



Acceso Lógico Seguro: El Papel de las Tarjetas Inteligentes en una Autenticación Más Sólida

Informe de la Smart Card Alliance

Fecha de publicación: Octubre de 2004

Número de la publicación: ID-04002

Smart Card Alliance
191 Clarksville Rd.
Princeton Junction, NJ 08550
www.smartcardalliance.org
Teléfono: 1-800-556-6828

Sobre la “Smart Card Alliance Latin America” (SCALA)

Smart Card Alliance América Latina (SCALA por su sigla en inglés) es una asociación sin fines de lucro, no partidaria, con múltiples miembros de la industria, líder en acelerar la aceptación a gran escala de las múltiples aplicaciones de la tecnología de tarjetas inteligentes. La Alianza incluye entre sus miembros a compañías líderes en la rama bancaria, servicios financieros, computación, telecomunicaciones, tecnología, servicios de salud, industria de venta al detal, control de acceso, transporte y entretenimiento, así como una gran cantidad de agencias gubernamentales. A través, de proyectos específicos, como programas educativos, investigaciones de mercado, cabildeo, relaciones industriales y foros abiertos; SCALA mantiene a sus miembros conectados con los líderes de la industria y el pensamiento innovador. Smart Card Alliance es la voz unificada de la industria de tarjetas inteligentes, liderando la discusión de la industria sobre el impacto y el valor de las tarjetas inteligentes en los Estados Unidos y América Latina. Para mayor información, visite www.smartcardalliance.org/latinamerica.

Copyright © 2003 Smart Card Alliance, Inc. Todos los derechos reservados. La reproducción o distribución de esta publicación de cualquiera forma es prohibida sin permiso previo de la Smart Card Alliance. La Alianza ha hecho el mejor de sus esfuerzos para asegurar, mas no puede garantizar, que la información descrita en este informe está actualizada a la fecha de su publicación. La Smart Card Alliance no asume ninguna responsabilidad en cuanto a la veracidad, integridad o adecuación de la información contenida en este informe.

Miembros de la Smart Card Alliance: Los miembros podrán acceder a todos los informes sin costo alguno. Favor de Consultar la sección de “login” para miembros del sitio “web” de la Smart Card Alliance para obtener información sobre los derechos de reproducción y distribución para miembros.

Agencias Gubernamentales: empleados de gobierno pueden solicitar copias gratuitas de este informe contactando info@smartcardalliance.org o registrándose en la Smart Card Alliance como un miembro gubernamental...

Tabla-de Contenidos

RESUMEN EJECUTIVO.....	5
INTRODUCCIÓN.....	8
VISIÓN GENERAL DE ACCESO LÓGICO.....	10
MÉTODOS ACTUALES PARA ACCESAR REDES DE COMPUTADORAS.....	10
PROGRAMAS DE INTERFASE O “DRIVERS” PARA MÉTODOS DE ACCESO LÓGICO MÁS SÓLIDOS.....	11
<i>Costos administrativos</i>	11
<i>Riesgos de Seguridad</i>	11
<i>Riesgos del incumplimiento de las leyes y regulaciones</i>	12
<i>Robo de la Privacidad y la Identidad</i>	12
<i>Evolución y Migración de la Tecnología</i>	13
EL PAPEL DE LAS TARJETAS INTELIGENTES	13
VISIÓN GENERAL DE LAS TECNOLOGÍAS DE AUTENTICACIÓN.....	15
CONTRASEÑAS	15
<i>Contraseña de Texto no Cifrado (cleartext passwords en inglés)</i>	16
<i>Conversión de Contraseña (password conversions en inglés)</i>	17
<i>Contraseñas de un solo uso (One-time Passwords en inglés)</i>	18
FACTORES BIOMÉTRICOS	19
LLAVE PÚBLICA CRIPTOGRÁFICA.....	21
FICHAS FLEXIBLES	22
TECNOLOGÍA DE TARJETAS INTELIGENTES.....	22
RESUMEN	24
FACTORES CLAVES A CONSIDERAR PARA LA IMPLEMENTACIÓN DE UNA AUTENTICACIÓN MÁS SÓLIDA EN EL ACCESO LÓGICO	25
AMBIENTE CORPORATIVO	25
TRANSFORMACIÓN EN NEGOCIOS Y PROCESOS DE REINGENIERÍA	26
REDUCCIÓN DE COSTOS Y RECUPERACIÓN DE LA INVERSIÓN	27
SEGURIDAD Y PRIVACIDAD	28
GERENCIA, UTILIZACIÓN Y CAPACITACIÓN.....	29
BENEFICIOS DE LA TECNOLOGÍA DE TARJETAS INTELIGENTES PARA UN ACCESO LÓGICO	30
SÓLIDA AUTENTICACIÓN	30
SEGURIDAD INTEGRADA AL SISTEMA.....	31
INCREMENTO DE LA SEGURIDAD Y CONVENIENCIA PARA LOS USUARIOS	32
PROTECCIÓN MEJORADA CONTRA FRAUDES DE IDENTIDAD.....	33
COBERTURA DE APLICACIONES BASADOS EN ESTÁNDARES.....	34
FACILIDAD DE INTEGRACIÓN.....	35
FACILIDAD DE ENVÍO	37
FUNCIONAMIENTO MULTIPROPÓSITO.....	37
TARJETAS INTELIGENTES COMO DISTINTIVOS DE IDENTIFICACIÓN INTELIGENTES: EJEMPLO DE UN ESCENARIO.....	38
VENTAJAS SOBRE OTRAS ALTERNATIVAS PARA ACCESO LÓGICO	40
TARJETAS INTELIGENTES Y LA INFRAESTRUCTURA INFORMÁTICA (IT).....	41
MICROSOFT WINDOWS.....	41
<i>Comunicaciones entre las Tarjetas Inteligentes y el Lector</i>	42
<i>Autenticación del usuario</i>	44
<i>Servicios de la Red y Correos Electrónicos</i>	44
<i>Criptografía de Sistemas de Archivo</i>	44
<i>Soporte Ofrecido por Diferentes Versiones de Windows</i>	45

LINUX	45
<i>Comunicaciones Tarjetas inteligentes- Lector</i>	45
<i>Autenticación del usuario</i>	47
<i>Servicios de la Red y Correos electrónicos</i>	47
<i>Criptografía de Sistemas de Archivo</i>	47
<i>Soporte Ofrecido por Variedades Diferentes de Unix</i>	48
USO DE TARJETAS INTELIGENTES PARA APLICACIONES MÚLTIPLES.....	48
USO DE APLICACIONES MÚLTIPLES	48
<i>Control de Acceso Físico</i>	48
<i>Pagos</i>	50
<i>Almacenaje y Administración de Datos Seguro</i>	51
<i>Acceso de la Red inalámbrica</i>	51
INSTALACIÓN DE LA APLICACIÓN.....	51
EJEMPLOS DE LA APLICACIÓN MÚLTIPLES	52
PROPUESTA DE NEGOCIO PARA TARJETAS INTELIGENTES Y ACCESO LÓGICO.....	53
BENEFICIOS INTANGIBLES	53
<i>Cumplimiento de las Regulaciones</i>	53
<i>Posicionamiento Estratégico</i>	53
BENEFICIOS TANGIBLES	54
<i>Simplificación en la administración del usuario</i>	54
<i>Eliminación de Fichas de OTP</i>	55
<i>Reducción de Infraestructura Global</i>	55
<i>Incrementando la Productividad</i>	55
INVERSIÓN	55
CONCLUSIONES	57
REFERENCIAS Y FUENTES	58
RECONOCIMIENTOS DE LA PUBLICACIÓN	60
APÉNDICE A: DEFINICIÓN DE TÉRMINOS Y SIGLAS	62

Resumen Ejecutivo

Las Contraseñas Proveen Insuficiente Seguridad para Acceso Lógico a los Recursos de la Red

Organizaciones de todos los tamaños y de todas las industrias están ansiosas por mejorar el proceso para identificar a los usuarios de sus sistemas de redes. Con el incremento del uso de redes cableadas e inalámbricas para acceder a recursos de información y el incremento de robos de identidad y ataques a redes corporativas, la autenticación de usuarios basada en claves de acceso se ha convertido en un riesgo significativo. Las contraseñas de acceso son comúnmente controladas por el propietario de éstas, quien puede usar una clave fácil de adivinar, compartirla con otros, escribirla, o usar la misma para acceder a múltiples sistemas. En adición, el hecho de almacenar información sobre claves de acceso en redes corporativas añade aún más vulnerabilidad para atacantes que ganan acceso a las redes.

La administración mediante contraseñas de acceso representa un costo significativo para las organizaciones. Las estadísticas de la industria muestran que del 30% al 50% de los recursos de soporte técnico de los sistemas de información (IT) son consumidos por el manejo y cambio de contraseñas de acceso.

Tanto las agencias gubernamentales como las empresas están reemplazando simples claves de acceso por otros sistemas multifactoriales de autenticación que fortalecen la seguridad de la información, responden al mercado y a las condiciones regulatorias y abaratan los costos de soporte técnico.

Una Variedad de Tecnologías pueden Autenticar a los usuarios para un Acceso Lógico

Las tecnologías usadas para autenticar la identidad de los individuos que utilizan un acceso lógico, incluye contraseñas de acceso (con un número de variaciones – texto simple, cifrados, de un solo uso), claves de acceso simétricas, claves de acceso público/ privado asimétricas e información biométrica. Los individuos comúnmente prueban su identidad usando un solo factor de autenticación. Sin embargo, un sistema de autenticación de identidad más sólido requiere el uso de dos o tres factores, tales como algo que tú tienes (un objeto o una ficha que tú posees), algo que tú sabes, (información que sólo tú sabes), o algo que tú eres (una cualidad física única o conducta que te diferencia de los demás).

Las tarjetas inteligentes respaldan todas las tecnologías de autenticación, almacenamiento de archivos de contraseñas de acceso, certificados de infraestructura de claves públicas, archivos semilla (seed files en inglés) de contraseñas de un solo uso y plantillas biométricas de imagen, así como, la generación de pares de claves de acceso asimétricas. Una tarjeta inteligente usada en combinación con una o más tecnologías de autenticación, provee mayor autenticación multifactorial y aumenta significativamente la seguridad de acceso lógico. La tecnología de tarjeta inteligente (Smart Card en inglés) también provee la flexibilidad para incluir todos los factores de autenticación en una sola tarjeta inteligente, incrementando la seguridad y la privacidad de todo el proceso de autenticación.

La Tecnología de Tarjetas Inteligentes Provee una Significativa Ventaja para Implementar una Autenticación más Sólida.

La Tecnología de Tarjetas inteligentes fortalece significativamente la seguridad, protegiendo tanto la credencial electrónica usada para autenticar a un individuo para un acceso lógico como el dispositivo físico. Desde que la credencial es almacenada permanentemente en la tarjeta, esta nunca está disponible en un programa (software) o en la red para que un usuario no autorizado la pueda robar. Las tarjetas inteligentes construyen protección dentro del dispositivo físico, respaldando las características de resistencia contra manipulación y técnicas de seguridad activa para encriptación de las comunicaciones.

Las tarjetas inteligentes se están convirtiendo en el método preferido de acceso lógico, no solo por su seguridad incrementada, sino también por su facilidad de uso, amplia cobertura de aplicación, su facilidad de integración con la infraestructura IT y su funcionalidad multipropósito. Los sistemas operativos de Microsoft® Windows® y Unix® ofrecen un significativo nivel de respaldo y funcionalidad en relación con la tarjeta inteligente, ya sea con un respaldo incorporado (fuera de la caja o “out-of-the-box”) o añadiendo un paquete de programas comerciales. La tarjeta inteligente basada en acceso lógico permite a las empresas emitir una sola tarjeta de identificación que respalda el acceso lógico, el acceso físico y almacenamiento de información segura, a la par con otras aplicaciones. Al combinar múltiples aplicaciones en una sola tarjeta de identificación, las organizaciones pueden reducir costos, incrementar la conveniencia del usuario final y proveer seguridad mejorada para diferentes aplicaciones.

La tecnología de Smart Card provee a las organizaciones con un acceso lógico rentable. Las tarjetas inteligentes conllevan una propuesta de negocios positiva para implementar cualquier tecnología de autenticación. Incrementar la productividad del usuario, reducción de costos de administración de contraseñas, reducir la exposición al riesgo, procesos de negocios alineados. Todo esto contribuye a un significativo y positivo retorno sobre la inversión.

Acerca de este informe

Este informe fue desarrollado por la Smart Card Alliance con miras a proveer una primicia de las tecnologías de autenticación usadas para accesos lógicos y para describir cómo las tarjetas inteligentes fortalecen los procesos de autenticación.

Diseñado como una visión general educativa para los tomadores de decisiones, este informe provee respuestas para las preguntas comúnmente hechas sobre el uso de las tarjetas inteligentes para acceso lógico, tales como:

- ¿Por qué las organizaciones buscan soluciones más sólidas de autenticación para acceso lógico a recursos de redes?
- ¿Qué tecnologías de autenticación están disponibles y como se comparan unas a otras?
- ¿Cómo son usadas las tarjetas inteligentes para autenticación y que beneficios traen para la empresa?
- ¿Cómo son integradas las tarjetas inteligentes en la infraestructura de informática (IT)?

-
- ¿Cuál es la propuesta de negocio para utilizar tarjetas inteligentes para acceso lógico?
 - ¿Qué otras aplicaciones pueden ser respaldadas usando la tecnología de tarjetas inteligentes de identificación, y cómo una tarjeta funciones múltiples beneficia a la organización?

El informe incluye perfiles de organizaciones que actualmente están usando tarjetas inteligentes de identificación para acceso lógico, como por ejemplo Boeing, Microsoft, Rabobank, Shell, Sun Microsystems, el Departamento de Defensa de los Estados Unidos y el Departamento de Estado.

Introducción

En los centros de trabajo de hoy en día, un acceso lógico seguro es una preocupación crítica. El Internet ha facilitado colaboración efectiva entre socios, clientes y proveedores. Nuevas tecnologías permiten a los trabajadores de campo comunicarse fuera de los perímetros de la seguridad tradicional, usando tecnología inalámbrica o trabajar remotamente sobre una red virtual privada (VPN). Las crecientes eficiencias operacionales motivan a un número cada vez mayor de empresas y organizaciones de servicio (tales como bancos y compañías de salud y seguros) para evolucionar a una red de negocios compuesta por portales corporativos, servidores de aplicación, y recursos Web protegidos. El creciente incremento de incidencia de robos de identidad y el advenimiento de nuevas regulaciones y legislaciones, tales como la "Health Insurance Portability and Accountability Act" (HIPAA), "Sarbanes-Oxley Act", y "Gramm-Leach-Bliley Act", también contribuyen a un ambiente en el cual un acceso lógico seguro es extremadamente importante. Por todas estas razones, organizaciones que manejan identidades de usuarios, políticas de autenticación y privilegios de usuarios están cambiando para prevenir que intrusos tengan acceso a información propietaria.

La infraestructura de acceso lógico actual, basada en el uso de contraseñas, falla en el manejo de estas nuevas amenazas, los nuevos modelos de negocios y el complejo crecimiento en el acceso a los recursos de la red. Las contraseñas son costosas en su manejo (un estimado del 30 % al 50 % de los costos de soporte técnico son atribuibles al reajuste de contraseñas de acceso) y pueden ser quebrantadas utilizando una amplia variedad de herramientas. Las preocupaciones suscitadas como resultado del uso de sistemas basados en el acceso por contraseñas y la conveniencia agregada que ofrecen las tarjetas inteligentes, pueden ser las dos principales razones por las que las organizaciones están emigrando al uso de sistemas de acceso lógico basados en tarjetas inteligentes. Según un sondeo realizado por Frost & Sullivan,¹ el 39% de las compañías pertenecientes al Grupo Fortuna 500, planean utilizar tarjetas inteligentes en los próximos tres años y el 63 % de las 500 compañías pertenecientes al Grupo Fortuna 500 ya han investigado o están investigando tarjetas inteligentes para la implementación de sus redes de seguridad.

