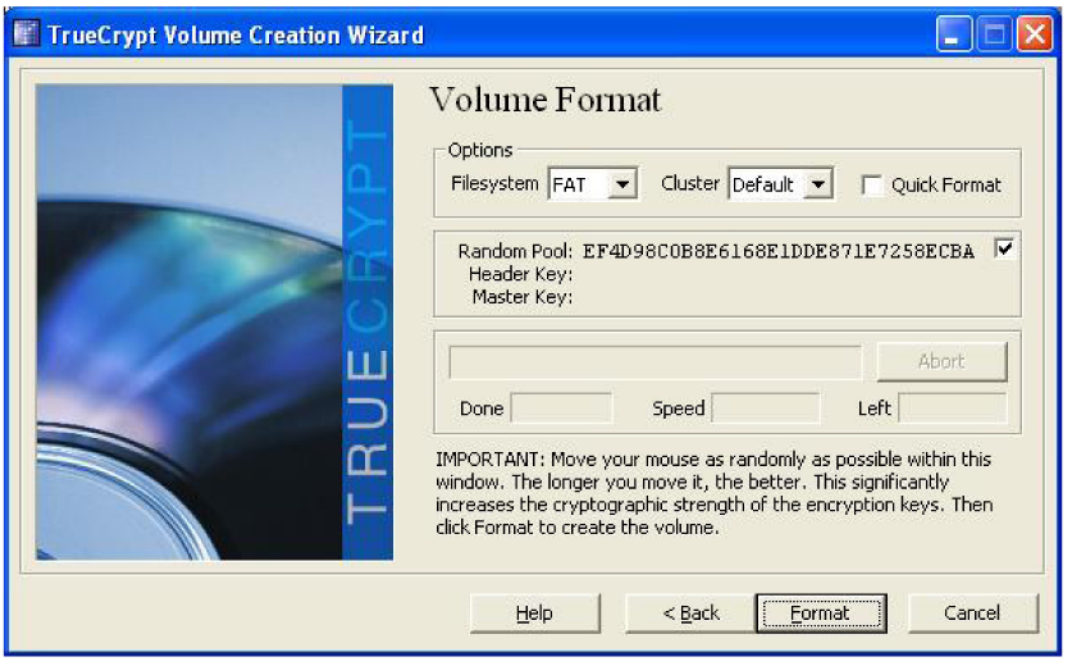
Ahora seleccione la Keyfile que desea establecer y luego presione "*OK*".



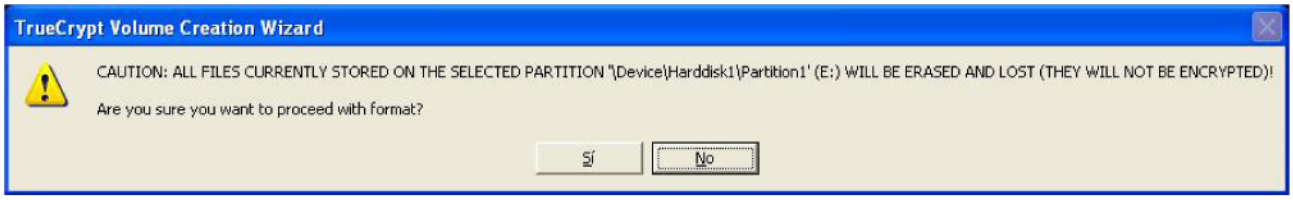
Luego volverá a la ventana anterior donde, en caso de que quiera establecer otra/s Keyfile/s adicionales, podrá hacerlo, realizando el mismo procedimiento anteriormente descripto.

Al terminar la elección de los Keyfiles necesarios para la autenticación haga click en "*OK*". Al volver a la ventana anterior haga click en "*Next*" para seguir con el proceso.

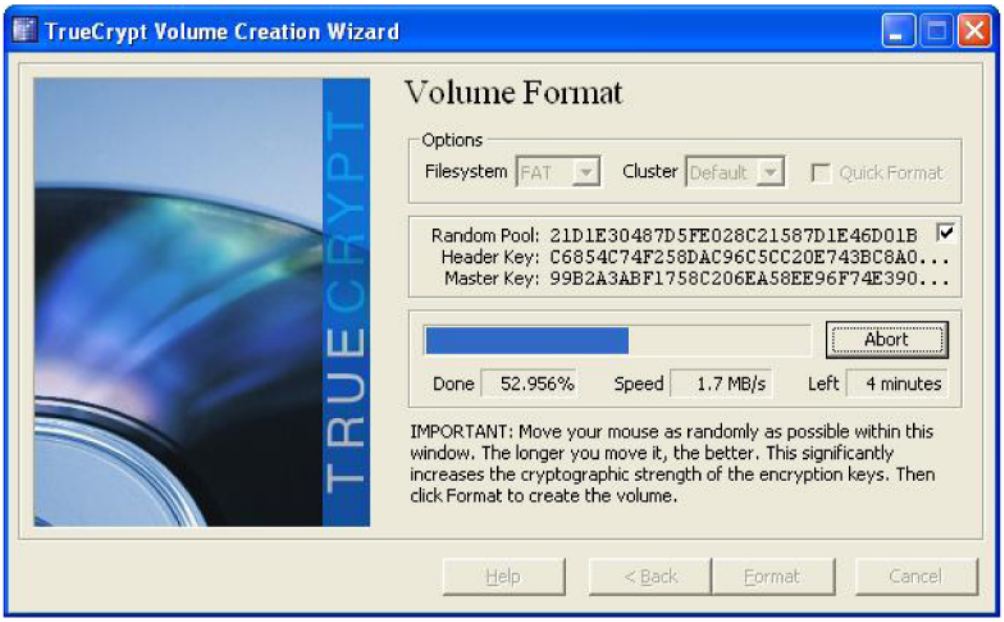
En este momento el asistente le requerirá que seleccione los parámetros de formateo (como el sistema de archivos por ejemplo). Cuando termine de establecer la configuración haga click en "*Format*" para iniciar la creación del volumen encriptado (en este caso también se formatea la unidad).



