

PROPUESTA INTEGRAL DE SEGURIDAD INFORMATICA

Podemos ofrecer un abanico de soluciones para la validación de accesos de usuarios a aplicaciones y sitios Web, y además para permitir transportar y proteger Certificados Digitales en esquemas PKI.



En toda implementación de seguridad existen distintos niveles de requerimientos, y por lo general los usuarios más numerosos son los que necesitan menores requisitos, y solo para un grupo reducido, que realiza las operaciones más críticas, es necesario utilizar mayores niveles de seguridad.

Contamos con tres líneas de productos para atender las necesidades de seguridad referidas a la validación de accesos y la protección / transporte de Certificados Digitales en esquemas de PKI:

- 1) Llaves Criptográficas iKey 2000/2032
- 2) Llaves criptográficas iKey 1000/1032
- 3) Llaves electrónicas HARDkey MIO

Las llaves iKey 2000/2032 poseen un poderoso procesador criptográfico que les permiten generar internamente el par de claves "Privada" y "Pública", garantizando que la clave "Privada" nunca existirá fuera del hardware de la llave evitando ataques a la misma. La única diferencia entre estos modelos es que la iKey 2000 tiene 8 Kbytes de memoria y la iKey 2032 tiene 32 Kbytes.

Las llaves iKey 1000/1032 tienen un procesador menos potente y por ello utilizan el procesador de la PC para generar el par de claves "Privada" y "Pública" y luego las almacenan junto con el Certificado Digital dentro de la llave, permitiendo transportarlas y protegerlas. Luego de este proceso las claves pueden ser utilizadas, al igual que con las iKey 2000/2032, en forma transparente para todo tipo de firmas y cifrado de documentos.

Las llaves iKey 2000/2032 tienen como principal ventaja el garantizar que la clave privada se genera y utiliza siempre dentro del hardware de la llave, evitando ataques para apoderarse de la misma. Pero por otra parte al no poder extraerse la clave privada no es posible realizar backups de la misma, y en caso de extravío o daño de la llave es imposible recuperar esta clave privada, y como consecuencia si se han cifrado documentos con ella no se podrán acceder más.

Las iKey 1000/1032 permiten realizar backups de seguridad del par de claves y del Certificado Digital, pudiendo importarlos y exportarlos de las llaves.

Las iKey 2000/2032 tienen un mayor nivel de seguridad ya que evitan ataques o el intento de duplicación de la clave privada, y son ideales para aplicaciones donde se desea garantizar al máximo la protección de la clave privada y donde se firman documentos pero no se cifran. Mientras que las iKey 1000/1032 son recomendadas en los esquemas donde se cifran documentos y se desea poder contar con un backup (guardado en una caja fuerte, por ejemplo) al que se pueda recurrir en caso de dañarse la llave original.

La tercera línea de productos está compuesta por las llaves electrónicas HARDkey MIO, ideales para ser utilizadas como alternativa a las llaves iKey en los esquemas donde no es imprescindible la utilización de Certificados Digitales, y es suficiente con contar con una autenticación fuerte por dos factores: "algo que tengo" la llave HARDkey MIO y "algo que conozco" su PIN de acceso.

Normalmente se firman "convenios entre partes" donde se acuerda utilizar cierta tecnología para la identificación de los usuarios, y son suficientes para hacerlos valer entre las partes ya que prevalecen sobre cualquier norma o ley general, con lo cual muchas veces no es imprescindible contar con tecnologías muy avanzadas, sino las más eficientes y económicas.

Las llaves HARDkey MIO son la mejor solución costo / beneficio con fácil y rápida implementación y sin costo de "START UP" ni de renovación anual como otras soluciones.

Podemos ofrecer una propuesta "escalable" para lograr una solución única para la "Validación de Accesos de Usuarios" por medio de un método seguro utilizando nuestras llaves HARDkey MIO, que permita ir implementando en forma escalonada niveles adicionales de seguridad.

En una primera etapa, todo acceso a aplicaciones con USUARIO y PASSWORD puede ser reemplazado o complementado fácilmente con la validación de una llave HARDkey MIO, con sólo agregar unas pocas líneas de código, en las aplicaciones o páginas web en las que se desea mejorar los niveles de seguridad. Esto es sólo un primer paso, pero resuelve los principales problemas de seguridad para la gran mayoría de los usuarios.

En una segunda etapa se puede incorporar para los usuarios más críticos, el uso de un CSP que permita con la misma llave HARDkey MIO (que ya se acostumbraron a utilizar en la etapa anterior) almacenar y transportar Certificados Digitales. Esto sólo implica adquirir la licencia del CSP e incorporarlo al esquema de validación.

De esta forma se puede dividir en etapas la solución, dejando la implementación del esquema de PKI para más adelante permitiendo incluso repartir en el tiempo, la inversión y la carga de trabajo que implican la implementación y puesta en marcha del esquema PKI completo.

Este esquema se puede lograr con las HARDkey MIO y con las iKey. Y en ambos casos se pueden incorporar otros módulos opcionales para los usuarios principales, que les permita controlar una misma llave el "LOGON a la PC", el "Almacenamiento y Administración de Password" (para no tener que recordar las password, y con sólo ingresar su PIN completar automáticamente este dato), tener un DISCO PRIVADO VIRTUAL CIFRADO, etc.