La tecnología de tarjetas inteligentes esta disponible en múltiples formas, tales como, tarjetas plásticas, (Universal Serial Bus) un dispositivo periférico externo (USB), o una tarjeta SIM (Subscriber Identification Module) en un teléfono celular. Cada una de ellas tiene un chip semiconductor que puede tener un microcontrolador, un cripto-coprocesador, memoria, un sistema operativo y un programa de aplicación. La capacidad computacional de las tarjetas inteligentes, iguala a la capacidad computacional de la primera computadora personal (PC); las tarjetas inteligentes poseen todas las características de una computadora, excepto un teclado y un monitor. Los microcontroladores basados en las tarjetas Inteligentes están diseñadas para resistir ataques utilizando una variedad de contramedidas cifradas en el chip por el fabricante, haciéndolo inverosímil que los datos almacenados en la tarjeta inteligente sean expuestos, robados, modificados, o destruidos. La capacidad única de las tarjetas inteligentes de proporcionar almacenaje de datos seguro y respaldar las sofisticadas funciones criptográficas la

¹ "Fortune 500 Companies' Preference for Corporate Security Applications," Frost & Sullivan, Feb. 17, 2003

convierten en la mejor opción para autenticar a individuos que solicitan un acceso lógico.

La tecnología de Tarjetas Inteligentes ha evolucionado durante los últimos 20 años, incluyendo un incremento en las capacidades de procesamiento y almacenaje, mayor seguridad, programas (software) maduros de manejo de tarjetas inteligentes, tecnologías sin contacto e integración de múltiples aplicaciones en un solo distintivo de identificación inteligente. Las Tarjetas Inteligentes pueden utilizar una variedad de aplicaciones utilizadas por organizaciones que incluyen, registrarse a Windows, administración de contraseñas, contraseñas de un solo uso (One Time Passwords OTP), autenticación VPN, criptografía de correos electrónicos y de datos, firmas electrónicas, entrada única al sistema de empresas, acceso a redes inalámbricas de manera segura, autenticación biométrica, pagos de cafetería, almacenamiento de información personal, acceso basado en roles, acceso físico seguro y lealtad del cliente. Hoy en día las tarjetas Inteligentes son esenciales en la solidez de la seguridad de los sistemas de manejo de identificación de las organizaciones, respaldando la sólida autenticación requerida para validar el acceso de individuos a los recursos red y proveyendo un crítico primer paso para bloquear a intrusos.

El trabajo de estandarización llevado a cabo por **"Global Platform"** y el **"Government Smart Card Interoperability Specification"** (GSC-IS) capacita a los que emiten tarjetas, el combinar soluciones de múltiples recursos, asegurando, por ende, interoperabilidad a larga escala y reduciendo los costos de propiedad al proveer un mercado abierto. Debido a las significativas inversiones que aún se requieren para integrar nuevos sistemas de autenticación dentro de una infraestructura preexistente, un compromiso continuo por parte de los altos ejecutivos y una dedicada administración del proyecto, son necesarios para hacer exitoso el nuevo sistema de administración de identidades y su implementación. Las organizaciones que adopten el uso de las tarjetas inteligentes para acceso lógico, ven un sólido retorno de sus inversiones y significativos beneficios, incluyendo mejoramientos en conveniencia y seguridad, mayor responsabilidad y mejores decisiones de seguridad, conformidad con las regulaciones, eficiencias operacionales y nuevas oportunidades de negocios.

Este informe explica los conceptos necesarios para entender que son las tecnologías de autenticación usadas para acceso lógico y cómo las tarjetas inteligentes pueden ser usadas para hacer el acceso lógico más seguro. Muchas organizaciones han utilizado las tarjetas inteligentes exitosamente en sus sistemas de acceso lógico, y los perfiles de siete de ellas -Boeing, Microsoft, Rabobank, Shell, Sun Microsystems, el Departamento de Defensa de los U.S., el Departamento de Estado de los U.S. – son incluidos en el apéndice de este informe.

Visión General de Acceso Lógico

Acceso lógico es el proceso mediante el cual se le permite a los individuos usar los sistemas computacionales (el cual puede incluir otros dispositivos digitales tales como agendas electrónicas (**PDAs**) y teléfonos celulares) y la red a la cual esos sistemas son unidos (tales como redes de áreas de uso corporativo y redes de área de uso abiertas, redes y telecomunicaciones, intranets/extranets, y redes sin cableado). El objetivo de acceso lógico seguro es asegurar que estos dispositivos y redes, y los servicios que ellos proveen, estén disponibles sólo a aquellos individuos autorizados para usarlos. La autorización es típicamente basada en algún tipo de relación predeterminada entre la red, el propietario del sistema y el usuario, como el suscriptor que paga, un empleado, un cliente o algún otro tipo de relación estrecha.

El sistema que conlleva el respaldo de tales servicios de red representa una significativa inversión; de hecho, este sistema puede representar el mayor activo propiedad de la organización. Estos activos requieren protección para evitar el uso por individuos u organizaciones no autorizados, quienes pudieran disminuir o destruir su valor. Por lo tanto, controlar el acceso a esos activos es de una importancia suprema para prácticamente todas las organizaciones que dependen de los sistemas de tecnología de la información (IT) para lograr sus objetivos.

Métodos Actuales para Accesar Redes de Computadoras

El método ampliamente más implementado para controlar el acceso lógico es la relación de la identidad del usuario con la contraseña. Los usuarios proveen su contraseña de identificación (usualmente el nombre del usuario), y un secreto que sólo el usuario conoce (usualmente una contraseña). Un simple buscador de datos programado determina que la contraseña está ligada al usuario, autenticando la identidad del usuario y garantizando el acceso. Cada sistema o aplicación, por lo general, asigna una identificación única del usuario y combina la contraseña de cada usuario y luego determina los niveles de control de acceso para ese usuario, basándose en esa identificación única del usuario.

Con el tiempo, sin embargo, este tipo de autenticación ha probado que es débil e ineficiente. La identificación de usuarios y contraseñas pueden ser comprometidas fácilmente con una variedad de bien conocidas técnicas. Cuando esta clase de información es obtenida por elementos criminales, esta puede ser usada para lograr una entrada ilegal y no autorizada a una red. Los resultados de controles de accesos comprometidos pueden ser desastrosos para el propietario de la red y para el usuario cuya red o sistema de identidad es robado. Adicionalmente, las identidades del usuario son típicamente manejadas aplicación por aplicación, creando ineficiencias operacionales en la medida en que los sistemas y aplicaciones en una organización crecen e introducen vulnerabilidades a la seguridad, dado que se torna cada vez más difícil controlar las políticas que establecen el uso de esas identidades.

Afortunadamente, están disponibles nuevas tecnologías que pueden fortalecer el proceso de autenticación, respaldando los controles de acceso y proveer niveles más altos de garantía asegurando que los usuarios son los que ellos dicen ser y que las credenciales de identidad presentadas son válidas. Estas tecnologías, las cuales son descritas en las siguientes secciones, generalmente emplean técnicas de cifrado, información

biométrica de algún tipo y/o la posesión de amuletos físicos o credenciales para mejorar la efectividad de los sistemas de control de acceso. A diferencia del uso de solamente un elemento (por ejemplo, la combinación de acceso de identificación de usuario y contraseña), la sólida autenticación requiere el uso de dos o tres factores para validar la identidad. Los factores podrían incluir alguna combinación de algo que tú sabes (una contraseña o el número de identificación personal que sólo tú conoces), algo que tú tienes (un objeto físico que posees) y algo que tú eres (una característica física o comportamiento que te distinga de otros individuos).

El uso de poderosas tecnologías de autenticación y múltiples factores de autenticación atenúa la pérdida potencial de información debido al acceso desautorizado a los activos de la red.

Programas de Interfase o “Drivers” para Métodos de Acceso Lógico Más Sólidos

Comprometer la seguridad no es la única razón por la cual se investigan mejoras en las técnicas de controles de acceso lógicos. Otras desventajas en el uso de una combinación de contraseña e identificación incluyen los altos costos administrativos, la capacidad inadecuada de manejar diversos riesgos y la incapacidad para aprovechar la seguridad adicional con la cual se están construyendo los sistemas computacionales y sus aplicaciones.

Costos administrativos

En la medida en que los usuarios acceden a un número cada vez mayor de servicios de la red, cada uno requiriendo una identificación y contraseña independiente, la habilidad de los usuarios para administrar y recordar información de acceso requerida se reduce. Como resultado, los usuarios tienen que escribir la información, lo cual lo hace vulnerable, o llaman a sus administradores de red. Los administradores de red por lo general tienen que lidiar con llamadas de los usuarios que han olvidado su combinación de contraseña e identificación.

Dichas llamadas de servicio son muy costosas y están en aumento, así como el incremento de los servicios que se ofrecen en un número cada vez mayor de redes. Muchas fuentes estiman que una sola llamada a un administrador para que reactive una contraseña olvidada tiene un costo aproximado de cuarenta dólares. Los costos asociados al respaldo de este método de autenticación y control de acceso están llevando a los administradores de red a buscar soluciones que sean más eficientes al igual que más confiables.

Riesgos de Seguridad

Recientemente, se han multiplicado los reportes de individuos no autorizados invadiendo las redes computacionales para robar información con propósitos financieros o políticos.

En el sector privado, el impacto de tales brechas de seguridad es medido en términos tanto de pérdidas financieras como de pérdida de la confianza del cliente. En los círculos gubernamentales, el riesgo es ampliado por el efecto potencial sobre la seguridad nacional y el impacto en la credibilidad pública y la confianza en organizaciones gubernamentales críticas.

En la medida en que ocurran más intromisiones, la habilidad para cuantificar su impacto negativo está aumentando. Instituciones tanto en el sector público como en el privado son más capaces de analizar los costos y beneficios de invertir en nuevas tecnologías para mejorar la seguridad de las redes, incluyendo tecnologías para mejorar el control de acceso y son capaces de justificarlo basados en sólidos retornos de inversión.

Riesgos del incumplimiento de las leyes y regulaciones

A raíz de los ataques terroristas del 11 de septiembre, una cantidad significativa de nuevas legislaciones han sido aprobadas, primariamente encaminadas a mejorar las redes de computadoras propiedad y administradas por el Gobierno Federal. Legislaciones adicionales promueven la adopción de sistemas que manejen los servicios gubernamentales electrónicamente. Una parte crítica de estas iniciativas es el respaldo para la autenticación lógica de individuos tratando de acceder a esos servicios.

Como resultado de ello, las redes y mecanismos de seguridad por medio de los cuales los usuarios tienen acceso a activos controlados por el gobierno se han colocado entre las prioridades de la agenda gubernamental. Las políticas y guías de implementación definen varios de los niveles de autenticación que son necesarios, basados en la sensibilidad de la información a acceder y una variedad de opciones de tecnologías candidatas han sido identificadas, que van desde la identificación del usuario y de su contraseña de acceso hasta infraestructuras de clave pública (PKI), biométricas y tarjetas inteligentes. Muchas agencias gubernamentales de Estados Unidos ya han implementado programas para emitir tarjetas inteligentes de identificación que respalden técnicas de autenticación más eficientes tanto para acceso físico como lógico.

De hecho, el gobierno ya exige a los contratistas que cumplan con estándares específicos para tecnologías, políticas y prácticas de seguridad. La tendencia del sector privado es adoptar tecnologías y prácticas implementadas por el gobierno, no sólo como un ejemplo de mejores prácticas, sino también como un medio para mitigar cualquier riesgo legal en que se pudiera incurrir por la no conformidad de estas. Los negocios están también sujetos a un número de nuevos requisitos de control de acceso y auditoria, como resultado de nuevas leyes y regulaciones tales como "Gramm-Leach-Bliley Act", HIPAA, el "Sarbanes-Oxley Act", y el "USA Patriot Act".

Robo de la Privacidad y la Identidad

De acuerdo con la "Federal Trade comisión",² en los últimos 5 años, 27.3 millones de americanos fueron víctimas de robos de identidad, en tanto que negocios e instituciones financieras perdieron cerca de \$48 billones de dólares a manos de los ladrones de identidad y por su parte las víctimas también incurrieron en gastos de su bolsillo por el orden de los \$ 5 billones por el mismo motivo. Los ataques en los computadores de los consumidores a través del fraudulento método denominado "phishing" y otros virus y ataques de "spyware", constituyen nuevas formas para robar los nombres de usuarios y las contraseñas. "Gartner" reporta que más de 1.4 millón U.S. de adultos han sufrido fraude por robo de identidad debido a ataques de

² "FTC Releases Survey of Identity Theft in U.S. 27.3 Million Victims in Past 5 Years, Billions in Losses for Businesses and Consumers," Federal Trade Commission press release, Sept. 3, 2003, <http://www.ftc.gov/opa/2003/09/idtheft.htm>

“phishing”, lo cual ha costado a los bancos y a los emisores de tarjetas de crédito alrededor de \$1.2 billón en pérdidas el año pasado.³

En la medida en que el robo de identidad se convierte cada vez más en un asunto de mayor interés (y es tema de discusión legislativa a nivel estatal y nacional), el sector privado tendrá que establecer métodos más estrictos de control en bases de datos de los clientes y la información personal que las empresas se han comprometido a proteger. Las compañías necesitarán controlar el acceso a información sensible y asegurar que dicha información es sólo accesible a aquellos con la autorización apropiada.

Evolución y Migración de la Tecnología

Debido a la creciente demanda de los usuarios de sistemas de información que requieren mejores mecanismos de control de acceso, los proveedores de sistemas de información están ofreciendo mayor seguridad en sus productos con el fin de proveer respaldo incorporado para las soluciones modernas de autenticación. Por ejemplo, el Windows ahora viene con respaldo para registro PKI y correo cifrado y firmado digitalmente. Más y más productos de una vasta variedad de vendedores permiten el uso de tecnología PKI, biométrica y tecnología de tarjetas inteligentes para respaldar métodos más poderosos de autenticación utilizando múltiples factores.

En la medida en que los sistemas computacionales son actualizados con el correr del tiempo, el respaldo tecnológico para lograr medidas de autenticación más poderosas a través del uso de múltiples tecnologías será más fácil de obtener. Como resultado de ello debería darse un creciente aumento en el uso de técnicas más poderosas de autenticación, mayores niveles de acceso de seguridad y mayor conveniencia para el usuario.

El Papel de las Tarjetas Inteligentes

La tecnología de tarjetas inteligentes puede desempeñar un rol clave en las soluciones que proveen poderosas respuestas de autenticación, una red de seguridad mejorada y protección de las identidades y privacidad de los individuos. Al igual que un dispositivo criptográfico, el microcontrolador en el corazón de la tarjeta inteligente puede respaldar un amplio número de usos y de tecnologías de seguridad. Las tarjetas inteligentes ofrecen almacenamiento seguro de datos y respaldan poderosas medidas de autenticación requeridas para acceder a la información, incluyendo lo siguiente:

- Soporte para aplicaciones de claves de acceso asimétricas y de PKI (por ejemplo, firmas digitales y encriptación de mensajes de correo electrónico), generadores de claves de acceso incorporados a la tarjeta, y protección para la privacidad de la clave de acceso del usuario.
- Almacenamiento seguro para plantillas biométricas
- Almacenamiento seguro de la identidad del usuario y de su contraseña de acceso
- Respaldo para la generación de contraseñas de acceso de un solo uso
- Almacenamiento seguro para llaves de acceso simétricas
- Respaldo para otras aplicaciones como accesos físicos de control de transacciones financieras

³ “Phishing Victims Likely Will Suffer Identity Theft Fraud,” Gartner press release, May 14, 2004, http://www3.gartner.com/5_about/press_releases/asset_71087_11.jsp

En su forma de formato, la tecnología de tarjetas inteligentes también puede ser utilizada en una placa de identificación de función múltiple, proveyendo una tarjeta de identificación visual así como permitiendo el acceso automatizado, autenticando accesos físicos y lógicos.

Visión General de las Tecnologías de Autenticación

En la historia de *Ali Babá y los Cuarenta Ladrones*, un tesoro robado por 40 ladrones es escondido en una cueva protegida por una roca mágica. La única forma de entrar a la cueva es pronunciar la palabra secreta “Ábrete Sésamo”. No importa quién la diga, aquellas palabras pronunciadas en la forma correcta, hacían que algo mágico sucediera, moviendo la roca y permitiendo al que las decía entrar.

Esta misma magia sucede cuando alguien accesa a una red de computadoras. La importancia de la autenticación no puede ser exagerada. Una vez que una persona es autenticada dentro de la red, los privilegios y derechos de acceso de ella serán basados bajo esa autenticación. El propósito de autenticación es, por lo tanto, permitir acceso a la red a cada usuario que está autorizado, manteniendo aquellos que no están autorizados fuera de ésta. La meta final de cada autenticación es negarles el acceso a impostores sin causarles molestias a los usuarios válidos.