Se mostrará una advertencia informando que todos los archivos que pueda contener la partición/dispositivo serán borrados y perdidos.

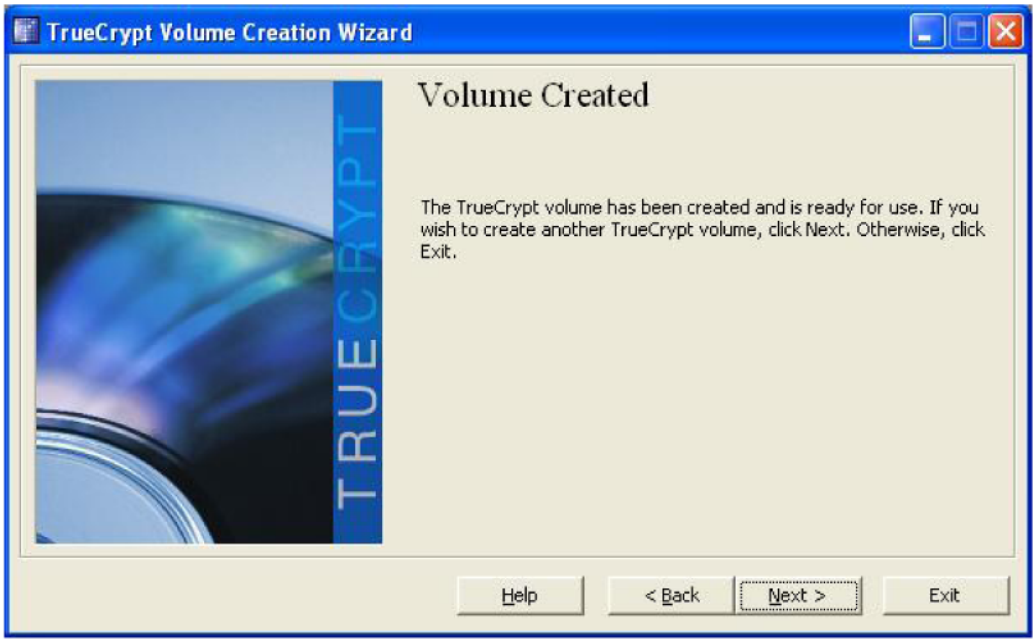


Haga click en "*Sí*" para que empiece el formateo y posterior encripción. Durante el proceso se mostrará el progreso del mismo y le dará la opción de abortarlo en caso de que por algún motivo en especial usted necesite hacerlo. (Advertencia: este proceso puede llevar varios minutos dependiendo del tamaño de la unidad a encriptar).



Al finalizar el proceso se mostrará un mensaje notificando que a partir de ahora la unidad solo podrá ser utilizada mediante el TrueCrypt y que la letra que le asigna el sistema operativo (Windows en este caso) ya no podrá ser utilizada para acceder al mismo. Se podrá volver a utilizar en caso de que formatee nuevamente (perdiendo la encripción del mismo).

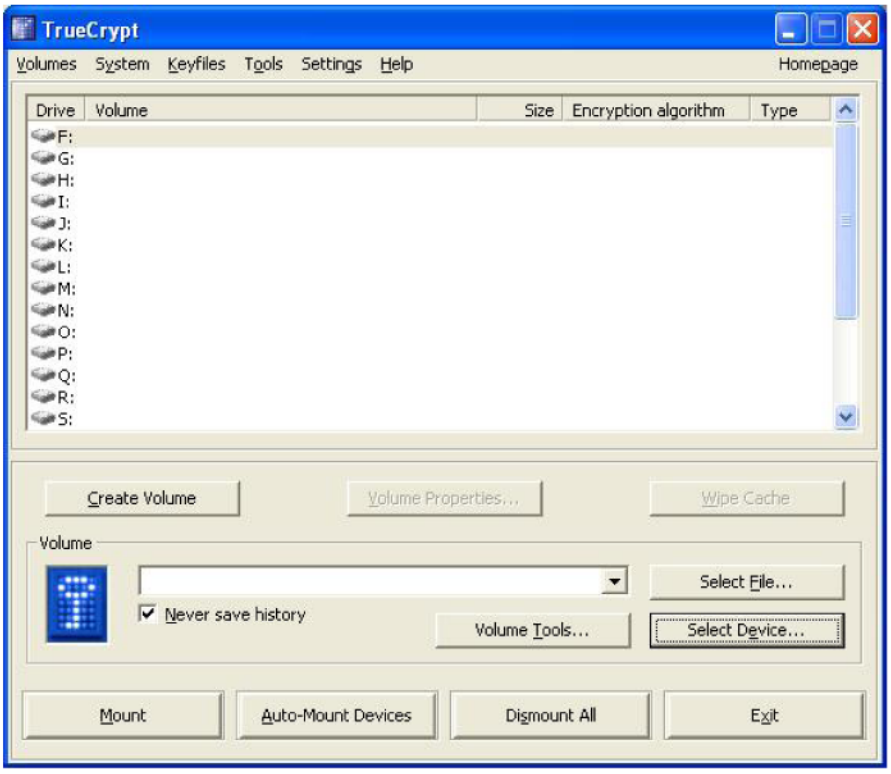
Luego se mostrará informandole que la creación del volumen TrueCrypt fue exitosa. A continuación haga click en "*Next*" si desea crear otro volumen TrueCrypt o en "*Exit*" en caso contrario.



