

Preguntas más frecuentes

¿Que nivel de seguridad obtengo protegiendo mi sistema con HARDkey?

El nivel de protección es excelente tanto en el componente de hardware que es la llave electrónica como en las librerías que interactúan con la aplicación. Todas las transacciones se realizan en forma completamente cifrada entre el protector y las rutinas que lo manejan. A su vez la librería y el ejecutable protegido están "envueltos" por rutinas que los cifran y les agregan código anti-debug y trampas de software para evitar ingeniería inversa. El corazón del sistema de protección está basado en una tecnología que cifra el software a través de la llave electrónica, lo cual hace virtualmente imposible que un hacker pueda "saltar las rutinas de protección".

¿Puedo proteger ejecutables y cifrar los archivos asociados para que no se puedan modificar por a fuera de la aplicación?

Si, mediante el entorno de protección automática es posible proteger directamente un programa (un EXE o DLL, sin necesidad de tener los fuentes) y declarar que archivos asociados se desean manejar en forma cifrada. Una vez protegida la aplicación, esos datos sólo podrán ser accedidos desde la aplicación que tiene embebidas las rutinas de cifrado ON-LINE de HARDkey. Esto resulta muy útil para poder proteger Catálogos, E-Books o documentación para capacitación, por ejemplo.

¿Puedo con una sola llave controlar las licencias de uso en una red?

Las llaves HARDkey NET (carcasa anaranjada) pueden ser compartidas para que una o varias aplicaciones puedan ser accedidas desde distintos puestos de una red. Nuestro sistema de protección no impone ninguna restricción al desarrollador, el cual puede optar por implementar un esquema con o sin control del número de licencias concurrentes de uso para su usuario final. Si decide realizar control de licencias, le brindamos las herramientas para limitar la cantidad de usuarios simultáneos que accedan a las llaves. Existe otros modelos de llaves que son exclusivamente para aplicaciones monousuario (HARDkey STD, HARDkey 797 y HARDkey USB).

¿Bajo que protocolos trabaja el chequeo en una red local?

La comunicación entre el servicio que administra el acceso a la llave y la aplicación protegida se realiza mediante la tecnología "MailSlot" de Windows lo cual garantiza el enlace a través de cualquier protocolo que esté usando la red para funcionar. Esto representa una ventaja importante ya que no se limita el funcionamiento a un protocolo en particular sino que el sistema se maneja con el protocolo que esté configurado (NetBios, IPX, TCP/IP, etc.). Además es posible configurar directamente la dirección IP o el nombre del Servidor para agilizar las búsquedas.

¿Puedo colocar la llave en cualquier terminal, o incluso en el servidor de una red?

Si, no hay restricciones en ese sentido. Puede optar por cualquiera de los dos esquemas. En el KIT se proveen los Drivers y utilitarios necesarios para cada caso.

¿Puedo evitar que luego de iniciada una aplicación, utilicen la llave para ejecutar una copia de la misma en otra PC o red ?

Si esto es posible y la forma de implementarlo depende del tipo de protección que haya elegido. Si trabaja con el entorno de Protección Automática, basta con activar la opción "Chequear la llave cada cierto período de tiempo configurable". En cambio si protege el programa mediante la librería DLL en forma Interactiva, debe invocar chequeos de la llave en lugares estratégicos como por ejemplo los cambios de pantalla o menú. Esto impide que el software continúe funcionando si retiran el protector una vez iniciada la aplicación.

¿Puedo combinar la Protección Automática y la Interactiva en una misma aplicación?

Si esto es posible y es lo más recomendable, porque de esa forma se logra un aún mejor nivel de seguridad en la protección de las aplicaciones, combinando la encriptación generada por la Protección Automática y la mayor flexibilidad de la Protección Interactiva.

¿Puedo tener más de una llave de diversos sistemas y proveedores en la misma PC?

Si, las llaves HARDkey pueden ser conectadas en cascada una detrás de otras. También son transparentes a llaves electrónicas de otros modelos y marcas.

¿Se puede usar una llave "personalizada" con un KIT, con los utilitarios de otro KIT?

No, una vez personalizada la llave sólo responde a los utilitarios y librerías de ese KIT. Tampoco es posible reiniciarla ni re-personalizarla con otro KIT.

¿Se puede usar una misma llave para proteger más de una aplicación o módulo?

Si, usando la Protección automática se pueden administrar hasta 32 módulos o aplicaciones diferentes, y usando la Protección Interactiva se pueden armar esquemas que permiten controlar todas las aplicaciones que se deseen con una misma llave.

■ ¿Puedo en Internet o una Intranet, desde un servidor de páginas (ASP- PHP – JSP) saber quien las levanta para "personalizar" y "limitar" el acceso ?

Si, desde cualquier página dinámica se pueden invocar todos los comandos disponibles en la Protección Interactiva. Entre ellos hay funciones para detectar si la llave está o no instalada, que número de serie y lote tiene, leer y grabar celdas de memoria, etc.

■ ¿Puedo armar un Canal Seguro de Comunicación en Internet o una Intranet, usando HARDkey?

Si, usando una llave HARDkey para validar el LADO CLIENTE de una comunicación y con un solo Certificado Digital de Servidor para validar el LADO SERVER, una vez verificado la identidad el cliente con la presencia de una llave HARDkey se puede armar un TUNEL SEGURO con SSL. De esta forma se garantizan una CONEXION SEGURA sin necesidad que todos los CLIENTES tengan Certificados Digitales. Esto permite bajar mucho los costos para lograr este tipo de comunicaciones, y es un esquema ideal para todo tipo de operaciones B2B.

■ ¿Puedo en forma remota cambiar datos grabados en la llave?

Si, el Sistema de Actualización Remota de Llaves (SAR) permite generar un ejecutable actualizador para enviar al cliente final, el cual al ejecutarse reconfigurará los parámetros deseados dentro de la memoria del protector. Además desde una página en un Servidor de Internet puedo cambiar cualquier dato en la llave con el solo requisito que el cliente acceda a la página desde el Explorer con la llave instalada en el puerto de su PC, por medio de un componente ActiveX, que permite leer o grabar cualquier celda de la llave.

■ ¿Puedo generar versiones con límites de uso para Demostraciones, Alquiler o Leasing?

Si, usando la Protección automática definir use puede definir una FECHA de VENCIMIENTO, un LIMITE de EJECUCIONES o LIMITE DE HORAS DE USO que queda grabado en la llave y puede ser cambiado en forma remota tantas veces como se quiera.

■ ¿Puedo usar las llaves HARDkey para validar el acceso de Usuarios a Aplicaciones ?

Si, usando las llaves HARDkey es posible reemplazar o complementar el uso de Usuario y Password. Esto permite que se pueda realizar para aplicaciones críticas una VALIDACIÓN FUERTE de usuarios por DOS FACTORES: algo que se tiene (una llave HARDkey) y algo que se conoce (el usuario y password). Es ideal para validar el acceso de los supervisores, administradores o los técnicos que realizan mantenimiento de los sistemas, evitando que alguien que consiga su usuario y password se haga pasar por ellos, dañando la integridad de los sistemas. La utilización de las llaves HARDkey para validar accesos de usuarios con algo más fuerte que usuario y password permite cumplir con la Norma ISO 17799.