Varios enfoques están dirigidos a lograr esa tarea vital. Todo descansa en la incorporación de uno o más de los tres factores críticos para la autenticación:

- Algún conocimiento que tenga la persona, tal como una contraseña. Este factor tiene que ver comúnmente con “algo que tú conoces”.
- Alguna característica física, como una huella digital. Este factor tiene que ver comúnmente con “algo que tú eres”.
- Algo que la persona posee, tal como una llave, una ficha, o una tarjeta inteligente. Este factor es comúnmente se refiere a “algo que tú tienes”.

Cada acercamiento individual es diseñado de forma única con el fin de autenticar a cada usuario de la manera más completa posible, sin crear gran incomodidad. También cada uno tiene una debilidad potencial. Usado en combinación, se fortalece la autenticación reduciendo la posibilidad de que un impostor accese.

Contraseñas

La contraseña es sin lugar a dudas la técnica de control de acceso de mayor uso. El usuario simplemente provee un nombre de usuario y contraseña, suministra la información, y se le autoriza o niega el acceso. Dentro de la computadora, este método de autenticación compara el nombre y contraseña del usuario para almacenar la información. Una respuesta electrónica garantiza o niega el acceso basado en el resultado de esta comparación. Proteger los nombres de usuarios, las contraseñas y la relación entre estos, es, por lo tanto, crítico para controlar el acceso lógico con contraseñas.

Existen muchas maneras para que individuos no autorizados puedan obtener acceso a las contraseñas. Algunas de los métodos más comunes son:

- **Ingeniería social (social engineering en inglés)** es probablemente la forma más conocida para obtener acceso a un sistema. Por ejemplo, individuos no autorizados usan halagos o razonamientos lógicos para obtener la contraseña de otra persona. Este riesgo es fácilmente mitigado educando a los usuarios acerca de la necesidad de una mayor y más eficiente seguridad.

- **Programas para abrir contraseñas (password cracking programs en inglés)** usan ya sea fuerza bruta o métodos de búsqueda de diccionario para intentar descifrar contraseñas protegidas.
- **Programas olfateadores (sniffer programs en inglés)** monitorean paquetes de información que viajan dentro de la red. Si una contraseña no cifrada pasa cerca, el olfateador la captura y la usa, comprometiendo la integridad del sistema. Sin embargo, la efectividad de las herramientas de olfateo ha disminuido con la amplia adopción de interruptores de redes y ruteadores, reduciendo grandemente la utilidad de las herramientas de olfateo.
- **Conocimiento personal** acerca de usuarios legítimos es usado para tratar de adivinar sus contraseñas.
- **Acceso a las estaciones de trabajo de los empleados.** Una persona se puede sentar en el escritorio de un empleado cuando no hay nadie cerca y buscar contraseñas que hayan sido escritas.
- **Mira y ve.** La forma más fácil de obtener una contraseña es mirar a la persona cuando la escribe en el teclado.

Con miras a salvaguardar la integridad de la contraseña, las políticas de seguridad requieren que los usuarios cambien sus contraseñas continuamente para impedir acceso a sus cuentas a través de métodos tales como hallar contraseñas escritas, ver a la persona registrar su contraseña, mediante el uso de programas de olfateo de teclado o adivinando. Tales políticas de seguridad de contraseñas son efectivas pero pueden llegar a ser bastante complicadas. Estas políticas usualmente señalan a los usuarios no reutilizar las contraseñas, obligándolos a crear nuevas que sean tan “difíciles de adivinar” por otros y fáciles de recordar para ellos. La protección de información almacenada es también crítica para una política de fortalecimiento de medidas de seguridad.

Las contraseñas pueden ser implementadas en una gran variedad de formas. En todos los casos, se recomienda la implementación de una fuerte política de medidas de seguridad. La política puede ser tan simple como pedir un número mínimo de letras, puede requerir la inclusión de letras mayúsculas y minúsculas, números y caracteres especiales.

Contraseña de Texto no Cifrado (cleartext passwords en inglés)

La forma más elemental de almacenamiento de contraseñas es mediante el uso de contraseña de texto o “cleartext” (es decir, no cifrado) en donde las contraseñas y los nombres de usuarios son almacenados en un fichero plano el cual es almacenado en la red. Este tipo de archivo tiene la siguiente apariencia:

USUARIO	CONTRASEÑA
AliceZ	myDOGsparkY
BobY	Home4holidays
CarolW	getthejobdone

Este acercamiento es fácil de implementar. El desafío recae en proteger la información contra el acceso o la manipulación inadecuada mientras que el archivo conserva la accesibilidad inmediata para el proceso de la conexión. Mientras que este acercamiento es apropiado para ciertas situaciones, es

extremadamente vulnerable a un ataque. Una vez que los atacantes descubren cómo la función de la conexión trabaja y determinan que las contraseñas son mantenidas en el fichero plano, el acceso se simplifica grandemente. Una vez dentro del sistema, el atacante lee simplemente el archivo y obtiene los privilegios y el acceso de la red que estén registrados en las cuentas existentes de los usuarios.

Conversión de Contraseña (password conversions en inglés)

Para atenuar la vulnerabilidad de almacenar contraseña de texto no cifrado, tres enfoques dependen en las técnicas que convierten la contraseña introducida por el usuario del texto no cifrado a otra forma de datos:

- Producción de un número único para cada entrada en una base de datos o “Hashing”
- Códigos de autenticación de mensajes o “Message Authentication Codes” (MACs)
- Criptografía

Los tres enfoques potencialmente sufren de la misma vulnerabilidad: todos dependen de la capacidad de la gente de elegir las contraseñas que son fáciles de recordar (sin tener que anotarlas), pero suficientemente complejos para resistir un ataque. Convertir una contraseña protege la forma almacenada de la contraseña, de forma tal que elimina el acceso a la base de datos de la contraseña. Sin embargo, la contraseña por si misma sigue siendo potencialmente vulnerable ante la adivinanza o la reproducción del husmeador o “sniffed replay” (en donde el atacante intercepta los datos que contienen la contraseña y extrayendo de esta la información).

“Hashing”. Hashing, conocido a veces como un resumen del mensaje, utiliza un algoritmo matemático unidireccional que crea un resultado de longitud fija de un mensaje de cualquier longitud. Hashing esencialmente crea una huella digital de un mensaje y en este caso, se utiliza para proteger contraseñas. Hashing cambia una contraseña a un formato binario y la divide en bloques de código de un tamaño predeterminado. Cada bloque después se procesa a través del algoritmo de hash y se combina con el siguiente bloque no procesado para que sea procesado nuevamente hasta que se hayan procesado todos los bloques.

El resultado entonces se reconvierte a texto ASCII. Hashing es un método confiable para convertir contraseñas porque el resultado de alimentar la misma contraseña en el mismo algoritmo es siempre igual. Sin embargo, virtualmente ningún acercamiento matemático o lógico puede obtener la contraseña original del resultado.

Los dos algoritmos de “Hashing” más populares son MD5, que produce un hash de 128 bits procedentes de cualquier entrada, y el Secure Hash Algorithm (SHA), diseñado para ser usado con el Estándar de Firma Digital o “Digital Signature Standard”, creado por el “National Institute of Standards and Technology” (NIST) y la “National Security Agency” (NSA). El SHA-1 produce unos 160 bits de hash.

Una contraseña SHA-1 sometida al proceso “hash” luce así:

USUARIO	CONTRASEÑA
AliceZ	c0f1ce0662f4a2f8d86613cf2e7ddc311fbcf3bd
BobY	6dc04707c1204dac18b73e5b388365deac43f70c
CarolW	2a70467b07eb3acfb90944c90e0261a5cb44649d

Message Authentication Codes. (MAC) .La protección de las contraseñas que usan un código de la autenticación del mensaje (MAC) depende de un proceso que primero somete al proceso “hash” la contraseña y entonces agrega una clave criptográfica simétrica. La seguridad es realizada por el hecho de que la contraseña sometida al proceso de “Hash” está cifrada. La localización verificada compara la contraseña a un valor almacenado.

La contraseña está preparada comúnmente para el transporte dentro de la computadora usada para conectarse a la red. Al igual que “hashing”, los MACs protegen las contraseñas solamente después que se registran.

Criptografía.

Las contraseñas se pueden también proteger usando la criptografía. Un algoritmo criptográfico, residiendo generalmente en la computadora de registro primario, cifra la contraseña y la envía a la localización en donde residen los datos de la contraseña .La contraseña entonces se compara a los datos almacenados y el resultado se envía de nuevo a la computadora inicial de registro.

Los algoritmos criptográficos simétricos se utilizan comúnmente, puesto que son rápidos y robustos. A diferencia de “hashing” y del MACs, la longitud resultante varía en relación con la longitud de la contraseña.

Un archivo de contraseñas cifradas luciría así:

USUARIO	CONTRASEÑA
AliceZ	60135d5b849c2700dc60ffc2606fb947
BobY	0c0dd92d4bd8d8ca864441d23e066d8b
CarolW	7b94228224366ce3b2a049acaa0bd3c2

Contraseñas de un solo uso (One-time Passwords en inglés)

Las contraseñas de un solo uso (OTPs) fueron desarrolladas para lidiar con los problemas generados por usuarios determinados, contraseñas fijas y con la administración de políticas de seguridad para el manejo de contraseñas. Las OTPs usan un algoritmo de tiempo-basado con un generador del número aleatorio que es único para cada usuario individual.

Cada vez que el usuario es autenticado por el sistema, se utiliza una contraseña diferente, después de lo cual esa contraseña caduca. La contraseña es computada, ya sea por un programa al registrarse al computador o por fichas del “hardware” OTP, que posee el usuario, que son coordinados a través de un sistema confiable.

Software-basado en OTPs. Los programas basados en OTP residen totalmente en la red y el ordenador central. Uno de los programas más

comunes basados en OTP es S/KEY®, que está disponible de forma gratuita en el Internet y se utiliza como ejemplo en la siguiente discusión.

S/KEY utiliza una combinación de una contraseña permanente de S/KEY que nunca se envía en la red y una llave de acceso de un solo uso. Cuando el usuario se conecta con la máquina remota, una caja de diálogo exhibe una llave de un solo uso y solicita una contraseña. La llave de un solo uso y la contraseña permanente de S/KEY del usuario se registran en una máquina local del cliente usuario de S/KEY, que entonces genera una contraseña que permita la conexión. Cada vez que el usuario se conecta con la máquina remota, la llave de un solo uso cambia; sin embargo, la contraseña permanente de S/KEY del usuario sigue siendo igual.

Una de las ventajas alegadas para este enfoque es que los secretos no se guardan en el servidor anfitrión. Sin embargo, el servidor necesita guardar el OTP utilizado recientemente para la autenticación. Por esta razón los programas basados en OTPs son vulnerables a los intrusos que obtienen los privilegios de raíz del servidor.

Fichas OTP. OTPs basados en “hardware” son generados por una ficha física u otro dispositivo que los usuarios llevan consigo. La generación de la contraseña se basa, ya sea basada en tiempo en algoritmos basados en tiempo o algoritmos de desafío – respuesta.

El algoritmo más popular basada en tiempo es incorporado en el producto de RSA SecurID. En esta implementación, el usuario lleva una ficha especial que genera y exhibe un número de seis-dígitos que cambia cada 60 segundos. Para ingresar en un sistema, el usuario incorpora un nombre de usuario y utiliza el número seis dígitos como la contraseña. Un servidor hospeda un programa que utiliza un reloj para coordinar con la ficha del “hardware”, manteniendo una base de datos con las contraseñas y la respuesta correcta al desafío. Si el número es lo que espera el servidor, se acepta la contraseña. En un sistema de desafío – respuesta, un desafío es dado por el sistema huésped, que entonces es utilizado por el usuario para computar la respuesta apropiada. La respuesta se puede computar con la ficha, un programa automático, o el software del usuario.

Técnicas de OTP alternativas están disponibles, incluyendo los enfoques que usan tarjetas inteligentes o tarjetas inteligentes basadas en fichas USB tales como un dispositivo físico OTP.

Mecanismo de un solo ingreso al sistema o “Single Sign-on”. Este es un mecanismo de autenticación que requiere a usuarios de la computadora firmar su acceso a un sistema (es decir, presentar una contraseña) una sola vez. El “single sign-on” entonces les provee a ellos el acceso a todas las aplicaciones y sistemas a los que están autorizados a acceder. Las soluciones “single sign-on” se están poniendo en ejecución comúnmente para reducir el error humano y la frustración del usuario. La aceptación de las soluciones “single sign-on” no ha sido universalizada, puesto que estas reducen a menudo solamente el número de las contraseñas requeridas o son demasiado complejas para integrarlas a las aplicaciones. Debido a que las soluciones de “single sign-on” dependen de las contraseñas, estas soluciones también sufren de las debilidades inherentes a todas las tecnologías de autenticación, a menos que otras soluciones de autenticación sean implementadas.

Factores Biométricos

Enfoques basados en factores biométricos abarca a grupo de tecnologías probadas y de métodos automatizados que identifican y verifican a

individuos basándose en sus características personales. Estos enfoques emparejan una característica en tiempo real contra un expediente de la característica que fue creada al registrarse en el sistema. Las tecnologías biométricas principales incluyen la huella digital, la cara, la geometría de la mano, el diafragma, la palma, la firma, la voz, y la piel.

El proceso de pareo se realiza en tres pasos:

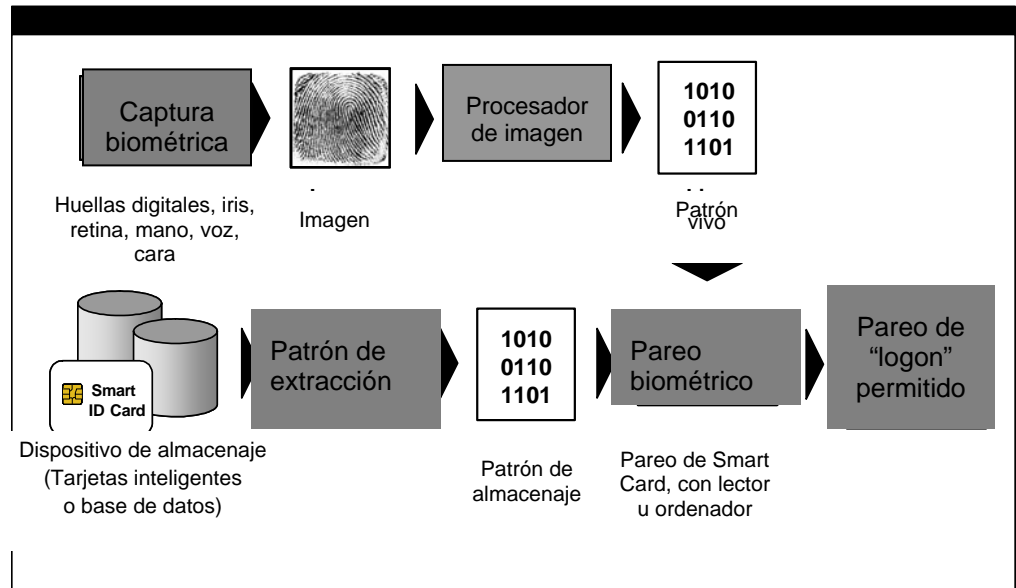
1. Una imagen de los datos biométricos (por ejemplo, una huella digital) se captura.
2. La imagen se convierte en una plantilla única.
3. Los algoritmos complejos comparan la plantilla con un expediente almacenado.

Las tecnologías biométricas se están utilizando con mayor frecuencia como control primario o secundario para el acceso lógico. En un escenario típico, los usuarios incorporan un nombre de usuario y colocan un dedo en un lector (en lugar de o en adición a proporcionar una contraseña). Un servidor compara la plantilla biométrica creada por el lector con un expediente almacenado en el servidor.

Como alternativa, los usuarios pueden insertar una tarjeta inteligente en un lector de tarjetas y utilizar una huella digital para autenticar que son los titulares válidos de la tarjeta. El biométrico capturado por el lector se compara con los datos biométricos de la tarjeta inteligente.

Si la información biométrica capturada iguala la información biométrica almacenada en la tarjeta, la tarjeta inteligente entonces libera la información secreta requerida para registrar al usuario en la red. En este caso, la comparación biométrica se puede hacer en el lector o en la tarjeta (llamada pareo dentro de la tarjeta)

Figura 1: Identificación de procesos biométricos de verificación



El valor de usar biometría para acceso lógico se incrementará en la medida en que la tecnología se vuelva más fácil y rápida de usar. Las características personales son un atractivo, conveniente y confiable mecanismo de autenticación. Las preocupaciones en materia de seguridad, sin embargo, se centran en el proceso de combinación de información biométrica, la cual por lo regular requiere ya sea que se envíe información no protegida en la red o almacenar la información en el servidor anfitrión. Este tipo de información es vulnerable para ser duplicada (resultando en accesos ilegales) o reemplazos (resultando en negación de acceso). Estas preocupaciones pueden ser mitigadas al proteger la información biométrica en tránsito o capturando y comparando los datos biométricos localmente (por ejemplo, con un lector o una tarjeta inteligente).