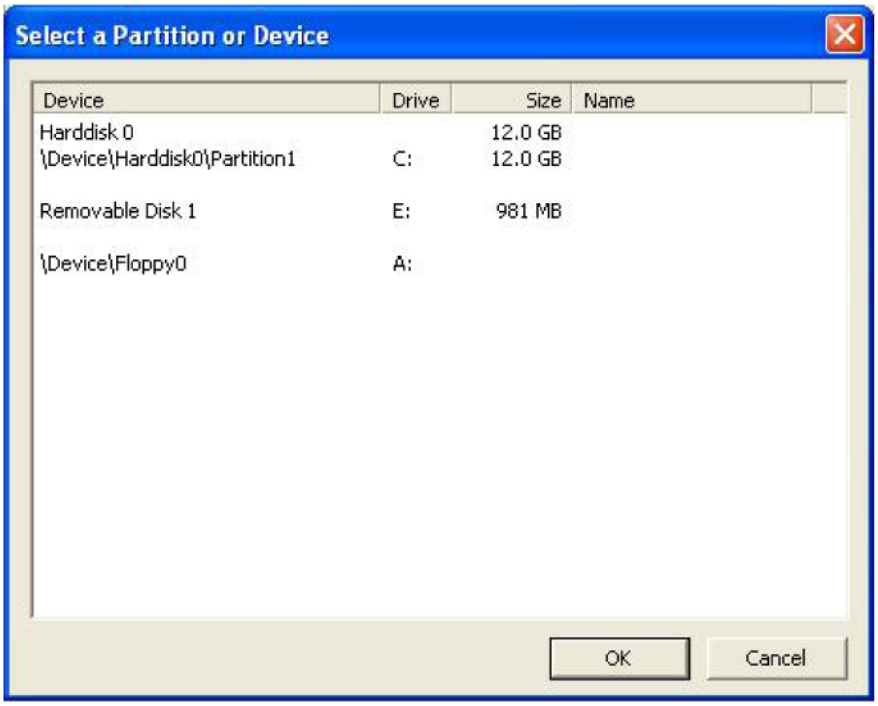
Si usted desea volver la partición/dispositivo a su estado original deberá formatearlo mediante la herramienta de Windows. Al realizar este proceso se pierde toda la información que usted pueda contener dentro de la partición/dispositivo.

8.2 Como utilizar una partición o un dispositivo que han sido encriptados.

Abra TrueCrypt y haga sobre "*Select Device…*".



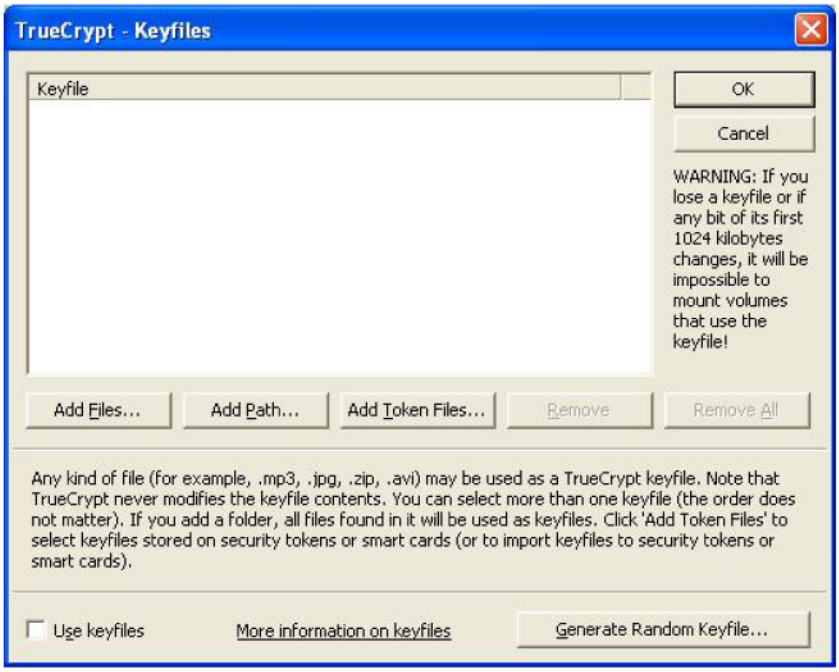
Luego seleccione el dispositivo/partición encriptado que desee utilizar y la letra donde desee que se monte la unidad.



Después de seleccionar el dispositivo haga click en "*OK*". Volverá a la ventana anterior donde deberá hacer click en "*Mount*".

