

MacroS@guridad

MAYORISTA EN SOLUCIONES DE SEGURIDAD



**WHITE PAPER
TECNOLOGIA DE AUTENTICACION
EPASS TOKEN USB**

Reseña Historica

Autenticación significa probar (constatar) que la persona "es" quien dice ser.

La autenticación de Usuarios en forma confiable es crucial para la continuidad de un negocio exitoso, y esta situación debe darse antes que puedan ganar acceso a los recursos informáticos de su organización.

Cuando usted sabe fehacientemente que solo los usuarios autorizados y autenticados – sean estos empleados, socios de negocios, o clientes – pueden acceder a su red y datos, recién en ese momento usted puede proveer a sus usuarios con mejor conectividad y servicios de negocios on line, los cuales no podría haber ofrecido de otra manera.

Esto significa mayores oportunidades de generación de negocios, reducción de costos operativos y mayor productividad.

Las passwords, son el método tradicional utilizado para autenticación, pero es débil y sumamente costoso de administrar. Un usuario típico hoy en día maneja más de 10 passwords diferentes para distintas aplicaciones (sean de la organización del banco, de un webmail, etc). Para manejarlas el usuario generalmente utiliza passwords fáciles de recordar o lo que es peor, las escribe en papel (bajando considerablemente los niveles de seguridad), y sino termina llamando al helpdesk de IT cada vez que se olvida la misma. Esto crea un riesgo en la seguridad y a su vez genera una carga adicional de trabajo en el helpdesk.

Autenticación Robusta de Usuarios - ¿Qué es?

Existen varios métodos para lograr autenticar a un usuario en forma efectiva. Lamentablemente eso solo no alcanza, para que el usuario además pueda probar su identidad en forma univoca, debemos agregar otro concepto muy diferente al de autenticación, para poder probar "quien realmente es", identificar al usuario. Este concepto tiene que ver con la verificación de una parte de su cuerpo humano.

Una robusta autenticación de usuarios se basa al menos en 2 factores, incrementando considerablemente la seguridad y a su vez logrando reducir significativamente los costos asociados a la utilización de passwords.

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, el escaneo de iris, ADN. 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 más aceptadas, 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 unívoca 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 ej. para firmar correo, firmar un PDF, o abrir una VPN.

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

Hasta hoy se debía digitar un PIN de acceso sobre el teclado para ganar acceso al 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.

Generalidades

La línea de productos ePass provee dos factores de autenticación robusta, ofreciendo mayor seguridad que las passwords. Para ganar acceso a los recursos de la red, o firmar un documento electrónico usted debe autenticarse al ePass Token USB (algo que usted tiene) con una Password o PIN del dispositivo (algo que solo usted debe saber).

Los ePass Tokens son extremadamente seguros ya que todas las operaciones se realizan dentro del chip criptográfico contenido en cada ePass. En esencia es una smartcard que se conecta al puerto USB de su PC- en vez de requerir una lectora adicional para conectarse. Toda la funcionalidad de una smartcard, pero en un solo dispositivo.

ePass puede almacenar de forma segura todas sus passwords, claves y credenciales, para que usted las pueda llevar consigo y pueda acceder a la red o aplicaciones en cualquier momento y lugar. Solo necesita recordar una única password, la del ePass, para acceder a todas sus credenciales, lo que significa que usted podrá hacer esta password de autenticación mucho más compleja y difícil de hackear. Si usted extraviase su ePass, su identidad no estará comprometida, pues todas las credenciales almacenadas en el ePass no podrán ser reveladas si no se sabe la password o PIN del ePass.

En la actualidad el reconocimiento unívoco de una persona puede elevarse al máximo nivel de seguridad a través de la solución BioPass.

Esta solución se presenta como un híbrido entre las dos tecnologías más reconocidas en este aspecto: por un lado las smartcards y por otro la Biometría. Este nivel de autenticación se logra utilizando el BioPass 3000 token USB que las incorpora en un solo producto.