Llave Pública Criptográfica

La clave pública criptográfica (también conocida como clave criptográfica asimétrica) cifra la información usando matemáticamente pares relacionados de claves criptográficas. Una clave en el par se utiliza para cifrar la información; la información entonces solamente podrá ser descifrada usando la otra clave. Los usuarios obtienen los pares dominantes de una autoridad confiable y los utilizan para intercambiar datos seguros y privacidad.

Cada par de claves abarca una clave pública y una clave privada. La clave pública se utiliza para cifrar la información confidencial. La clave privada autentica al poseedor de esta y descifra la información que ha sido cifrado usando la clave pública. La clave privada se debe mantener secreta. La persona que usa la clave privada puede por lo tanto estar segura que la información que la clave puede descifrar fue destinada para ellos, y la persona que envía la información puede estar segura que solamente el poseedor de la clave privada puede descifrarla.

La información que describe la clave pública se registra en un certificado firmado digitalmente por una autoridad certificada. Un usuario puede proporcionar la clave pública a un remitente, o la clave se puede recuperar de un directorio en el cual se publique.

El uso de claves asimétricas es apoyado por PKI. PKI es una combinación de estándares, de protocolos, y de software integrados por lo menos de los componentes siguientes:

- Una Autoridad Certificada o “Certificate Authority” (CA), que publica y verifica certificados digitales
- Una autoridad del registro (RA), que verifica la identidad del solicitante antes que sea generado y asignado un certificado digital
- Uno o más directorios, donde los certificados (con sus claves públicas) y las listas de revocación de certificados (CRL) son almacenadas.

La clave pública criptográfica ofrece un nivel adicional de seguridad, puesto que no hay secretos compartidos. Generalmente, el certificado de PKI se almacena en una computadora de registro o un dispositivo de almacenamiento (por ejemplo, una tarjeta inteligente) y se utiliza para cifrar la contraseña antes de que se envíe para ser autenticado.

Fichas Flexibles

Las fichas flexibles o “soft tokens” (también conocidos como tarjetas virtuales) son archivos de programas que contienen las claves criptográficas usadas para la autenticación. Los usuarios se autentican en la red al probar su posesión y control de esta clave criptográfica (usualmente almacenada en disco o algún otro dispositivo). El medio utilizado para almacenar las claves criptográficas es a su vez cifrado por una contraseña de conocimiento único del usuario. En cada momento de activación se requiere el registro de una contraseña que descifre el contenido del “soft token”. La copia no cifrada de la clave de autenticación se borra después de cada autenticación.

Las fichas flexibles (soft tokens) se perciben como artículos de bajo costo, de fácil manejo, y desechables. Sin embargo, este método de autenticación no es comúnmente portátil; los usuarios deben estar ubicados en la computadora de un cliente para que puedan autenticarse.

Algunas fichas flexibles (soft-tokens) ofrecen movilidad al usuario, permitiendo que las claves sean almacenadas en los servidores y descargadas al sistema del usuario según se necesite, o empleando los componentes claves generados a partir de contraseñas combinadas con los componentes claves almacenados en los servidores.

Las fichas flexibles (Soft tokens) se respaldan en un cliente confiado y en un servidor de confianza. Además, el usuario debe tener otra clave para tener acceso a la ficha flexible (soft token); si no, cualquier persona con el acceso a la máquina del cliente puede ser autenticada.

Tecnología de Tarjetas Inteligentes

Cuando es utilizada para el acceso lógico, la tecnología de la tarjeta inteligente viene generalmente en dos formas una tarjeta de crédito o un dispositivo USB, cada uno con un procesador incorporado. En gran medida la forma más popular es la tarjeta de crédito, debido a su capacidad de incluir una foto e información corporativa visible y de recibir otros mecanismos de la seguridad tales como una clave magnética o código de barra.

Sin importar su apariencia, las tarjetas inteligentes se pueden utilizar para implementar cualquier forma de autenticación descrita arriba. Las tarjetas inteligentes tienen la capacidad de:

-
- Almacenar de forma segura las contraseñas
 - Generar pares de claves asimétricos y almacenar de forma segura certificados PKI
 - Almacenar de forma segura las claves simétricas
 - Almacenar de forma segura los archivos raíz de los OTP fichas
 - Almacenar de forma segura las plantillas biométricas de imagen

Usar una tarjeta inteligente para almacenar contraseñas es el uso más simple que tienen las tarjetas inteligentes para obtener acceso lógico. Las ventajas de este tipo de sistema son:

- Los usuarios no tienen que recordar sus contraseñas.
- Las contraseñas almacenadas pueden ser muy grandes y casi impenetrables utilizando un ataque del diccionario.
- La tarjeta se puede activar por un número de identificación personal (PIN) o biométrico si se requiere, agregando un valor de autenticación.
- Esta implementación es usualmente la que más económica le resulta al sistema.

Las tarjetas inteligentes se pueden también utilizar para respaldar esquemas más poderosos de autenticación. Por ejemplo, en un sistema que utilice claves simétricas, la tarjeta puede almacenar con información secreta compartida implantada al momento de la fabricación.

Esta clave se puede entonces utilizar durante el proceso de la autenticación con un servidor seguro como parte de una sesión algorítmica de cambios y de respuesta. Las tarjetas inteligentes también se reconocen ampliamente como el portador ideal de las credenciales de PKI; las tarjetas inteligentes pueden almacenar certificados de claves públicos con seguridad, respaldar la generación de claves dentro de la tarjeta o "support on-card key generation" y proteger la clave privada del usuario.

El uso de una tarjeta inteligente con uno o más de estos enfoques puede proporcionar medios más seguros de acceso lógico, aunque la combinación necesariamente no llene los criterios de dos o tres formas de autenticación.

Por ejemplo, una tarjeta inteligente por si misma no puede autenticar a un usuario en una red, pero la tarjeta inteligente puede almacenar información que proporcione un mecanismo de acceso. Una tarjeta inteligente que almacena el certificado de la conexión de PKI de un usuario puede autenticar al usuario en la red llenando los requisitos que posea el usuario. Sin embargo, combinar una tarjeta inteligente con un PIN o una protección biométrica logra la autenticación de dos formas. Una tarjeta inteligente con ambas, un PIN y datos biométricos proporciona la autenticación de tres formas.

La Tabla No. 1 resume el uso de la tarjeta inteligente con las formas de autenticación.

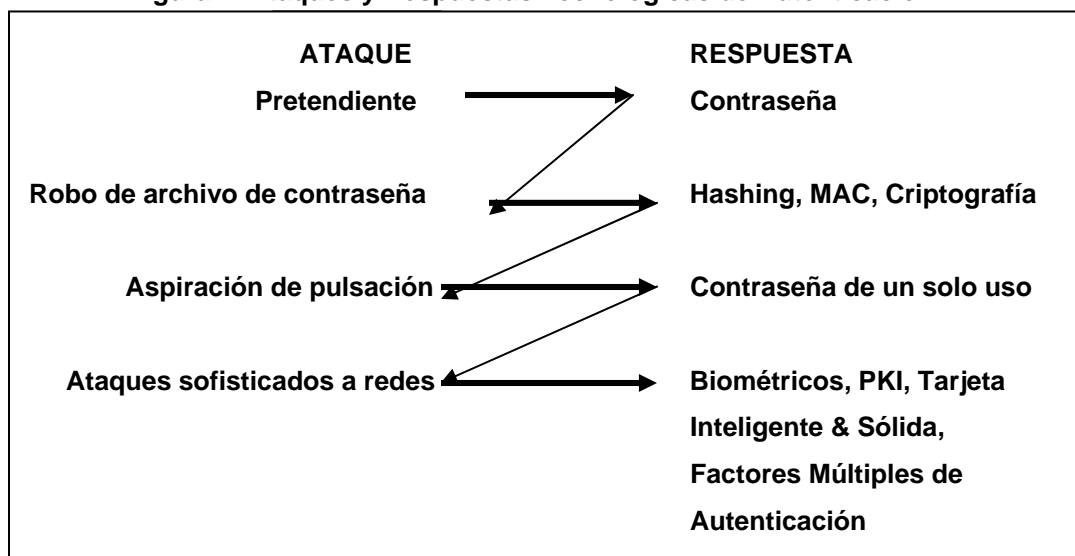
Tabla 1: Enfoques de Autenticación Individuales y Múltiples

Enfoque de Autenticación	Factor		
	Algo que tu poseas	Algo que tu sepas	Algo que tu seas
Contraseñas		✓	
OTP archivo base de Fichas	✓		
Plantilla de una imagen Biométrica en una base de datos			✓
Tarjetas inteligentes	✓		
Tarjetas inteligentes con PIN	✓	✓	
Tarjetas inteligentes con certificado de registro PKI de tarjetas inteligentes	✓		
Patrón de imagen biométrica almacenada en una tarjeta inteligente	✓		✓
Tarjetas inteligentes con PIN y contraseña (o certificado) almacenado en la tarjeta	✓	✓	
Tarjetas inteligentes con PIN y contraseña (o certificado) y biométrica en la tarjeta	✓	✓	✓

Resumen

Según se muestra en el cuadro 2, las tecnologías de autenticación han evolucionado en forma compleja como respuesta a los nuevos ataques en los sistemas y redes se han desarrollado en complejidad en respuesta a nuevos ataques contra sistemas y redes. El propósito de la tecnología de autenticación es simplemente el de no permitirles el acceso no autorizado a los individuos a la información y a los programas, sin importar su propósito. Pues la información llega a ser cada vez más vital, es crítico que los individuos autorizados tengan los privilegios que permitan acceso a la información y a los programas que son apropiados y esenciales para sus funciones y roles. Los ataques en contra de los sistemas han creado la necesidad de tener respuestas tecnológicas que se pueden utilizar para frustrar las intrusiones.

Figura 2: Ataques y Respuestas Tecnológicas de Autenticación



Factores Claves a Considerar para la Implementación de una Autenticación más Sólida en el Acceso Lógico

Los negocios y las organizaciones están descubriendo que el enfoque actual a la autenticación del acceso lógico es obsoleto e inadecuado. Un número de factores importantes están llevando a las compañías y a las agencias estatales a reevaluar sus estrategias y planes lógicos del acceso, dando por resultado una tendencia hacia el uso de una autenticación más poderosa basada en el acceso lógico. Esta sección revisa algunos de las consideraciones y de los requisitos dominantes del negocio que conducen esta tendencia y discute cómo métodos más poderosos pueden ayudar en la búsqueda de estos requisitos.

Ambiente Corporativo

Los cambios en el ambiente de negocios pueden ser poderosos agentes para la reingeniería de los procesos tecnológicos y la implementación de una autenticación más poderosa en el acceso lógico y físico.

- **¿Está su negocio intentando adecuarse a las nuevas regulaciones, tales como “HIPAA”, “Sarbanes-Oxley”, “Gramm-Leach-Bliley”, “Visa Waiver Program”, o “Internacional Civil Aviation Organization” (ICAO) “Machine-Readable Travel Documents” (MRTD)?** Muchas de estas regulaciones afectan a aquellos quienes toman las decisiones al igual que al departamento de Sistemas de Información. Métodos más poderosos de la autenticación pueden ayudar a lidiar con los requisitos de acceso y auditoria que son integrales para estas regulaciones. Por ejemplo, hacer cumplir una autenticación más sólida mediante el uso de las tarjetas inteligentes y huellas digitales biométricas pueden ayudar a dar respuesta a muchos de los requerimientos de privacidad para cumplir con las regulaciones de HIPAA.

-
- **¿Su organización o un socio de negocio ha sufrido recientemente una abertura en su seguridad, o ha realizado una auditoria que no ha reflejado la vulnerabilidad de su seguridad?** A pesar de que tales acontecimientos pueden ser desagradables hay que lidiar con ellos, estos pueden proveer una motivación extra y financiamiento que permita implementar poderosas medidas de seguridad de acceso lógico donde sea necesario
 - **¿Esta su organización contemplando, planeando, o implementando un sistema de acceso físico nuevo o mejorado? ¿Ha considerando usted la integración de sus sistemas de acceso físico y lógico?** Considere actualizar sus procedimientos lógicos de acceso al mismo tiempo. El tener una vista integral de los requisitos de acceso puede ofrecerle un sistema de seguridad poderoso, más integrado y amigable. Los enfoques de integración del acceso lógico y físico pueden proveer de igual forma ahorros significativos, eliminando o reduciendo el número de placas o tarjetas de identificación requeridas por el sistema, evitando el reemplazo de los lectores o los costos de actualizarlos y agilizando los procedimientos de provisión de identidades.
 - **¿Estuvo su organización implicada recientemente en una adquisición o una fusión? ¿Se encuentra usted integrando o migrando múltiples Sistemas de Información?** Muchas compañías se enfrentan al desafío de lidiar con sistemas de acceso lógicos complicados al integrarse diferentes ambientes de Sistemas de Información. Muchos grupos rechazan estas nuevas iniciativas hasta que se hayan integrado los diferentes sistemas de información. Pero este enfoque puede ser riesgoso y costoso en lo referente al acceso lógico. En su lugar, considere la implementación de poderosas medidas de autenticación como una ayuda en la migración dentro del proceso de la integración.

Por ejemplo, una poderosa autenticación puesta en ejecución con una sola credencial de tarjetas inteligentes podría sustituir el uso de múltiples tarjetas de identificación y contraseñas de usuarios añadiendo seguridad a los sistemas de Información.

Transformación en negocios y procesos de reingeniería

Muchas organizaciones consideran una poderosa autenticación como un componente clave en proyectos de reingeniería de procesos de los Sistemas de Información en la compañía.

- **¿Su organización ha estado considerando integrar la administración integral de la identidad? ¿Esta usted pensando en compartir sus credenciales de identidad con sus socios, proveedores o las agencias estatales?** Si es así tales planes pueden ayudarle a determinar qué tipos de prácticas de autenticación se deben implementar con miras a la conservación de sus socios corporativos mostrándoles como estas prácticas fortalecerán la administración de la identidad de manera global. Una poderosa autenticación también será un componente integral de cualquier sistema de gerencia federado en el que usted decida participar. Requerir el uso apropiado de una poderosa autenticación en un sistema de gerencia federado lo protege no sólo contra las debilidades potenciales dentro

de su propia organización pero también contra debilidades potenciales en otras partes de la federación.

- **¿Tiene usted una estrategia Web de servicios o de despliegue de servicios en curso? ¿Responde esta estrategia a sus empleados, clientes, o a ambos?** La migración a una infraestructura Web-céntrica para ambas internas y externas aplicaciones representa una oportunidad excelente de centralizar, de integrar, y de consolidar políticas y prácticas lógicas de acceso.
- **¿Está su organización esperando sustituir las identificaciones y contraseñas de múltiples usuarios con una sola credencial?** Aspectos relacionados con el uso, el manejo de contraseñas y las preocupaciones relacionadas con la seguridad (concernientes a la reutilización de contraseñas o el uso de contraseñas fáciles de recordar) han estimulado iniciativas de un registro único o de un número reducido de registros en los sistemas de muchas organizaciones. El tener una credencial de registro único para ingresar al sistema, dictamina la necesidad de utilizar métodos más sólidos de autenticación cuando se utiliza esta “súper” credencial.

Reducción de Costos y Recuperación de la Inversión

La implementación de una sólida autenticación puede ayudar a reducir los costos globales de los Sistemas de Información y a obtener un retorno de la inversión obligado. Entre las dudas claves a considerar tenemos:

¿Cuál es el costo total de manejar identificaciones de usuario y sus contraseñas a lo largo de su organización, incluyendo costes intangibles tales como la satisfacción del cliente y la productividad del empleado? Además de los riesgos de la seguridad inherentes en el uso de identificaciones de usuario y sus contraseñas, otros costes incluyen la administración del sistema, la ayuda del puesto de información, y la productividad perdida. Los métodos poderosos de autenticación pueden ahorrar el dinero mientras que realzan seguridad. Entender el coste total de los actuales procedimientos lógicos de acceso puede ayudar a cuantificar las ventajas de realizar una migración a métodos de autenticación más poderosos.