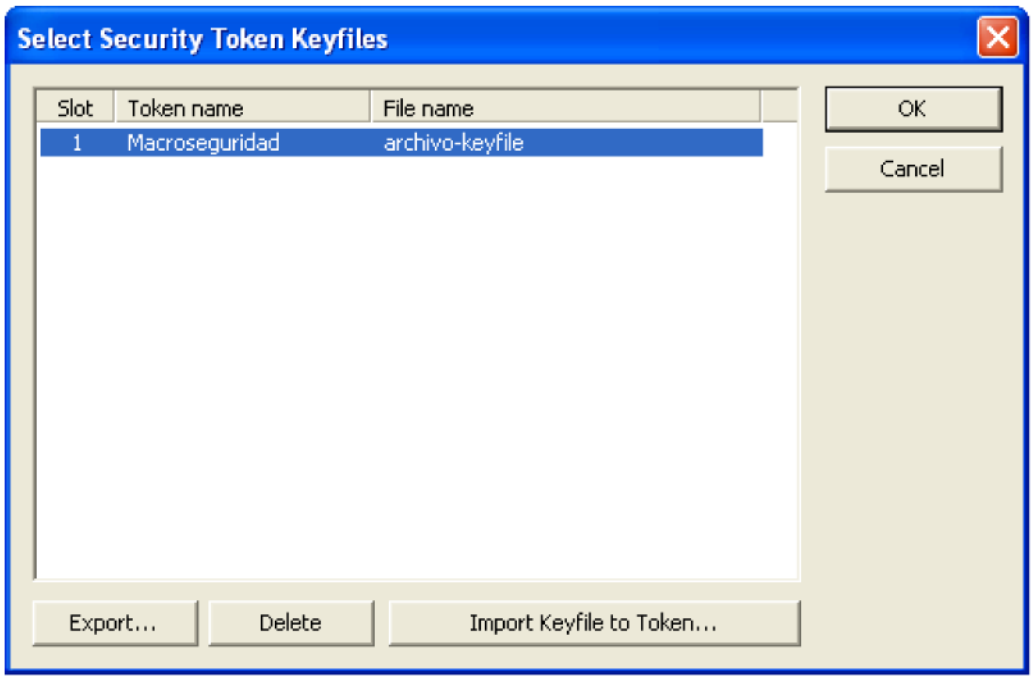
A continuación le requerira que seleccione el Keyfile que sirve para autenticarse al volumen.

Haga click sobre "*Keyfiles*" y luego sobre "*Add Token Files…*"



En caso de que no haya iniciado sesión o la sesión haya expirado el Token/Smartcards le requerirá que se autentique.

Seleccione la Keyfile y haga click en "*OK*".



Luego haga click en "*OK*" y al regresar a la ventana anterior haga click en "*OK*" también.

Su dispositivo podrá ser utilizado mediante el explorador de Windows pero con una letra diferente a la original y con toda la seguridad que brinda la encripción del TrueCrypt integrada con los Dispositivos Criptográfico que Macroseguridad provee al almacenar el Keyfile, mediante el uso de robustas políticas de seguridad, dentro del token/smartcard.

También puede utilizar la opción de "*Auto-Mount Devices*" con la cual el sistema reconocerá los dispositivos TrueCrypt conectados a la PC y en caso de tener sus Keyfiles como default lo montara automáticamente, sino nos pedirá que seleccionemos las keyfiles.

Ud como usuario puede sufrir el robo de una notebook pero el acceso a los datos sensibles de su PC estará garantizado por las ventajas de utilizar TrueCrypt con un Token USB / Smartcard de Macroseguridad. Esta solución termina siendo ciertamente robusta, por utilizar el mecanismo de doble factor que poseen los dispositivos criptográficos de Macroseguridad. Por este motivo es que nos ferefimos a un **sistema de encripción** y no de un software de encripción solamente, ya que se dispone de una solución robusta para encriptar datos, como lo es TrueCrypt, con el agregado de transportar las claves de encripción y desencripción en un dispositivo seguro y externo a la PC o notebook como lo son los Dispositivos Criptográficos de Macroseguridad.

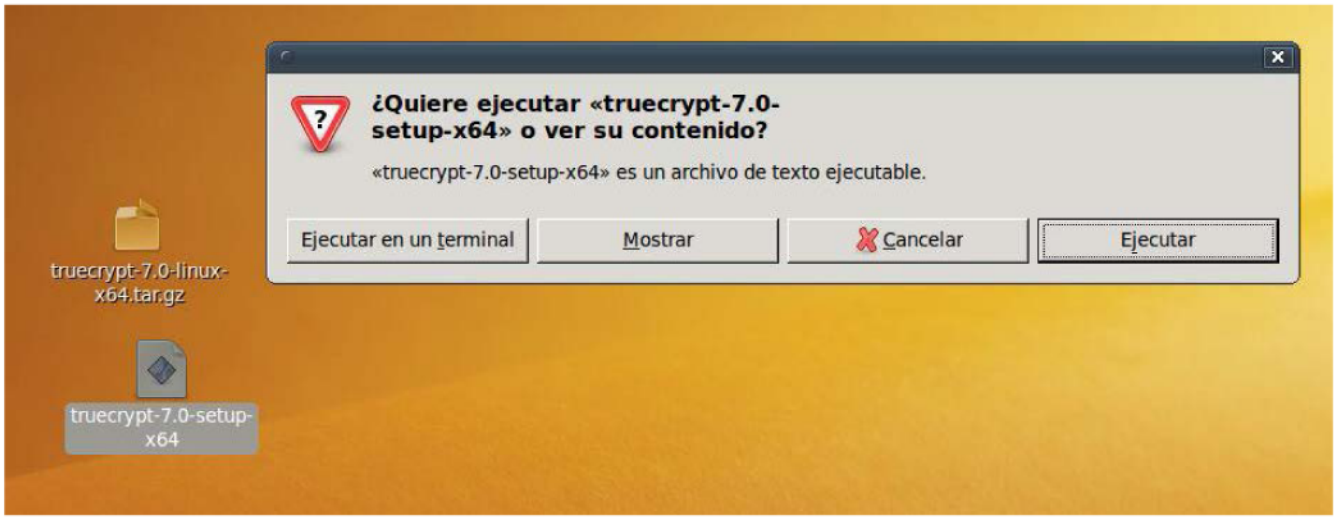
Utilizando estas dos poderosas herramientas es que se logra que la información crítica de un usuario esté verdaderamente a salvo.