Beneficios de ePass Token USB

A las organizaciones, ePass les provee:

- **Más Negocios**
Con acceso seguro, las organizaciones pueden ofrecer negocios a través de la conectividad de la red y proveer servicios online en todo lugar y todo momento, como son las transacciones comerciales, bancarias y tramites On-line.
- **Seguridad**
ePass protege la información sensible que hacen al negocio, contra accesos no autorizados
- **Ahorro en Costos**
ePass reduce los costos de administración de password, reduce las pérdidas por violación de información, y provee una amplia gama de soluciones que se adecuan a las necesidades del cliente
- **Cumplimiento de Reglamentaciones Internacionales**
ePass Token USB, ayuda a cumplir con las leyes y reglamentaciones protegiendo la información y privacidad, como lo son Sarbanes-Oxley, HIPAA, la ley de firma digital, y el Standard de Seguridad PCI. Es totalmente auditable y escalable.

A los usuarios, ePass les provee:

- **Protección de la identidad digital**
ePass brinda a los usuarios una solución de protección de la identidad digital, en forma confiable y fidedigna, protegida contra robo y abuso.
- **Portabilidad y conveniencia**
ePass permite a los usuarios llevar en forma segura sus certificados digitales y credenciales de acceso donde quiera que vayan.
- **Facilidad de uso**
ePass permite un trabajo intuitivo y transparente para los usuarios gracias a toda la interface de trabajo en castellano y soporte local. Manuales y Documentacion y castellano, que acorta la curva de aprendizaje
Posibilidad de desarrollar aplicaciones para recordar una única password y acceder a las mismas.

A los administradores de sistemas, ePass provee:

- **Simplicidad** – Solo es necesario instalar el middleware de ePass para lograr su integración con la mayoría de las aplicaciones PKI del mercado, trabajando sobre cualquier plataforma: Linux, MAC y Microsoft.
- **Administrador de Certificados ePass** – provee una administración completa de los dispositivos ePass y sus soluciones de seguridad asociadas a través de una única interface de aplicación tanto para plataformas Microsoft, Linux y MAC.
- **Personalización** - Se proveen herramientas para el formateo de los tokens (Set to factory), permitiendo la personalización de características de seguridad del ePass (longitud del PIN, tiempo de expiración y time-out, etc.), de acuerdo a las políticas de la empresa.
- **Eficiencia** – ePass reduce las llamadas al helpdesk relacionadas con passwords, ofreciendo toda la interface del producto en idioma español. Se proveen los Manuales y Guías en castellano.

Las Soluciones de ePass

Seguridad en el Acceso a la Red – ePass asegura el acceso a las redes locales (Windows logon, smart card logon, escritorio remoto, terminal server) como también acceso remoto seguro (VPN y web), soportando múltiples métodos de autenticación incluyendo, passwords, infraestructura PKI, y soluciones de autenticación Biométrica además de combinar la utilización de certificados digitales para tal fin.

- Logon a la Red

ePass permite autenticación robusta de usuarios en el logon a recursos protegidos de la red, soportando tanto tecnología smartcard logon utilizando PKI y el Microsoft logon nativo (GINA API) almacenando passwords de usuario y credenciales de acceso. Así como también utilizar la biometría con GINA de Microsoft y PKI para ganar acceso a los equipos.

- Seguridad para las VPN (Acceso Seguro Remoto)

ePass permite autenticación robusta de usuarios cuando acceden en forma remota a la red corporativa, ofreciendo una fácil integración con los sistemas VPNs líderes. ePass soporta múltiples métodos de autenticación VPN incluyendo certificados digitales, OTP y la tecnología biométrica incorporada a los ePass Token USB para permitir el acceso solo a las personas realmente habilitadas.

- Acceso a la Web (certificados digitales y Web Based VPN)

ePass Token USB permite una robusta autenticación de usuarios al acceder a un portal restringido. Permite firmar digitalmente transacciones e información sensible, ya sea a través de doble factor de autenticación (lo que tengo "el ePass" y lo que conozco: el PIN del ePass), como también a través de la autenticación univoca de una persona, utilizando el BioPass 3000 Token, ya que debo presentar mis huellas dactilares para acceder a las credenciales, claves o certificados digitales almacenados dentro del dispositivo y por ejemplo poder firmar digitalmente un documento.

- Protección de la Información

ePass Token USB permite proteger su información en forma robusta, garantizando la integridad y confidencialidad de los datos que se transmiten en ambientes inseguros como emails y transacciones on line - a través de encriptación y firma digital.