¿Cuántas aplicaciones, sistemas, y redes puede utilizar o maneja su organización? ¿Cuántos usuarios accesan estas aplicaciones, sistemas, y redes? Cuantos más sistemas posea usted y cuanto más grande sea la población de usuarios, mayores pueden ser los ahorros alcanzados al migrar a un método de autenticación más poderoso. Mientras que los mayores ahorros de coste proviene de una seguridad mejorada, los ahorros de coste administrativo pueden contribuir de manera significativa al éxito del negocio.

¿Cómo esta compuesta su población de usuarios? ¿Pueden sus socios de negocios accesar sus sistemas? ¿Los usuarios tienen acceso a sus sistemas desde redes externas? Mientras más variada sea su población de usuarios,

mayor es el retorno en la inversión como resultado de la migración a métodos más poderosos de autenticación. Tal migración ofrece la flexibilidad de elegir y de hacer cumplir los procedimientos más eficaces de autenticación para cada variedad de usuarios. Por ejemplo, la autenticación de dos-formas (tal como una tarjeta inteligente y una biométrica) se puede requerir para lograr el acceso remoto a una Intranet, mientras que solamente mediante una sola forma de acceso (tal como una tarjeta inteligente o una biométrica) se puede requerir para el acceso de red localizado en un “campus” universitario.

Seguridad y Privacidad

El mejorar la seguridad del acceso a los Sistemas de Información y proteger la privacidad de los individuos son las principales prioridades de las organizaciones que implementan nuevos sistemas de acceso lógico que utilizan poderosas técnicas de autenticación. Entre los factores claves a considerar tenemos las siguientes interrogantes:

- **¿Su organización tiene una política de privacidad que proteja la información del usuario contra el acceso desautorizado?** Por ejemplo, los administradores de sistema no deben poder hojear la información personal de los usuarios según sea su voluntad. Los procedimientos poderosos de autenticación pueden permitir los administradores realizar plenamente sus tareas mientras que prevé que estos acceden información confidencial de los usuarios.
- **¿Sus métodos existentes de la autenticación proporcionan bastante seguridad y privacidad? ¿Depende su seguridad lógica de acceso local de contraseñas solamente?** El control de acceso puede ser fortalecido usando múltiples formas de autenticación (algo que usted tiene, algo que usted sabe, y algo usted es). Niveles más altos de seguridad y privacidad se alcanzan cuando los métodos de autenticación utilizan formas de varias categorías en combinación con múltiples formas de una o más categorías (por ejemplo, biométrica múltiple). Un sistema sólido de autenticación correctamente implementado puede hacer cumplir una variedad de políticas y de procedimientos de la autenticación, basándose en las necesidades particulares de las aplicaciones utilizadas y en las necesidades de la población de usuarios.
- **¿Su organización utiliza distintivos o tarjetas de identificación? ¿Cómo se producen y se distribuyen estas tarjetas?** Los poderosos procedimientos de autenticación pueden nivelar y mejorar una infraestructura existente de una tarjeta de identificación emitida y se pueden implementar usando la producción central o distribución de la tarjeta. La producción y la distribución central proporcionan seguridad extra y reduce los costos de equipo y mantenimiento. Distribuir el punto-de-inscripción proporciona un rápido retorno en la inversión, aumenta la satisfacción del cliente, y representa una oportunidad adicional de entrenar a usuarios.
- **¿Esta la tecnología biométrica lista para ser utilizada? ¿Qué tipo de tecnología biométrica es la correcta para su aplicación o sistema?** Los abastecedores de tecnología biométrica continúan haciendo avances en exactitud, funcionamiento, y costos. Los sistemas biométricos de hoy ofrecen capacidades compatibles utilizables y aceptables, mientras que proporcionan el funcionamiento y confiabilidad para los usuarios del

sistema. Es importante seleccionar la tecnología biométrica que es apropiada guardar para un futuro como un requisito del uso y de la autenticación. Si la huella digital, el diafragma, la voz, la cara, un cierto otro factor biométrico, o la biométrica múltiple están utilizados, la tecnología biométrica puede ayudar a hacer cumplir niveles más altos de la seguridad y de la privacidad en un sistema lógico del acceso, mientras que también proporciona beneficios útiles.

Gerencia, Utilización y Capacitación

Las soluciones sólidas de la autenticación pueden simplificarla gerencia y mejorar la utilidad de los procesos de la autenticación. Considere las preguntas siguientes al poner nuevas soluciones de control de acceso en ejecución.

- **¿Cómo su organización detecta y desactiva las credenciales perdidas o robadas? ¿Cómo usted sabe cuándo se ha comprometido una contraseña?** Éstos son problemas serios para los usos lógicos del acceso, especialmente si los usos son protegidos solamente por contraseñas estáticas. La autenticación sólida reduce al mínimo estos riesgos. Por ejemplo, requerir el uso de una tarjeta inteligente y de una contraseña reduce al mínimo el riesgo que una contraseña será compartida o comprometida. Usar datos biométricos con una tarjeta inteligente con eficacia hace la tarjeta inútil si se pierde o si es robada.
- **¿Cómo su organización entrena a usuarios en seguridad?** El entrenamiento de la seguridad es un elemento dominante al plan total de la seguridad de cualquier organización. La autenticación fuerte proporciona un recordatorio constante a los usuarios que la seguridad es importante. También ofrece una oportunidad adicional de entrenar a usuarios en seguridad. Por ejemplo, durante la emisión de la tarjeta de la identificación, los usuarios pueden ser mandados en el uso apropiado de sus credenciales fuertes de la autenticación. Esta instrucción puede incluir una demostración de cómo presentar una huella digital de la alta calidad y describir cómo se protegen y se almacenan los datos biométricos y quién tiene acceso a él. Las credenciales fuertes de la autenticación son también un recordatorio a los empleados que las actividades de la red están supervisadas y que la seguridad de la red y de la computadora es extremadamente importante.
- **¿Su organización tiene áreas de trabajo comunes o múltiples claves operacionales que requieren sitios de trabajo para ser utilizados por múltiples usuarios?** Un problema común de la seguridad en estos tipos de ambientes es la carencia de los controles de acceso del usuario o de compartir de las credenciales del usuario. Los usuarios encuentran comúnmente maneras de evitar los controles de acceso incómodos que retrasaron el flujo de trabajo. La autenticación sólida puede ayudar a proporcionar una seguridad mejor para el Departamento de Informática (IT) y realzar la utilidad para los usuarios, tratando las necesidades de ambos grupos. Por ejemplo, usar una huella digital para firmar una transacción provee de administradores de responsabilidad y de un rastro de intervención a un usuario individual, mientras que también siendo más rápido y más fácil para el usuario que entrando y apagando un nombre de usuario y una contraseña.
- **¿Cuántas identidades los usuarios necesitan manejar hoy? ¿Cuántas identificaciones de usuario y contraseñas deben**

recordar? En apenas alrededor de cada trabajo y cada industria, los usuarios deben obrar recíprocamente con un número de usos. Esto es compuesta a menudo por la tendencia a la entrega electrónica de las ventajas, de las comunicaciones, y del entrenamiento del empleado. Los usuarios no sólo necesitan manejar identidades para aplicaciones relativas al flujo de trabajo y de procesos, pero deben también recordar a menudo varias identificaciones de usuario y contraseñas correspondientes para recursos humanos, atención médica, y usos financieros también. Una autenticación fuerte puede ayudar a simplificar en manejo de identidad, tanto para los usuarios como para los administradores, a la vez que proporciona niveles más altos de la seguridad.

Beneficios de la Tecnología de Tarjetas Inteligentes para un Acceso Lógico

Para la mayoría de las organizaciones hoy en día, los recursos de las computadoras y de la red son accedidos usando una identificación de usuario o “user-id” y una contraseña. Cada sistema o aplicación asigna comúnmente una identificación de usuario y una contraseña a cada usuario y después determina los controles de acceso para ese usuario basado identificación única. Sin embargo, como el número de sistemas y aplicaciones en una organización crece, administrar y utilizar esas identidades crea ineficacias operacionales significativas .El incremento en el número de aplicaciones también introduce vulnerabilidades en la seguridad, mientras que llega a ser más difícil controlar políticas alrededor del uso de esas identidades.

Sólida Autenticación

Más y más organizaciones buscan soluciones de sólida autenticación más allá de identificación de usuarios y contraseñas para validar que los sistemas de acceso de los usuarios son quienes ellos dicen ser. Las organizaciones que han manejado autenticaciones sólidas (comúnmente en forma de fichas de contraseñas dinámicas) tradicionalmente ofrecen esa solución sólo a los empleados a distancia. Esta práctica está basada en el supuesto de que los individuos que se pueden localizar dentro de un edificio son confiables. Sin embargo, la encuesta de vigilancia de crímenes electrónicos o “E-Crime Watch Survey” del 2004 (desarrollada por “CSO Magazine” en cooperación con el Servicio Secreto de Estados Unidos y el “CERT Coordination Center”) reveló que 36% de los 350 encuestados experimentaron “acceso no autorizado por alguien de adentro” como uno de los crímenes electrónicos cometidos contra su organización en 2003.⁴ Este tipo de crimen fue el cuarto ataque más común, detrás de virus, negación de servicios y basura electrónica o “spam”. IDC estima que más del 60% de todas las amenazas son internas, provienen de los empleados, contratistas, consultores, integradores de sistemas, socios, distribuidores y otros con acceso privilegiado.⁵

⁴ “2004 E-Crime Watch™ Survey” Shows Significant Increase in Electronic Crimes,” CSO Magazine survey conducted in cooperation with the United States Secret Service and Carnegie Mellon University Software Engineering Institute’s CERT® Coordination Center, May 25, 2004 (www.csoonline.com/releases/052004129_release.html)

⁵ “Endpoint Security Management: Maximizing Best of Breed,” IDC report, March 4, 2004

Las fronteras de los sistemas de información y data continúan expandiéndose. La tecnología del Internet y las tecnologías inalámbricas proveen creciente número de puntos de acceso convenientes para empleados, pero crean una pesadilla para IT. Para incrementar el apoyo dado a la seguridad en una organización como un todo, se necesita un método para proveer fuerte y consistente autenticación para acceso a todos los recursos de la red. La tecnología de Tarjetas inteligentes es la mejor plataforma para asegurar todos los puntos de acceso en una organización.

Las tarjetas inteligentes aumentan significativamente la seguridad de las credenciales digitales de un usuario al margen de la naturaleza de las credenciales. Las credenciales son almacenadas permanentemente en una tarjeta, la cual está en posesión del usuario final, y nunca disponible en software o en la red para que un usuario no autorizado la robe. Las tarjetas inteligentes son por lo general usadas para permitir dos factores de autenticación, incorporando alguna cosa que tú tienes (tarjetas inteligentes) y algo que tú conoces (comúnmente un PIN que activa las funciones criptográficas de la tarjeta). Tomar el control de la identidad digital de un usuario requiere robar la tarjeta inteligente y adivinar el PIN. Los usuarios se percatan rápidamente de cuando una tarjeta es robada y pueden contactar al administrador de la red para que revoque las credenciales robadas. Adicionalmente, demasiados intentos fallidos de adivinar la contraseña de la tarjeta puede hacer que está se bloquee.

La tecnología de tarjetas inteligentes también respalda la adición de tecnologías biométricas (alguna cosa que tú eres) para habilitar la autenticación con tres factores/elementos. Como una alternativa, la biometría puede simplemente reemplazar el PIN, lo cual mientras refuerza la seguridad incrementa la conveniencia del usuario. Añadir la autenticación biométrica al control de acceso es fácil, puesto que la tarjeta inteligente puede almacenar la información biométrica del usuario y llevar a cabo el proceso requerido para determinar una combinación. No se requiere una base de datos auxiliar o "back-end" de datos biométricos. Contar con las credenciales para acceder una aplicación almacenada de forma segura en la tarjeta inteligente y protegida por los datos biométricos del usuario provee a la organización con una seguridad biométrica sin tener que tocar aplicaciones de procesamiento auxiliar o "back-end applications".

Seguridad Integrada al Sistema

La tarjeta inteligente es típicamente un dispositivo del tamaño de una tarjeta plástica de crédito con un chip de computador incrustado. El chip puede contener tanto un microcontrolador como una memoria interna o sólo la memoria. Los chips inteligentes también pueden estar incrustados en otro dispositivo, incluyendo las fichas que se conectan directamente a un puerto de computador USB, a un chip SIM chips que se conectan a los celulares GSM.

Microcontroladores-basados en chips son la más práctica elección para aplicaciones de acceso lógico seguras, debido a que esos chips pueden almacenar grandes cantidades de información y tienen la habilidad para procesar información y realizar una variedad de funciones. Esta habilidad única respalda la adición de métodos activos de seguridad a la tarjeta inteligente, dependiendo de los requerimientos de la aplicación. La mayor parte de las soluciones de tarjetas inteligentes actualmente disponibles para

acceso lógico están ya listas y cargadas encriptación y algoritmos con las más amplia utilización, tales como DES, 3DES, y RSA6.

Además, la mayoría de los microcontroladores-basados en chips inteligentes son diseñados para resistir ataques. Los fabricantes de chip inteligente construyen una variedad de contramedidas que detectan y reaccionan a un número de posibles ataques, incluyendo voltaje, frecuencia, manipulaciones de la luz o temperatura, y ataques de energía estática o diferencial. La reacción típica a la mayoría de los ataques es de bloquear el chip, haciendo éste inoperable.

Los ataques sofisticados a las tarjetas inteligentes consumen mucho tiempo y son muy costosos, y el atacante debe tener en sus manos la tarjeta. Si la tarjeta inteligente de un usuario se extravía, éste debe reportarla y ésta es inhabilitada antes de que cualquier ataque pueda tener lugar. Cuando las credenciales son almacenadas en software o en la computadora de un usuario, sin embargo, el usuario nunca podría saber que éstas han sido robadas.

Incremento de la Seguridad y Conveniencia para los Usuarios

Los usuarios en la mayoría de las organizaciones enfrentan el reto de manejar múltiples contraseñas para múltiples sistemas y aplicaciones. Este requerimiento tiene implicaciones para la seguridad y la productividad del usuario. Algunos departamentos de Informática eligen el camino de menor resistencia, permitiendo a los usuarios usar la misma contraseña para cada aplicación. Esta práctica representa el mayor riesgo de seguridad, puesto que todas las aplicaciones son comprometidas si una sola contraseña es adivinada o robada. Otros departamentos de Informática pudieran establecer una política más fuerte, requiriendo una contraseña diferente para cada aplicación y una contraseña más compleja, que contenga una mezcla de tipos de caracteres (alfanumérica, mayúscula, minúscula, símbolos). Adicionalmente, una política segura de contraseñas pudiera requerir que las palabras claves fuesen cambiadas cada cierto tiempo. Establecer políticas más fuertes respecto de las contraseñas es un paso importante cuando el acceso depende de una sola palabra clave fija, pero reforzar estas políticas puede ser un reto. La mayoría de los usuarios tiene dificultad para recordar palabras claves de ingreso complejas, por ende, ellos las escriben o almacenan en un texto de sus computadoras, donde pueden ser fácilmente robadas.

Los Departamentos de Informática también enfrentan los cambios en la administración de contraseñas para múltiples usuarios y aplicaciones múltiples sin sacrificar productividad y sin crear usuarios infelices. Las estadísticas industriales muestran que del 30% al 50% de los recursos de soporte técnico de los departamentos de informática son absorbidos por el manejo y reseteo de las contraseñas. La productividad del usuario final también se ve afectada, desde el momento en que el usuario no puede acceder a las aplicaciones hasta que la nueva contraseña es asignada.

Varias "administraciones de identidad" están disponibles para manejar esos asuntos de productividad. Consolidar las identidades de los usuarios en directorios centrales e implementar herramientas provisionales para administrar esas identidades minimiza las pérdidas de productividad

⁶El RSA algoritmo de encriptación viene a ser el estándar internacional para transmisiones seguras.

atribuibles al hecho de tener que manejar diferentes identidades para diferentes cuentas. Este tipo de soluciones también enfoca las vulnerabilidades de seguridad poseídas por las cuentas que permanecen en un sistema luego de que el acceso del propietario ya no es válido. Soluciones similares están disponibles para contenidos y aplicaciones basados en el "Web". Sin embargo, este tipo de soluciones no puede ser implementado de la noche a la mañana. Adicionalmente, ellas requieren un cambio gradual en la infraestructura informática de la organización. Y los usuarios seguirán necesitando manejarse con múltiples contraseñas para sus aplicaciones. Otras soluciones para manejo de identidad simplifican la experiencia del usuario final al usar la sincronización de contraseñas, administración de contraseña por auto-servicio, o registro único para ingresar al sistema, pero éstas, por lo regular, también requieren modificación a la infraestructura de informática (IT) y no responden a las preocupaciones de seguridad derivadas del uso de contraseñas.