9 Instalar Truecrypt en Linux

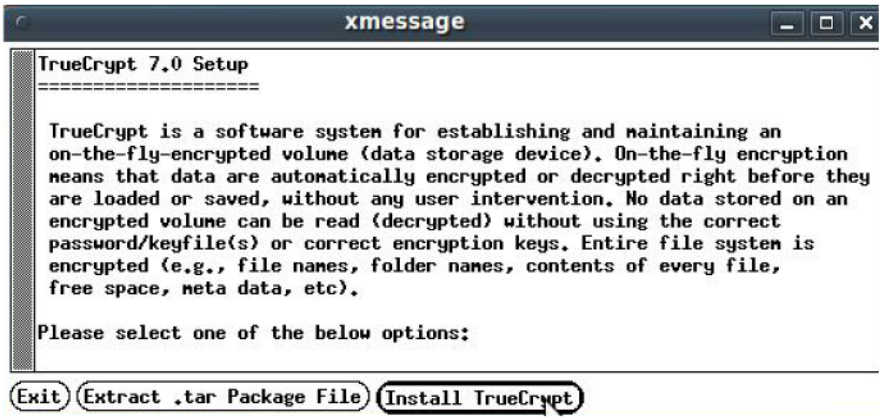
Ud. puede acceder al software haciendo un download del TrueCrypt 6.3a desde **aquí**.

Una vez descargado, extraiga en el escritorio el paquete "*truecrypt-X.X-linux-xXX.tar.gz*

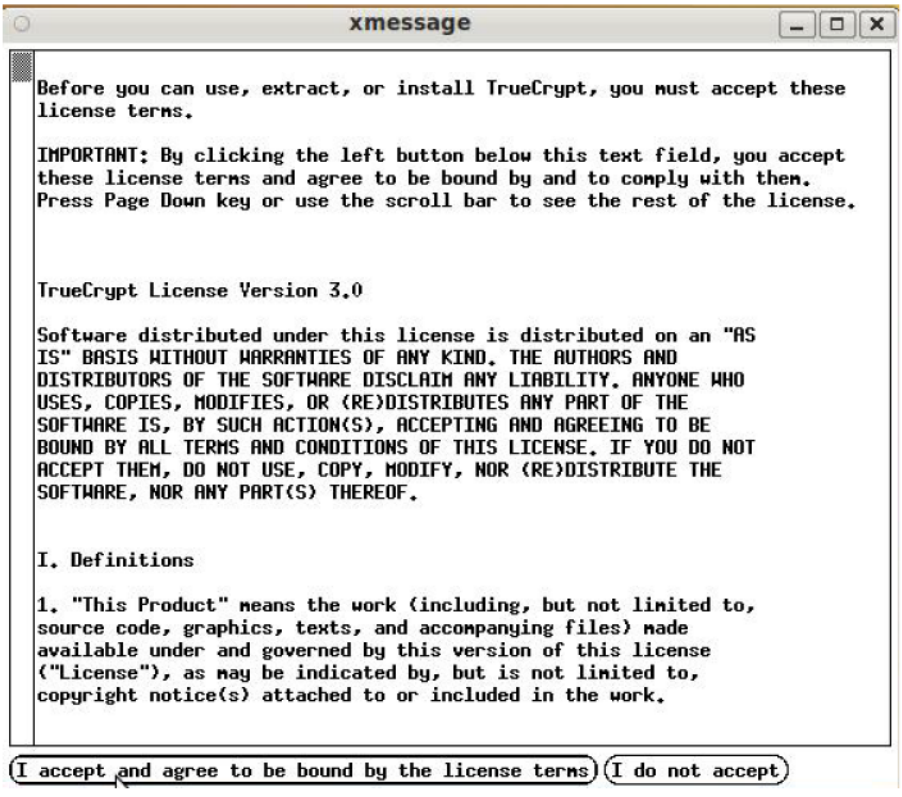
Ejecute el archivo extraido "*truecrypt-X.X-setup-xXX*"". Se mostrará un mensaje que le preguntará si quiere ejecutar el archivo o ver su contendio. Haga click sobre "*Ejecutar*".



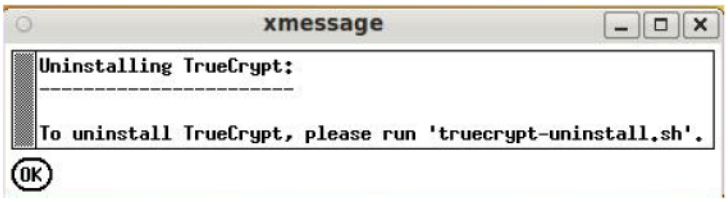
El asistente de instalación se abrirá. Haga click sobre "*Install TrueCrypt*" para comenzar con la instalación.



Lea atentamente el contrato de licencia, si esta de acuerdo con el mismo seleccione "*I accept and agree to be bound by the license terms*" (tenga en cuenta de que si no lo acepta no podrá seguir con la instalación)

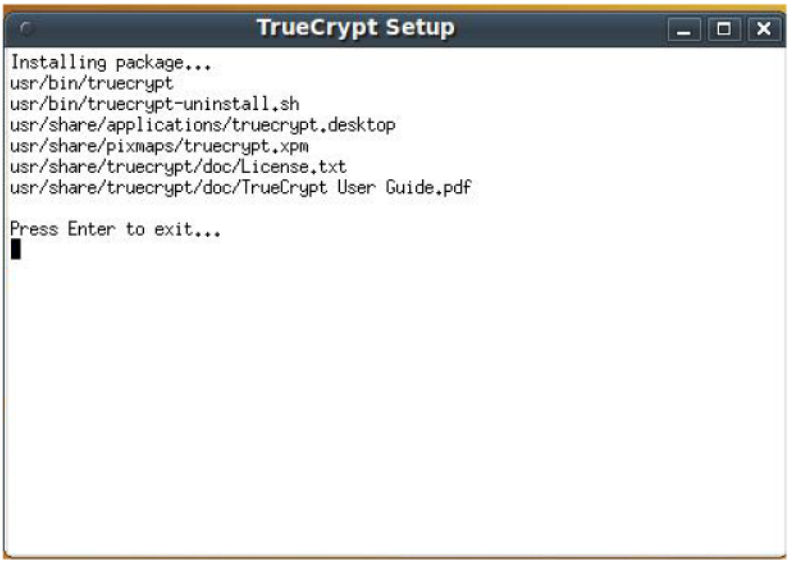


Un mensaje informado de que manera debe desintalarse TrueCrypt se mostrará. Haga click en "*Ok*" para continuar.