- Protección de Archivos y Encriptación de datos

ePass Token USB, se integra con los más prestigiosos productos de encriptación, ya que los mismos trabajan a través de estándares de mercado y nuestro foco es siempre mantener esa compatibilidad.

- eMail Seguro

ePass ofrece la posibilidad de firmar y encriptar correo electrónico con la más simple y fácil integración con los clientes de email más importantes utilizando características de seguridad inigualables.

- Firma Digital (No-repudio)

Las transacciones y documentos técnicos pueden ser firmados digitalmente con ePass a través de tecnologías PKI, asegurando la autenticidad de las transacciones electrónicas. El no repudio está dado por dos actores protagónicos. Por un lado el que recibe un documento firmado digitalmente, y por el otro el que emitió esa firma y que es el dueño de ese certificado.

La garantía del no repudio no solo está dada por el uso de tecnología PKI (certificado digital) para una de las partes, sino, que el dueño de ese certificado digital debe tener también la certeza del almacenamiento seguro del mismo para evitar la posibilidad de duplicidad o acceso a dicho certificado por alguna persona no autorizada.

- Administración de Passwords

ePass provee almacenamiento seguro de credenciales de acceso.

- Enterprise Sign-On

Pueden integrar ePass dentro de diferentes aplicaciones y soluciones como ser Microsoft Smartcard Logon, Terminal Server, Escritorio remoto, PAM en Linux y otros métodos de logon a la red corporativa, utilizando la tecnología PKI pueden reemplazar las claves y passwords por las credenciales de 1 solo certificado.

Familia de Productos ePass

Se compone de:

- Dispositivos – Una amplia gama de dispositivos de autenticación de usuarios basados en smartcard, USB Tokens, OTP (One Time Password) y Biométricos y la posibilidad de ofrecer bajo requerimientos de los clientes la posibilidad de incluirles una memoria flash.

- Middleware – Aplicaciones de Seguridad

Una gran variedad de aplicaciones pueden integrarse simplemente instalando el middleware de ePass en la PC que Ud. va a utilizar.

- ePass Management Tools

Herramienta centralizada para el control y administración del ePass y los certificados almacenados en él. Se proveen dos herramientas, diferenciando las operaciones que puede realizar un Administrador (SO-Security Officer) y las que puede realizar un Usuario Final en el dispositivo.

- Deploy Simplificado

Para aquellos usuarios que no requieren instalar nada más que los drivers del dispositivo, se provee una interfaz de instalación simple y liviana, a fin de que la implementación en grandes redes resulte lo más sencillo y amigable posible.

- SDKs

Cada uno de los productos que comercializamos, dispone de un SDK para que las empresas, las organizaciones, instituciones de gobierno o terceras partes que desean desarrollar sus propias aplicaciones puedan integrar la seguridad de ePass para autenticar sus usuarios y realizar operaciones de firma y encriptación en documentos electrónicos.

Dispositivos ePass

Todos los dispositivos ePass brindan a las organizaciones gran flexibilidad para encarar sus necesidades individuales. Desde Tokens USB para PC y ambientes remotos a smartcards para control de acceso. La eficiencia y portabilidad de ePass son la elección inteligente para las organizaciones que buscan estar siempre un paso adelante en este cambiante mundo digitalizado.

? ePass1000

ePass1000 ofrece una simple, robusta funcionalidad de seguridad onboard utilizando algoritmos HMAC-MD5. Almacena certificados, passwords, claves, permitiendo trasladarlas en un dispositivo seguro y portátil.

? ePass1000ND

Es una solución driverless, se provee en formato USB con una memoria de 8kb, permite interactuar con las aplicaciones que soportan los estándares CAPI y/o PKCS#11. Se provee también una API privada para las empresas que lo quieren integrar a sus desarrollos.

? ePass 2000 Token (USB)

Es una smartcard en formato de dispositivo USB, que no requiere de ningún hardware adicional. Posee la mejor relación costo beneficio del mercado. Permite la autenticación robusta de usuarios a través de 2 factores, siendo muy fácil de integrar con su actual plataforma o en su ambiente de seguridad PKI. ePass2000 es seguro, genera claves de 1024bits on board y posee la certificación de compliance con FIPS 140-2 Level2.