Las organizaciones que usan la tecnología de tarjetas inteligentes para acceso lógico no tienen que esperar por la implementación de un sistema informatizado de administración de identidad para darse cuenta de las eficiencias operacionales y el retorno de su inversión. Las identidades y credenciales del usuario pueden ser consolidadas en una tarjeta inteligente inmediatamente, proveyendo al usuario con un simple y consistente acercamiento al acceso lógico, independientemente de que el usuario esté en una estación de trabajo o en red o accediendo a una red remoto mediante un VPN. La experiencia que queda consistente del usuario cuando la organización actualiza sus infraestructuras de identidad gerencial: insertando una tarjeta inteligente y dando entrada a un PIN.

Una tarjeta inteligente es la clave personal del usuario para toda su información y las aplicaciones. Adicionalmente, debido a que la clave es portátil los usuarios no están atados a una sola estación de trabajo en la cual sus credenciales están ubicadas. Pueden ir de máquina en máquina, una ventaja crítica para usuarios que trabajan en múltiples sitios.

Protección Mejorada contra Fraudes de Identidad

Las tarjetas inteligentes pueden ayudar a defenderse contra los atentados, cada vez más ingeniosos, de "phishing". Phishing usa un mensaje de la Internet para intentar engañar a los individuos para que divulguen la información de sus cuentas. Por ejemplo, un intento de phishing podría usar un e-mail enviado a una víctima potencial, que pareciera ser una genuina petición de alguien confiable (por ejemplo, un banco o un proveedor de servicios de Internet). El individuo podría entonces responder a la petición proveyendo números de cuenta, PINs o contraseñas a un sitio "Web" subrepticio o engañoso, que se hace pasar como una entidad legítima. Los ataques de phishing explotan la falta de autenticación entre el que envía el e-mail y el destinatario, y entre sitio "Web" subrepticio y el individuo.

Las tarjetas inteligentes pueden ser usadas para combatir los ataques de phishing al aplicar mutua autenticación de doble vía para asegurar el acceso a los servicios del sitio Web. Cuando las cuentas de los emisores ofrecen un servicio de Web (por ejemplo, para administración de cuenta), ellos pueden emitir tarjetas inteligentes a los cuenta habientes que les permita acceder al legítimo sitio Web. La credencial de la tarjeta inteligente puede autenticar al usuario para el sitio Web y autenticar el sitio Web como legítimo.

Al proveer sólida y multifactorial autenticación, al permitir la autenticación mutua, las tarjetas inteligentes pueden ayudar a vencer a los ataques “phishing”. Se les puede asegurar a los individuos que ellos se están comunicando con un sitio legítimo y que sus credenciales de identidad están siendo protegidas de acceso no autorizado.

Cobertura de Aplicaciones Basados en Estándares

La tecnología de tarjetas inteligentes se está convirtiendo en el medio de acercamiento preferido para acceso lógico, no sólo por la incrementada seguridad de las tarjetas inteligentes, sino también por su fácil uso, amplia cobertura de aplicación, facilidad de integración y funcionalidad de propósito múltiple.

Las tarjetas inteligentes proveen a las organizaciones con una solución costo-efectiva que puede ser distribuida fácilmente y la cual es ampliamente aceptada por el usuario final.

Diferentes aplicaciones imponen diferentes requerimientos de los usuarios antes de permitirles el acceso. Algunas aplicaciones respaldan sólo un método para garantizar el acceso: otras, respaldan múltiples métodos. Pocas aplicaciones permiten que las credenciales sean compartidas.

Algunos de los más comunes métodos de acceso a las aplicaciones son una combinación del nombre del usuario y la contraseña, sólo la contraseña, un secreto compartido, OTP, biométricos, y PKI o certificado digital. La combinación del nombre del usuario y la contraseña, con todo y que es el acercamiento menos seguro, es actualmente el método primario usado para control de acceso. Métodos más seguros, tales como OTPs o certificados PKI, pueden incrementar la seguridad sólo para aplicaciones que respalden esos métodos y requieren infraestructura adicional para administrarse.

En la medida en que los métodos multiplican los requerimientos para acceder a las aplicaciones, la aceptación de los usuarios decrece, lo cual a menudo conlleva a un decrecimiento en la seguridad.

Las tarjetas inteligentes, a diferencia de otras soluciones, pueden proveer al usuario con todos estos métodos de acceso en una sola tarjeta, y para acceder sólo requiere de un PIN del usuario. La funcionalidad adicional permite a las tarjetas inteligentes generar OTPs que reemplazan las fichas de una única utilización o “single-use tokens” y usa factores biométricos para reemplazar el PIN. Productos comerciales que refuerzan la seguridad y la portabilidad de las tarjetas inteligentes están disponibles para almacenar nombres de usuarios y contraseñas para todas las aplicaciones. En adición, las tarjetas inteligentes son más flexibles que la tradicional tecnología de ficha, debido a que son dispositivos criptográficos que pueden respaldar una amplia gama de funcionalidad. Ellas no dependen de la presencia de un servidor, y pueden ser borradas y reprogramadas para un uso continuo dentro de una organización.

Las tarjetas inteligentes pueden ahora proveer a un usuario con un solo interfase para acceder a todas las aplicaciones independientemente de la credencial requerida para la aplicación. Esta capacidad incrementa la aceptación y conveniencia mientras se implementan y refuerzan las políticas de seguridad de la organización.

En los últimos años, los estándares han evolucionado al punto de que proveen la interoperabilidad necesaria para permitir a las tarjetas inteligentes acceder a múltiples fuentes/recursos de la organización. Por ejemplo,

estándares criptográficos, tales como “PKCS #11” y “Microsoft Crypto API” (CAPI) permiten aplicaciones para usar un certificado digital almacenado en una tarjeta inteligente para autorizar el acceso al usuario final. La clave privada es almacenada en el chip de la tarjeta inteligente y sólo puede ser acesada por un usuario que provea el PIN correcto cuando la aplicación abre.

La adopción del estándar llamado: “Personal Computador/Smart Card” (PC/SC) y la proliferación de lectores y “drivers” de lectores ha contribuido también a que haya una aceptación más amplia de las tarjetas inteligentes para acceso lógico. El precio de los lectores ha disminuido y su calidad y su disponibilidad se ha incrementado, al punto de que muchos de los principales fabricantes de computadoras ahora incorporan un lector al teclado de una computadora o “laptop” por un pequeño costo adicional.

Facilidad de Integración

Las tarjetas inteligentes incluyen la incrustación de funcionalidad que simplifica su integración en la infraestructura informática (IT) de una organización. La mayoría de las aplicaciones que requieren otras credenciales aparte del nombre del usuario encajan en uno de los estándares listados arriba. Por esta razón, permitir el acceso de tarjetas inteligentes es por lo general simple, requieren de la instalación de una pequeña aplicación “middleware” en el computador. Las tarjetas inteligentes pueden entonces ser usadas para registrarse al sistema, obtener acceso VPN, sellado y encriptación del correo electrónico, acceso SSL-basado en Web, y factores biométricos basados en registrarse en el sistema o “logon”.

Muchos de los líderes de CAs han adoptado tarjetas inteligentes como la plataforma preferida para almacenamiento y uso de certificados digitales. UnCA puede usar ya sea PKCS #11 o Microsoft CAPI interfase para generar claves, certificados cargados y realizar las funciones criptográficas. Requeridas. Configurar un CA para usar tarjetas inteligentes es en modo directo, comúnmente consiste sólo en seleccionar la interfase correcta.

Los lectores de tarjetas inteligentes ahora son fácilmente integrados con aplicaciones y sistemas operativos de escritorio a través de dos estándares: el estándar PC/SC y el CCID, o el dispositivo del chip de la tarjeta interfase, especificación.

El estándar de PC/SC permite que integren a los lectores de tarjetas inteligentes fácilmente con middleware u otras aplicaciones, sin importar fabricante o sistema de comando. No obstante, este estándar fue desarrollado para uso de un ambiente Microsoft, ahora se considera de hecho el mejor el estándar para muchas otras plataformas.

La especificación de CCID fue desarrollada para los lectores de tarjetas inteligentes del USB. Fue diseñada para apoyar la integración fácil de los lectores de tarjetas inteligentes con los sistemas operativos de escritorio, de tal modo quitando la necesidad de instalar software adicional del conductor del lector sobre el tablero del escritorio del usuario. La especificación fue definida por el foro del ejecutor del USB (USB-IF)⁷ conjuntamente con la industria inteligente de la tarjeta. CCID define un sistema de comando y un

⁷ Información adicional sobre CCID puede ser encontrada en USB Implementer's Forum web site, <http://www.usb.org>.

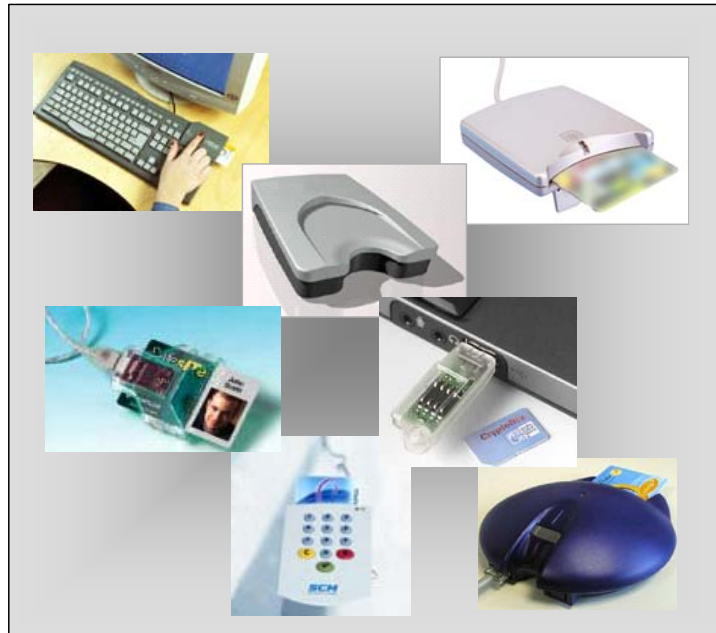
protocolo del transporte sobre el USB de modo que un sistema huésped pueda comunicarse con un lector de tarjetas inteligente. Una clase específica del USB ahora se define para los lectores de tarjetas inteligentes.

La adopción de la especificación de CCID permite a fabricantes inteligentes del lector de tarjetas construir los dispositivos que son obedientes con esta especificación. Los vendedores del sistema operativo pueden escribir un conductor que adhiera a esta especificación y apoye a todos los lectores CCID-obedientes. Microsoft ha lanzado un conductor CCID-obediente en la actualización de Windows para el Windows 2000 y Windows XP. El conductor será incluido en paquetes del servicio y todos los lanzamientos futuros del sistema operativo. El virar hacia el lado de babor al CE de Windows también se está considerando. Otros vendedores importantes del sistema operativo (por ejemplo, Apple y sol) también están incluyendo conductores nativos de CCID en sus sistemas operativos.

El uso de un lector de tarjetas inteligente CCID-obediente proporciona la ayuda verdadera del enchufe-y-juego, quitando cualquier necesidad del software adicional de ser instalado. Esto realza grandemente la experiencia del usuario.

El cuadro 3 demuestra una variedad de soluciones para conectar una tarjeta inteligente con una computadora, incluyendo contacto y lectores de tarjetas inteligentes sin contacto, dispositivos inteligentes de la tarjeta del USB y un lector de tarjetas inteligente con el lector biométrico integrado.

Figura 3: Ejemplos de Lectores de Tarjetas inteligentes⁸



⁸ Fotos facilitadas por Atmel, Axalto, Datakey, Gemplus, Honeywell, y SCM Microsystems. Información adicional sobre lectores de tarjetas inteligentes se puede encontrar en Smart Card Alliance smart card reader catalog en www.smartcardalliance.org.

Facilidad de Envío

Las herramientas de gerencia y los métodos de despliegue están disponibles para facilitar los largos despliegues de las tarjetas inteligentes. Los sistemas de gerencia de tarjeta integrados en el directorio de una organización o el sistema de consecución proporciona la funcionalidad necesitada para desplegar y para manejar tarjetas inteligentes y sus credenciales. Los conductores del lector y el middleware inteligente de la tarjeta son maduros y desplegados también fácilmente a través de una organización.

Tanto la alta gerencia como la gerencia dedicada a respaldar el proyecto siguen siendo aspectos críticos para una puesta en práctica acertada. Desplegar una nueva, cobertura del sistema de gerencia de la identidad de la organización que incluya tarjetas inteligentes, puede ser un proyecto complejo que se extienda a través de organizaciones múltiples y afecte negocio de base procesa.

Funcionamiento Multipropósito

Las tarjetas plásticas son un accesorio común dentro de muchas organizaciones y tienen muchas aplicaciones, tales como identificación, acceso físico, y tiempo y atención. Las tarjetas inteligentes permiten que las organizaciones realicen las ventajas de combinar todos tales usos en una tarjeta. El usuario puede entonces llevar una sola tarjeta para el acceso físico, el acceso lógico, la identificación, y otras funciones del negocio. Otras tecnologías asociadas a menudo a una tarjeta plástica, tal como cintas magnéticas, códigos de barras, tecnología de la radiofrecuencia (RF), y seguridad laminada se pueden utilizar conjuntamente con la tarjeta inteligente. En adición, así como los chips inteligentes la tecnología si contacto sigue haciendo avances en su capacidad⁹, las tarjetas inteligentes pueden hospedar aplicaciones que requieren la identificación sin contacto, tal como acceso físico a los edificios y a los servicios del transporte.

Las tarjetas inteligentes que respaldan la identificación sin contacto se describen a menudo como tarjetas inteligentes del procesador del híbrido o de –interfase dual. Una tarjeta híbrida contiene dos procesadores, una que apoya un interfaz de contacto y una que apoya un interfaz sin contacto. Los procesadores no están conectados generalmente. Una tarjeta de procesador de interfase dual contiene un chip sencillo que apoya el contacto e interfaces sin contacto. Las tarjetas del –interfase dual proveen de contacto y de la funcionalidad sin contacto un chip sencillo en una sola tarjeta, con diseños actuales permitiendo que la misma información sea alcanzada usando el contacto o a lectores sin contacto.

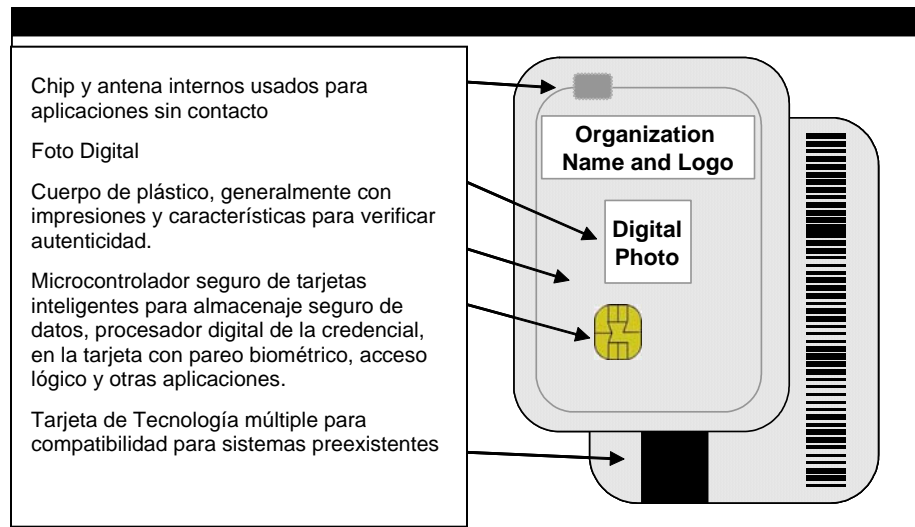
La mayoría de las organizaciones que utilizan actualmente las tarjetas inteligentes para el acceso físico y lógico han desplegado tarjetas inteligentes híbridas, usando el interfaz sin contacto para el acceso físico y el interfaz de contacto a un lector de tarjetas inteligente estándar de PC/SC en la computadora del usuario para el acceso lógico. Esto es porque, hasta hace poco tiempo, la tecnología inteligente sin contacto de la tarjeta no podía apoyar aplicaciones altamente seguros, basados en encriptación, y la infraestructura requerida para apoyar las puestas en práctica sin contacto para el acceso lógico (las aplicaciones y los lectores) no estaban disponibles. Hoy, los fabricantes de procesadores inteligentes están

⁹Un chip inteligente sin contacto se comunica con el lector usando RF y no requiere contacto físico con el lector.

comenzando a entregar procesadores de interfase dual con las capacidades del funcionamiento y de proceso requeridas para apoyar usos lógicos más sofisticados del acceso lógico. Las tarjetas del interfase dual ahora con certificación disponible que han alcanzado FIPS140-2, del nivel 3 (como una tarjeta acabada) o cc. EAL 5+ (como circuito integrado). Estos niveles de la seguridad son tan altos como están disponible de entran en contacto con solamente tarjetas inteligentes. Los vendedores de aplicaciones también están desarrollando las aplicaciones de acceso lógicos que utilizan estos procesadores de contacto o sin contacto. Además, los vendedores inteligentes importantes de lectores de tarjetas están comenzando a entregar estándares-basados en los lectores de la PC que se comunican en cualquier modo.