Ahora deberá ingresar la password de Administrador de el sistema operativo que este utilizando.

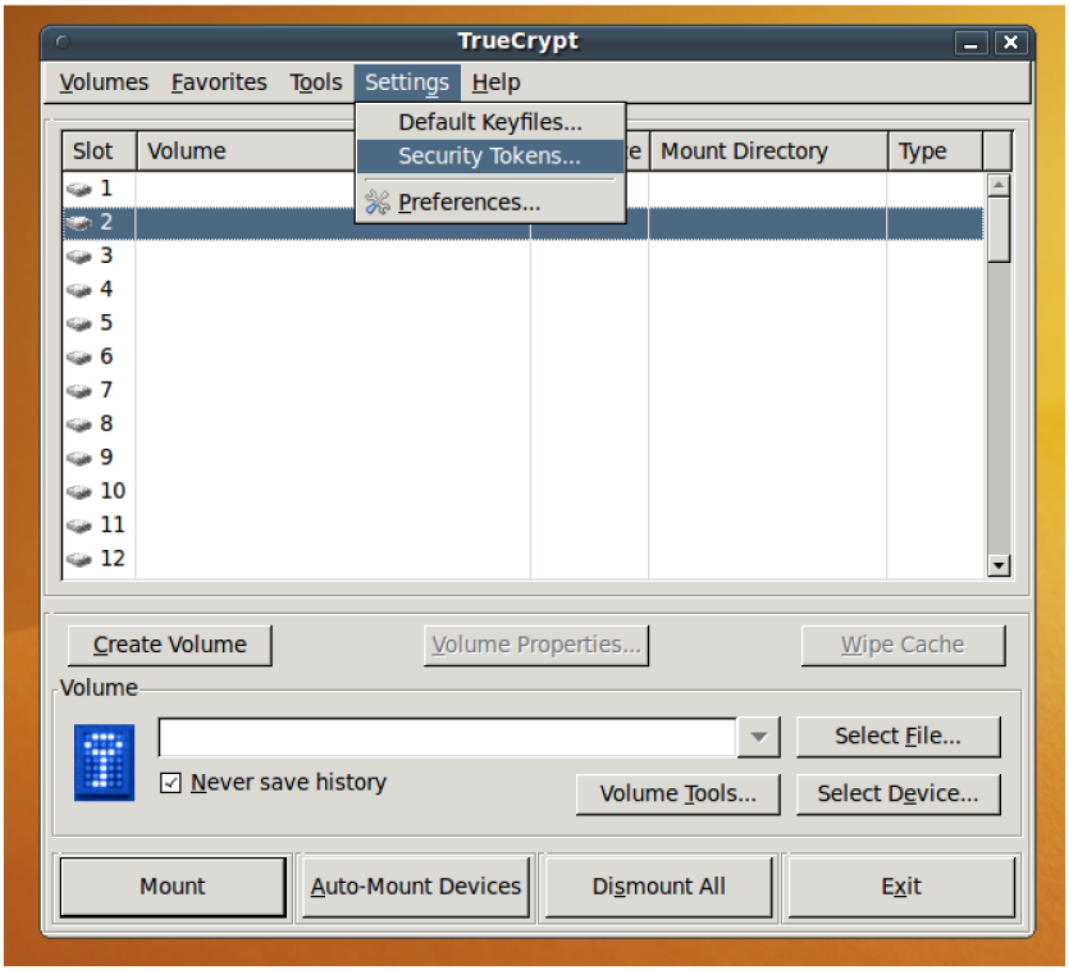
Al finalizar la instalación presione la tecla Enter para terminar. TrueCrypt estará instalado en su sistema.