? ePass3000 Token USB

Es la evolución en soluciones de smartcards, incorpora un procesador de 32 bits, 4 veces más rápido que cualquier otro token del mercado. Genera claves RSA de 512/1024 y 2048-bits on-board, soporta DES, 3DES y SHA-1 y se integra transparentemente con la mayoría de las aplicaciones PKI existentes.

? BioPass 3000 Token

Combina lo mejor de dos de las tecnologías más reconocidas en seguridad: las smartcards y los controles biométricos otorgando a los usuarios una autenticación unívoca. No solo garantiza la integridad y autenticación, sino lo más importante es que garantiza unívocamente la identidad de esa persona en particular.

? ePass Token EF (ePass FLASH)

Las soluciones de autenticación ePass pueden integrarse bajo requerimientos de nuestros canales o de los clientes (mediante un proyecto) con cualquier tipo de solución de almacenamiento masivo. La capacidad de la memoria flash dependerá de la necesidad concreta del proyecto.

? ePass 2000 Token (Smartcard)

ePass2000 SmartCard ofrece la misma funcionalidad que el ePass2000 Token USB pero en el tradicional formato de tarjeta de crédito. En este caso las smartcards deben trabajar con una lectora como ser el Rockey200 o el Rockey400

? Lectoras

Las lectoras smartcard Rockey200 y Rockey400 (driverless) presentan la mejor relación costo beneficio (soportando todos los sistemas operativos), y brindan el complemento ideal para cualquier tipo de smartcard en formato tipo tarjeta de crédito.

Soluciones Integradas con algunos de nuestros Partners

Check Point Software Technologies Ltd.

Categoría: Cliente VPN

La Solución integrada:

Con referencia a crear túneles VPN entre una usuario remoto y el VPN-1 Gateway, SecuRemote/SecureCliente autentica el usuario en el gateway VPN-1 antes o durante la comunicación. ePass Token soporta la autenticación basada en PKI y certificados (Checkpoint VPN-1 NG) esta versión utiliza el estándar de Mercado basado en CAPI ePass Token USB es OPSEC certificado tanto en VPN v4.1 y NG y superior.

Cisco Systems Inc.

Categoría: Cliente VPN

La Solución integrada:

Los clientes que utilizan el Cliente VPN de Cisco, pueden interactuar en forma transparente con cualquiera de las soluciones ePass Token USB, los usuarios podrán autenticarse con el dispositivo criptográfico a un cliente VPN o contra un Cisco VPN 3000 Concentrator. Corporativamente, los administradores pueden garantizar a la gerencia que los usuarios que necesitan acceder a los sistemas críticos que hacen a la continuidad del negocio, lo harán con una tecnología de identificación univoca como es BioPass 3000 Token.

Microsoft

Categoría: Cliente VPN

La Solución integrada:

Microsoft brinda una solución integrada para establecer VPN, con un servidor Windows 2000/2003 y un cliente XP. El servidor de Acceso remoto presente en cualquier Windows Server permite utilizar el protocolo L2TP, requiriendo certificados digitales para establecer el túnel VPN. Asimismo, el cliente VPN de Microsoft presente en cualquier Windows 2000/XP o VISTA se provee como una funcionalidad adicionada al sistema operativo sin costo adicional. ePass Token USB es totalmente compatible con este cliente, y permite trabajar en forma totalmente transparente con los certificados digitales almacenados en el dispositivo (smartcard). De esta manera, puede establecerse un túnel VPN de máxima seguridad desde el mismo sistema operativo, sin requerir la instalación de ningún otro cliente de software adicional para realizar la VPN.

OpenVPN

Categoría: Cliente VPN

La Solución integrada:

OpenVPN es una solución integral gratuita (opensource) que permite a los usuarios de equipos móviles conectarse con la red corporativa en forma segura sobre una conexión insegura (como es Internet o una conexión WiFi).

OpenVPN soporta íntegramente los dispositivos criptográficos de autenticación y de portabilidad de certificados a través del conocido estandar de PKCS#11; el mismo permite trabajar con certificados digitales almacenados dentro de la familia de productos ePass Token USB. OpenVPN puede correr tanto sobre plataforma Microsoft como la plataforma Linux, a su vez las soluciones de ePass soportan íntegramente las 3 familias de productos "Microsoft, Linux, MAC"