Figure 4 ilustra los componentes de una típica tarjeta de identificación inteligente

Figura 4: Ejemplo de tarjetas inteligentes de Identificación



Tarjetas Inteligentes como Distintivos de Identificación Inteligentes: Ejemplo de un Escenario

Para ilustrar qué sucede cuando las organizaciones proveen a los empleados con un distintivo inteligente de identificación que se utilice tanto para el acceso lógico como físico, considere un día típico en la vida de Kay Smith, el encargado ficticio de servicio al cliente para una compañía ficticia, "Enterprise Systems". La Enterprise Systems implementa un sistema de distintivos de tarjetas inteligentes para sus empleados desde hace dos años para sus empleados hace 2 años para integrar seguridad a través de la organización y para obedecer las políticas corporativas de seguridad en toda su extensión.

Antes de que La Enterprise Systems adoptará la sencilla solución de tarjeta inteligente de identificación, los accesos a los estacionamientos de la compañía era utilizando una tarjeta de cinta magnética. Las nuevas identificaciones inteligentes incluyen cintas magnéticas de modo que La Enterprise Systems puede seguir utilizando sus aplicaciones existentes de acceso al estacionamiento. Al principio de su día, Kay Smith tiene acceso a la porción del estacionamiento que ella tiene de la misma forma siempre, birlando su distintivo a través de un lector.

Una vez dentro del edificio, Kay debe presentar su divisa inteligente de la identificación al protector para verificar que la divisa es de hecho su divisa. El protector comprueba la foto en la divisa y la agita a través. Después, Kay agita su divisa cerca del lector RF-basado de la puerta así que ella puede dejar el pasillo y entrar en el área principal de la oficina. Los sistemas de la empresa podían mantener a sus lectores existentes del acceso del RF e incorporar la capacidad de acceso física en la divisa inteligente de la identificación. Las tarjetas inteligentes nuevas de la identificación fueron entregadas con las antenas integradas del RF que tienen interoperatividad con los lectores. El único cambio para los empleados es que ahora utilizan la misma tarjeta para conseguir en la porción del estacionamiento de la compañía y el área principal de la oficina.

Ahora que Kay está en su escritorio, ella gira su computadora e inserta su distintivo en el lector de tarjetas inteligente adjunto. El proceso estándar de la conexión de Windows reconoce a lector de tarjetas inteligente, y Kay es impulsada para entrar el PIN de su distintivo, que solamente Kay sabe. Kay ahora se registra sobre su computadora y puede seguir trabajando. Como ella tiene acceso a sus varias aplicaciones (por ejemplo., E-mail, base de datos del cliente, base de datos de respaldo) la impulsan para dar acceso a la contraseña o la otra credencial. La tarjeta inteligente de la identificación proporciona automáticamente la información requerida para tener acceso a esos usos, proveyendo de Kay una firma sencilla (sign-on) (usando el PIN de la autenticación inicial de la tarjeta). Antes de que a Kay le fuera dado su nuevo distintivo, ella tuvo que recordar 12 diversas contraseñas para diversos usos corporativos, que la frustraron .Ella a menudo escribió contraseñas abajo de las libretas, al lado de su computadora. Kay ama su nuevo distintivo, porque el proceso ahora es igual para ella no importa a qué aplicación ella tiene acceso. La tarjeta inteligente de la identificación es también configurable de modo que La Enterprise Systems puedan requerir diversos procesos de autenticación o las credenciales para cada aplicación si son necesarias (por ejemplo, requerir el PIN de entrada de la tarjeta para cada aplicación).

Kay requiere adherirse a ciertas políticas del E-mail de la compañía. Los mensajes sensibles del E-mail con respecto a ediciones de la información de producto nuevo o del recurso humano deben ser firmados y cifrados ser cifrados. Certificados digitales de las aplicaciones la Enterprise Systems para el E-mail. Para asegurar un mensaje del E-mail, Kay accesa a los mensajes de las opciones de seguridad y presiona sobre “firma y encriptación.”El sistema automáticamente accesa a la información de la firma digital sobre el distintivo de la tarjeta inteligente de Kay. Solamente el recipiente válido puede ahora abrir y leer el mensaje de Kay.

Es también una política de Enterprise Systems que los empleados deben llevar sus distintivos inteligentes de identificación siempre. Kay se dirigió hacia una reunión, teniendo donde ella va. Tan pronto como la tarjeta se quite del lector de escritorio, el tablero del escritorio de Windows es inaccesible hasta que Kay vuelve, reinsertó su distintivo, y reingresa su entra su PIN.

En casa a finales del día, Kay decide tener acceso a su E-mail y también confirmar una orden de pedido. Enterprise Systems utiliza los certificados digitales para el acceso de VPN. Kay utiliza su tarjeta inteligente conjuntamente con un VPN cliente en su ordenador personal para conectar con los sistemas Intranet de la empresa. La única información que ella necesita proporcionar es su PIN inteligente de la tarjeta, y estará conectada.

Durante el curso de su día laborable, Kay ha utilizado una sola tarjeta inteligente basada en distintivo inteligente para sustituir las tarjetas múltiples que concedían el acceso físico a las instalaciones de su empleador. El mismo distintivo ha facilitado y asegurado el acceso a los recursos de la información de su empleador, tanto local como distante y permitida en la utilización de estos recursos más eficientemente. Como este panorama ilustra, las tarjetas inteligentes son un acercamiento eficaz para combinar seguridad robusta con facilidad de utilización.

Ventajas Sobre Otras Alternativas para Acceso Lógico

El cuadro2 resume las ventajas que las tarjetas inteligentes pueden proveer para acceso lógico cuando es usada con diferentes mecanismos de autenticación.

La tecnología de tarjetas inteligentes representa un medio flexible y rentable para implementar cualquier técnica de autenticación. La tecnología ofrece ventajas tanto para el usuario de la tarjeta como para el que la emite, mejorando la experiencia de ambos a la vez que fortalece la autenticación y seguridad para acceso lógico.

Tabla 2: Reasaltando la Autenticación con Tarjetas Inteligentes

Mecanismo de Autenticación	Resultado	Valor añadido por Tarjetas inteligentes
Factor Simple de Autenticación		
Contraseñas estáticas	Fácil de adivinar, olfatear o robar Dificultad para reforzar las sólidas políticas de contraseñas Frustración del usuario y resistencia a cambiar y memorizar contraseñas Cuesta administraras	Un sistema de tarjetas inteligentes provee un contenedor seguro para contraseñas y automatiza el logon del usuario, aliviando al usuario de los requerimientos para administrar. Las políticas de contraseñas sólidas es fácil de reforzar.
Ficha pasiva o activa sin un PIN	Ficha perdida o robada	Un sistema de tarjetas inteligentes provee seguridad para la ficha básica (el token seed) y también añade PIN-basado en el acceso de la tarjeta, implementando una fuerte autenticación de dos factores. .
Lector biométrico	Respuesta al ataque Ataque disfrazado Credenciales Biométricas y pareo de seguridad	Un Sistema de Tarjetas inteligentes provee un almacenamiento seguro para patrones biométricos realiza el pareo biométrico en la tarjeta, y adiciona el PIN basado en acceso a la tarjeta implementando tres factores de autenticación.
Autenticación de dos factores		
Contraseña de uso único y ficha con PIN	Infraestructura compleja Figura en medio de un ataque Producto de una sola función OTP protección básica Costo del Ciclo de vida de la	Un sistema de tarjetas inteligentes reemplaza una ficha de una sola función por una de múltiples capacidades (asegurando la aplicación y acceso a la red)y reduce la complejidad total y el

Mecanismo de Autenticación	Resultado	Valor añadido por Tarjetas inteligentes
	ficha	<p>costo del ciclo de vida.</p> <p>La inversión en la tarjeta inteligente puede ser reforzada usando la tarjeta inteligente como un distintivo para un acceso seguro a los edificios.</p> <p>Las tarjetas inteligentes son programables. Las tarjetas pueden ser reutilizadas fácilmente, respaldando una mayor rentabilidad, para emitir una tarjeta de acceso temporal. Las funciones de las nuevas tarjetas inteligentes pueden ser agregadas después de ser emitidas, respaldando las actualizaciones a los nuevos sistemas de aplicaciones.</p>
Lector Biométrico y contraseña	Compleja infraestructura de red (back-end) Credencial de Seguridad	Un sistema de tarjetas inteligentes provee un almacenamiento seguro para los patrones biométricos y realice los pareos biométricos en la tarjeta.
Autenticación de tres factores		
Ficha, biométrica, PIN	Credencial de seguridad, ya sea en el servidor o en la estación de trabajo Infraestructura Compleja	Un sistema de tarjetas inteligentes provee un bajo mecanismo de 3 factores de autenticación cuando se integra con pareos biométrico en las capacidades de la tarjeta

Tarjetas Inteligentes y la Infraestructura Informática (IT)

Los sistemas operativos de escritorio modernos ofrecen un nivel significativo de la funcionalidad inteligente-relacionada, con cualquiera ayuda incorporada (fuera-de-la-caja) o los paquetes de software adicionales comerciales. Esta sección describe las capacidades integradas en los sistemas operativos de Microsoft® Windows® y los sistemas operativos libremente disponibles de Linux. Capacidades más sofisticadas están también disponibles de vendedores de tercera persona

Microsoft Windows

La familia del Microsoft Windows de sistemas operativos ha incluido la funcionalidad de la tarjeta inteligente, desde que el lanzamiento del ® 4.0 de Windows 98 y de Windows NT. Esta funcionalidad apoya tres tipos de operaciones:

- Comunicaciones de la tarjeta inteligente y el lector
- Control de acceso
- Servicios del Web y del E-mail

Comunicaciones entre las Tarjetas Inteligentes y el Lector

PC/SC

La tecnología básica para la comunicación entre los ordenadores personales y las tarjetas inteligentes es PC/SC, definido por el Workgroup de PC/SC, PC/SC define un Application Program Interface (API) que provee unos software desarrollados con un sistema estándar con un juego de herramientas para manejar a lectores de tarjetas inteligentes y comunicarse con los lectores y las tarjetas. El interfaz de PC/SC define los interfaces estándares para una variedad de relacionado-operaciones inteligentes de la tarjeta. Los más comunes son:

- Enumerando y describiendo a lectores de tarjetas inteligentes adjuntos.
- Petición de la información sobre estados de la tarjeta y del lector
- Cambio de comandos con las tarjetas

Microsoft ha puesto el PC/SC en ejecución API como parte del Win32® API, que es el set de herramientas fundamental para los usos de Windows del edificio. Microsoft es también un miembro del Workgroup de PC/SC.

El respaldo de Microsoft para la implementación de PC/SC se maneja como parte de ayuda del sistema operativo de Windows en su totalidad. Microsoft apoya contratos que están disponibles, al igual que la cuota de respaldo por incidentes.

Instalación de los conductores del lector

Microsoft lleva el mismo acercamiento para la instalación de conductores del lector de tarjetas inteligentes como para instalar otros orientadores (drivers) del hardware en el sistema operativo de Windows. Los fabricantes del lector proporcionan los orientadores de dispositivo que son instalados por el usuario. Después de que el orientador está instalado, el lector es visible con el PC/SC API. Además, instalan previamente a un puñado de lectores recomendados con Windows 2000, Windows XP, y Windows 2003.

La complejidad del proceso de la instalación depende de la conexión del hardware. La instalación y la configuración de un lector de tarjetas inteligente unido al puerto del USB son directas. El usuario conecta al lector con el puerto, inserta un disco del conductor (en caso de necesidad), y sigue los avisos. Los lectores que conectan con el puerto serial son algo más difíciles de instalar, puesto que el sistema operativo no puede reconocer automáticamente el tipo de dispositivo unido. Sin embargo, el proceso básico es igual: una al lector e instale el conductor.

Microsoft tiene un programa logo de Windows para los lectores de tarjetas inteligentes, que certifica que los lectores han sido probados por Microsoft y verificar su conformidad con la puesta en práctica de Microsoft de los estándares de PC/SC. Microsoft recomienda que las pruebas se realicen únicamente con lectores de tarjetas inteligentes aprobados con los sistemas operativos de Microsoft. Sin embargo, la mayor parte de los fabricantes de los lectores de tarjetas no aprobados han hecho un esfuerzo considerable en asegurarse de que su hardware es compatible con los sistemas operativos de Microsoft, y los problemas de la compatibilidad son raros.

CCID

La especificación del dispositivo del interfaz del chip de la tarjeta (CCID) es un acercamiento a la comunicación inteligente del lector de tarjetas que está ganando en renombre. La especificación define un protocolo de comunicación

estándar para los lectores de tarjetas inteligentes que conectan con una computadora vía el USB, permitiendo que el mismo conductor del anfitrión-lado se comunique con cualquier lector de tarjetas inteligente CCID-obediente. Microsoft proporciona un conductor de CCID a través del sistema de la actualización de Windows. Todo el nuevo lector de tarjetas inteligente que los despliegues deben considerar seriamente el usar de lectores CCID-obedientes, para reducir ediciones de la instalación del conductor y para asegurarse de que, en el futuro, los lectores de tarjetas inteligentes instalados puede ser fácil y transparentemente substituidor por cualquier otro lector CCID-obediente.

Lectores de tarjetas inteligentes sin contacto

Con especificaciones de PC/SC y ahora de CCID, los lectores de contacto han sido muy bien-estandarizados y fáciles de integrar. Con la finalización de la Revisión de la especificación de PC/SC 2.0, que se espera sea lanzada pronto, respaldo similar se ha introducido para los lectores de tarjetas inteligentes sin contacto. Se recomienda que las organizaciones interesadas en desplegar a lectores de tarjetas inteligentes sin contacto utilicen a lectores de PC/SC-complacidos.

Comunicación con Aplicaciones

Después de que un lector de tarjetas inteligente esté instalado y configurado, un programador de aplicaciones puede utilizar el PC/SC API para intercambiar comandos con una tarjeta inteligente en el lector. PC/SC hace una tentativa de ocultar las complejidades de diversos protocolos de comunicaciones del lector de tarjeta: pero no proporciona actualmente una abstracción de alto nivel de diversos tipos de tarjeta.¹⁰ El API proporciona un canal de comunicaciones para los comandos de la tarjeta. Inteligente La estructura de estos comandos es definida por estándares de ISO, pero el significado de comandos específicos es definido en gran parte por el fabricante de la tarjeta inteligente individual. El comunicarse con las tarjetas inteligentes en el nivel del uso requiere habilidad de programación.

Puesto que la semántica de los comandos está definida por la implementación única de cada tarjeta inteligente, las aplicaciones que se desean operar con diferentes tipos de tarjetas deben determinar de cuál tipo de tarjeta se trata y adaptar a los conjuntos de comandos de la tarjeta. Para algunas aplicaciones, como el de planilla usan la especificación EMV, el comando es estandarizado y la interoperatividad es asegurada por el vendedor de la tarjeta. Otras aplicaciones pueden alcanzar el mismo efecto usando sistemas operativos de tarjetas programables, tales como Java Card™ o MULTOS, de tal forma que esas tarjetas de diferentes vendedores pueden ser configuradas para responder al mismo conjunto de comandos de aplicaciones

Selección de la Aplicación

PC/SC proporciona la selección automática de la aplicación. Las aplicaciones se pueden registrar con PC/SC, solicitando la notificación cuando un tipo particular de tarjetas inteligentes se inserta en el lector. La inserción de una tarjeta acciona el cargamento de una aplicación que sabe como utilizar esa tarjeta.

¹⁰ Version 2.0 of the PC/SC specification is in progress and will provide some higher-level abstractions.