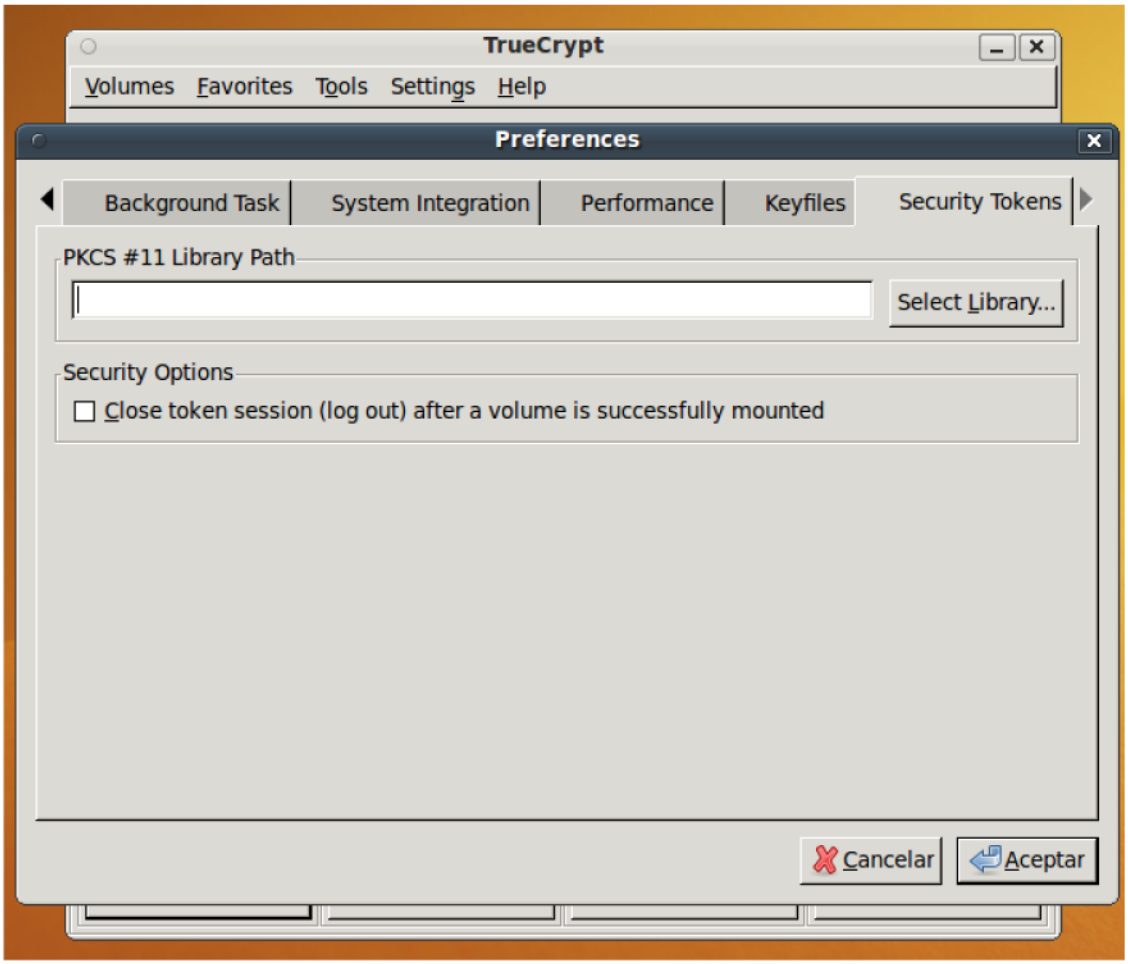
10 Como configurar un Dispositivo Criptográfico de Macroseguridad y la solución de TrueCrypt.org en Linux

Por favor inicie el programa que se encuentra ubicado en *Aplicaciones* > *Accesorios* > *TrueCrypt*

Haga click sobre "*Settings*" en el menú y luego sobre "*Security Tokens*"



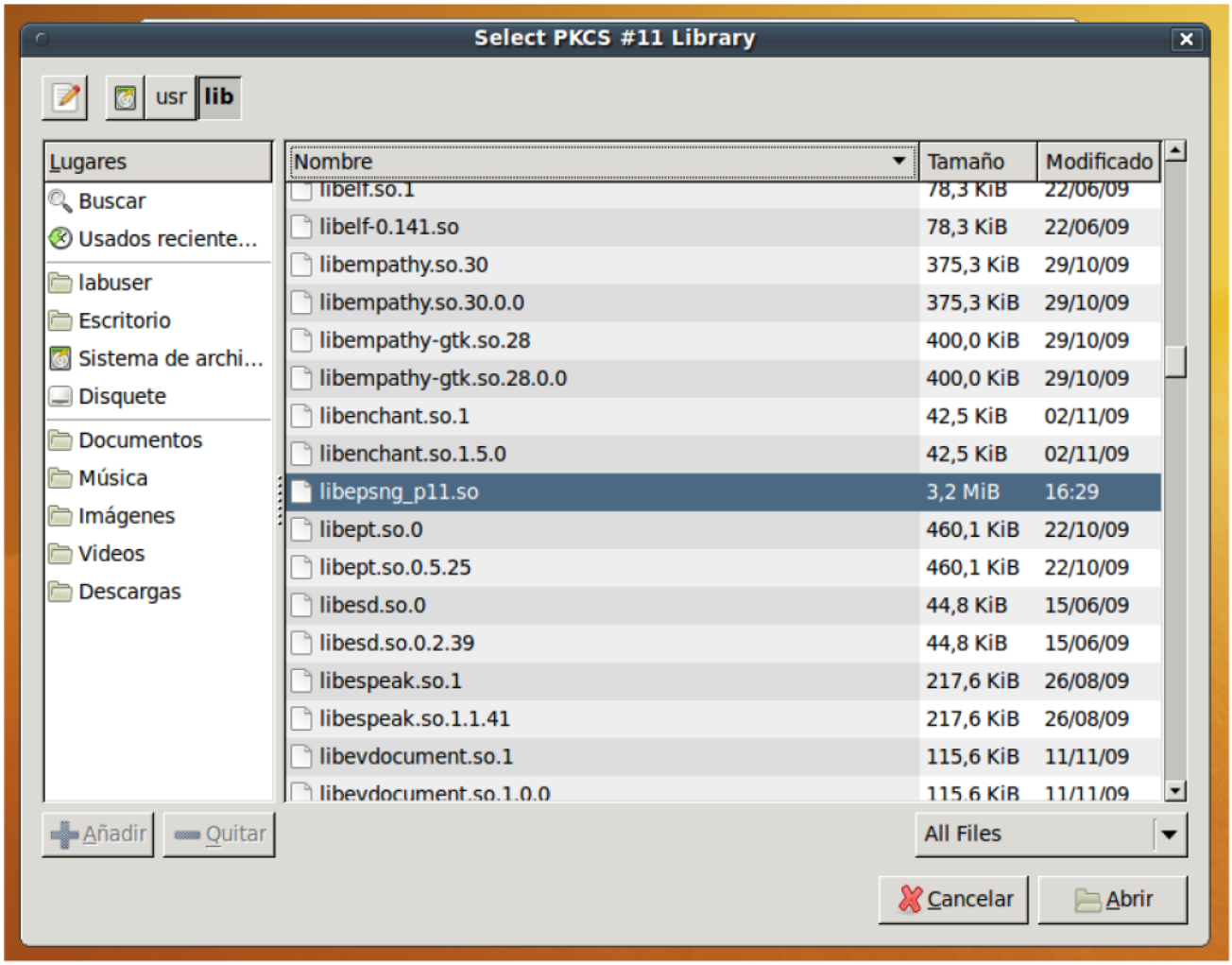
Se abrirá una ventana como la siguiente.



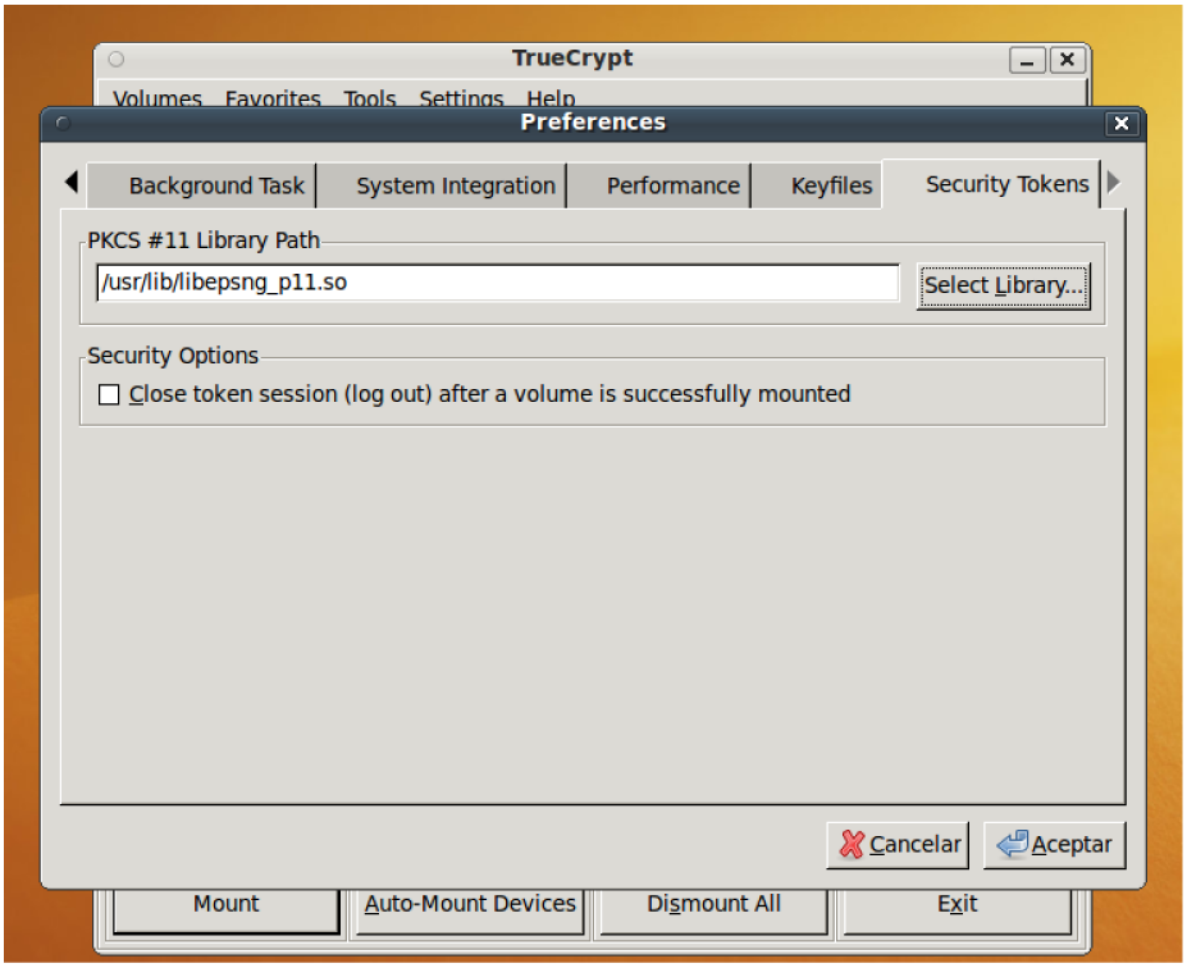
Haga click en "*Select Library…*"

Busque la librería correspondiente a su dispositivo criptográfico, en este caso "*libepsng_p11.so*"" en la carpeta /usr/lib/, selecciónelo y haga click en abrir.

Refiérase al documento Compatibilidad_Token_USB_Macroseguridad-PKCS#11 para saber cual es la librería correspondiente a su Token USB / Smartcard (http://www.macroseguridad.net/soporte/docs/faqs_token.htm).



Una vez que seleccionó la librería que soporta el estandar de PKCS#11 de su Token USB / Smartcard, recomendamos activar el checkbox dentro de "*Security Options*" que refiere a "*close Token session (log out) after a volumen is succesfully mounted*", para mayor seguridad. Esta opción cierra la sesión del dispositivo criptográfico luego de montar una unidad.



Luego haga click en "*Aceptar*" y habrá finalizado la configuración de su token.