Autenticación del usuario

El Windows 2000 y Windows XP proporcionan el respaldo total a las tarjetas inteligentes-basadas en logo y autenticación, tanto una máquina local como un servidor del dominio de Windows. El sistema de autenticación de Windows se integra alrededor de PKI, usando un Certificate Authority central para publicar los certificados de la pre-tarjeta que se asocian al nombre del usuario de la máquina o del dominio del titular de tarjeta. Las aplicaciones de Microsoft Internet Explorer y de Outlook® Pueden también utilizar los certificados en tarjetas inteligentes.

Servicios de la Red y Correos Electrónicos

Muchos de los navegadores del Web que funcionan bajo Windows (tal como Internet Explorer y las familias populares de Netscape® y de Mozilla) pueden utilizar la tarjeta inteligente como símbolo PKCS#11. Un símbolo PKCS#11 sostiene certificados y realiza operaciones dominantes privadas. La certificación en la tarjeta inteligente puede realizar la certificación del lado del cliente basado en la autenticación de un servidor web, usando los protocolos de SSL/TLS. Además, la certificación puede firmar digitalmente en formato Web. No sólo una firma digital proporciona integridad y autentica el origen del contenido de la forma, en algunos lugares que puede también ser una firma legalmente reconocida

Muchos de los clientes del E-mail que funcionan en la plataforma de Windows, tal como Microsoft Outlook y los clientes del E-mail integrados en los navegadores de Netscape y de Mozilla, pueden también utilizar certificados inteligentes basados en tarjetas para firmar y para cifrar mensajes del E-mail. Un E-mail firmado digitalmente asegura que el recipiente pueda confiar en la identidad del remitente - especialmente importante puesto que el campo "De" en un mensaje de E-mail puede ser manipulado fácilmente. El cifrado del E-mail se asegura de que solamente el recipiente previsto pueda leer un mensaje y cualquier dato adjunto. Puesto que los mensajes del E-mail atraviesan rutinariamente muchos servidores y secuencias (routers) a menudo públicos, la criptografía es necesaria cuando se desean comunicaciones privadas.

Microsoft Outlook apoya la tecnología estándar de S/MIME para los mensajes de firma digital y cifrados. S/MIME utiliza los pares dominantes públicos/privados, incorporados a certificados, para realizar la firma, el cifrado, y operaciones del desciframiento. El estándar PKCS#11 permite a perspectiva utilizar una clave privada almacenada en una tarjeta inteligente para realizar operaciones digitales de la firma y del desciframiento. Se realiza la encriptación usando las claves públicas almacenadas por Outlook en la PC del usuario.

Criptografía de Sistemas de Archivo

El sistema de archivos NTFS proveído por Windows NT, Windows 2000, y Windows XP ofrece criptografía por archivo y por directorio para proteger el contenido de los archivos (pero no los nombres de los archivos). Las claves de la criptografía de archivos están cifradas con una o más claves públicas y guardadas con los archivos cifrados. La clave privada usada para conseguir la clave de los archivos cifrados es también usualmente guardado en el archive local del sistema pero también puede ser guardado en una tarjeta inteligente para mayor seguridad.

Para el usuario del sistema, la encriptación y desencriptación son transparentes. Una vez que el sistema es configurado, el usuario puede seleccionar los archivos que deberían ser asegurados. Estos archivos abrirán sólo cuando la tarjeta inteligente es insertada y serán inaccesibles cuando ésta es removida.

Acceder y escribir en archivos cifrados es a menudo notoriamente más lento que la misma operación en archivos no cifrados

Soporte Ofrecido por Diferentes Versiones de Windows

Diferentes versiones de los sistemas operativos de Windows ofrecen diferentes niveles de respaldo para tarjetas inteligentes. La más reciente versión, Windows XP, tiene el mejor respaldo. Esta provee todos los rasgos descritos arriba y vienen con discos integrados para una mejor selección de un mejor lector de tarjetas inteligentes. Casi todos los otros fabricantes de lectores de tarjetas inteligentes les proporcionan los discos para el uso con Windows XP. Windows 2000 también tiene un amplio respaldo para tarjetas inteligentes. La única diferencia significativa entre Windows 2000 y Windows XP está en la selección de discos de lectores de tarjetas inteligentes ofrecidos fuera de la caja. Pero, repetimos, otros fabricantes de lectores pueden proveer discos que funcionan con este sistema operativo.

Windows NT, Windows ME, y Windows 98 proporcionan un cierto nivel de respaldo para las tarjetas inteligentes. Proporcionan la mayor parte de las capacidades descritas anteriormente pero no proporcionan una selección amplia de los discos de lectores. Además, las dificultades son de menor importancia cuando ocurren, y son particularmente durante el proceso de la instalación. Windows ME y Windows 98 no utilizan el sistema de ficheros de NTFS y no proporcionan características del cifrado del sistema de ficheros, ni proporcionan la conexión inteligente-tarjeta-basada.

Windows 95 y Windows 95SE proporcionan respaldo no integrado para tarjetas inteligentes. Microsoft ha creado un módulo que puede ser instalado para implementar respaldo a las tarjetas inteligentes, pero el módulo es notoriamente difícil de poner a trabajar. Actualmente, Microsoft ha formalmente dejado de proporcionar respaldo a Windows 95, y no está claro por cuanto tiempo más Microsoft continuará distribuyendo el módulo de respaldo de tarjetas inteligentes

Linux

Las tarjetas inteligentes han estado disponibles durante varios años para sistemas que ejecutan el sistema operativo Linux. No hay respaldo de la tarjeta inteligente disponible dentro del núcleo de Linux, pero las herramientas del usuario proporcionan un ambiente de gran alcance para la tecnología de la tarjeta inteligente. La mayor parte de el trabajo de la tarjeta inteligente para Linux y otros sistemas operativos de Unix® es realizado por el proyecto MUSCLE (para más información, vea www.musclicard.com).

Una diferencia clave entre el respaldo de la tarjeta inteligente provisto por Linux o por la variedad de Unix y el sistema operativo Windows son las opciones. Las opciones disponibles de Microsoft son pocas pero complementarias. El mundo abierto de recursos provee grandes alternativas, pero muchas de las herramientas, particularmente para implementar funcionabilidad de alto nivel, de alguna forma son repetitivas. Los usuarios de las funciones de seguridad de tarjetas inteligentes en el mundo de los recursos debe hacer más investigación para entender cuáles opciones están disponibles, pero este esfuerzo es generalmente recompensado con una más apropiada y más flexible solución, para la cual a menudo no se requiere el pago de licencia.

Comunicaciones Tarjetas inteligentes- Lector

El componente central de la infraestructura de la tarjeta inteligente de Linux es una herramienta llamada PCSC Lite. PCSC Lite pone el PC/SC en ejecución API definido por el grupo de trabajo de PC/SC. Esta puesta en práctica proporciona

las mismas herramientas básicas que la implementación de PC/SC en Win32 API de Microsoft.

PCSC Lite

PCSC Lite es un software de recurso abierto, bajo licencia del BSD®- licencia de estilo que esencialmente da permiso a todos para hacer algo que les gusta, con tal de que ellos pasen la licencia a lo largo del módulo (véase el aviso de copyright en los archivos de fuente de PCSC Lite para los detalles). PCSC Lite se ha portado a muchas diversas plataformas, incluyendo Linux, Solaris™, FreeBSD, NetBSD, OpenBSD, Mac OS® X, HP-UX, y Microsoft Windows. Portarlo a otros sistemas operativos es bastante fácil.

PCSC Lite es estable, rápido, y fácil de utilizar. De hecho, algunos despliegues de Windows de tarjetas inteligentes han optado por utilizar PCSC Lite, más que la implementación nativa de Windows PC/SC, debido a la transparencia y la flexibilidad de PC Lite.

El libre respaldo para PCSC Lite está disponible a través de la lista del correo del proyecto, que es también donde ocurren las discusiones del diseño y del desarrollo. Las preguntas son contestadas a menudo dentro de una hora y casi siempre dentro de un día o de dos, a menudo por los mismos desarrolladores de PCSC Lite. La mayoría de las preguntas de la instalación y del desarrollo pueden ser contestadas buscando los archivos de la lista. El respaldo pagado está disponible por parte de algunos de los desarrolladores de PCSC Lite y se puede también obtener de las compañías que se especializan en el respaldo de software de recursos abiertos, tal como Red Hat.

La mayoría de las distribuciones de Linux proporcionan paquetes binarios fáciles de instalar que automáticamente instalan y configuran PCSC Lite

Disponibilidad de los Discos (Drivers) Lectores

Muchos de los fabricantes de tarjetas inteligentes ofrecen discos lectores PCSC Lite. Cuando los dispositivos de los discos lectores del fabricante proveído no están disponibles, algunas veces hay drivers de fabricantes independientes.

Discos para una selección grande de lectores de tarjetas inteligentes están disponibles en www.musclecard.com/drivers.html. Además, muchos lectores de tarjetas inteligentes usan conjuntos de chip compatibles, para que los lectores que no se listan explícitamente a menudo funcionen con un disco apropiado. El mejor acercamiento es seleccionar a un lector que se conoce para tener un buen respaldo del fabricante de PCSC Lite. Sin embargo, pueden localizarse a menudo discos para otros lectores a través del fabricante del lector o el PCSC Lite que manda por lista de correo. Si es necesario, un programador experimentado con las habilidades correctas y la documentación del fabricante apropiada debe poder producir un disco sólido de 1 a 2 semanas. Muchos de los desarrolladores del PCSC Lite ofrecen sus servicios para desarrollo de discos (drivers).

La mayoría de las distribuciones de Linux proporcionan pre-paquetes y a menudo preinstalación de discos para los lectores de las tarjetas inteligentes más comunes.

CCID

Hay un disco de CCID para PCSC Lite, para que todos los lectores de la tarjeta inteligente CCID-puedan trabajar en todas las plataformas respaldadas por PCSC Lite.

Autenticación del usuario

El proyecto MUSCLE proporciona las herramientas requeridas para implementar el "logon" basado en las tarjetas inteligentes y otra autenticación para cualquier sistema operativo que usa el sistema para la autenticación Pluggable Authentication Modules (PAM). Estos sistemas incluyen Linux y la mayoría de los sistemas operativos de Unix. MUSCLE proporciona el módulo de PAM, un applet de Tarjeta Java (para la tarjeta inteligente), herramientas de dirección, e instrucciones completas para instalar y usar el sistema de autenticación Muscle Card. Oberthur Authentic y Axalto se apoyan en tarjetas de Cryptoflex fuera-de-la-caja, como son todas las otras tarjetas inteligentes PKCS#11.

El sistema de MuscleCard también ha sido portado a Windows, como el Proveedor del Módulo del Servicio de Criptografía para Windows, permitiéndole a la infraestructura de la tarjeta inteligente ser usado con tarjetas de MuscleCard

Servicios de la Red y Correos electrónicos

El proyecto de MuscleCard proporciona módulos PKCS#11 que permiten la autenticación de Web y formatos de firmas a la mayoría de los navegadores de Linux, Unix, y Macintosh®. El proyecto también ofrece una cercana integración de S/MIME para todos los clientes del e-mail que respaldan S/MIME. El respaldo provee cualquier tarjeta obediente PKCS#11 o cualquier Tarjeta de Java a través del MuscleCard applet.

En adición algunos clientes de correo electrónico, tal como Kmail, proveen PGM/MIME para firma digital, encriptación y descripción de los mensajes de correo electrónico.

Criptografía de Sistemas de Archivo

Aunque Linux incluye varias herramientas para el cifrado del archivo, ninguno proporciona la conveniencia del archivo de encriptación NTFS. Sin embargo, las herramientas están disponibles para que las tarjetas inteligentes puedan abrir cualquiera de los sistemas de encriptación de archivos Linux.

Una herramienta Linux 2.4, Cryptoloop, transparentemente encripta y describe una partición del disco entera. Configura en una vía, Cryptoloop, que puede cifrar un sistema entero, para que el sistema ni siquiera se calzara las botas sin presentación de una contraseña apropiada o tarjetas inteligentes. Configurado otra manera, Cryptoloop puede proteger un bloque de almacenamiento dentro de otra parte partición no segura. En cualquier configuración, Cryptoloop tiene la ventaja que los nombres de los archivos y tamaños, así como los volúmenes del archivo, están ocultos de los usuarios no autorizados. Desafortunadamente, la seguridad de Cryptoloop ha sido cuestionada por expertos.

Con la introducción de Linux 2.6, los dm_crypt vieron a serla manera más recomendada de lograr encriptación del archivo transparente. Tal como Cryptoloop, el dm_crypt trabaja en particiones del disco completas o en los bloques de almacenamiento que el acto como las particiones. El dm_crypt tiene actuación significativamente mejor que Cryptoloop y, dependiendo del "cipherencryption" escogido, casi se puede operar tan rápidamente como un sistema de archivo de s encriptación.

Además, de los archivos transparentes del sistema del nivel de las herramientas, las herramientas que proporcionan servicios de encriptación para archivos sencillos o archivos archivados están disponibles. Algunas de estas herramientas protegen nombres del archivo y tamaños así como los volúmenes del archivo, y muchos de ellos integran con tarjetas inteligentes. El usuario debe tomar pasos para cifrar o descifrar cada archivo para el uso. Aunque una apreciación global completa de estas herramientas está más allá del alcance de

este documento, un ejemplo, KGPG, proporciona la encriptación de archivo de arrastrar-y-colocar (drag-and-drop) y desencriptación usando la herramienta GÑU Privacy Guard.

Soporte Ofrecido por Variedades Diferentes de Unix

Casi toda la funcionalidad de la tarjeta inteligente descritos aquí están disponibles bajo cualquiera de los sistemas operativos de Unix, incluso NetBSD, FreeBSD, OpenBSD, Solaris, HP-UX, Mac OS X, IRIX®, y muchos otros. Las únicas excepciones son Cryptoloop y dm_crypt que sólo operan bajo Linux.

Para más información sobre la tarjeta inteligente- relacionada con las herramientas y funciones sobre plataformas de no-Windows, use cualquier navegador de Internet que investiga (como Google) y el PCSC Lite que manda lista por correo

Uso de Tarjetas Inteligentes para Aplicaciones Múltiples

Organizaciones que seleccionan tarjetas inteligentes para el control de acceso lógico pueden incluir aplicaciones adicionales en la tarjeta. Dos recientes desarrollos lo han hecho para práctico usar una sola tarjeta inteligente para las aplicaciones múltiples. Primero, las capacidades de memoria de tarjeta han aumentado. Segundo, los sistemas operativos de multi-aplicación están disponibles ahora.

Las aplicaciones múltiples de respaldo en la misma tarjeta ofrecen varias ventajas:

- Reduce los costos. El aumento marginal en costo por agregar aplicaciones a una tarjeta es significativamente menor que emitir tarjetas adicionales.
- La conveniencia de los portadores de tarjetas .Es más conveniente llevar una tarjeta que muchas.
- Aumenta la eficacia. En algunos casos, puede ser posible usar las mismas credenciales digitales para varias aplicaciones y puede aumentar los beneficios de tarjetas de aplicación múltiple.
- Permite la propuesta comercial. Con el respaldo de aplicaciones múltiples con un sol distintivo de tarjetas inteligentes de identificación, las organizaciones pueden mejorar el retorno de la inversión para la tecnología de ID y preservar la flexibilidad para manejar necesidades futuras apoyando.

Uso de Aplicaciones Múltiples

Las tarjetas inteligentes que implementan aplicaciones de acceso lógico pueden respaldar una variedad de otras aplicaciones, incluso lo siguiente:

- Aplicaciones de acceso físico
- Aplicaciones de pago
- Almacenamiento de los datos seguro
- Aplicaciones de firma de documento segura
- Aplicaciones de formato de realización
- Acceso de la red Inalámbrica

Control de Acceso Físico

Las tarjetas inteligentes están idealmente preparadas para las aplicaciones de control de acceso físico, gracias a su integración en capacidades del multi-

aplicación. Las tarjetas inteligentes sin contacto constituyen una versión revisada de la tecnología ideal en particular a las que ampliamente usaron 125-kHz como tecnología de proximidad, ofreciendo la conveniencia y medioambiental – y características de rasgos vándalo-resistentes de tecnología de proximidad mientras agregaban capacidades de seguridad significativas, capacidad de mayor almacenamiento y respaldo de aplicación múltiple.

A diferencia del pasado, cuando las tarjetas estaban equipadas con menos memoria y menos rasgos de seguridad, hoy día el control de acceso a las aplicaciones puede ahora ser implementado usando diferentes mecanismos. En los sistemas tradicionales de control de acceso, una tarjeta contiene un número único que En sistemas de mando de acceso tradicionales, una tarjeta contiene un único número que apunta a una entrada en un banco de datos que graba el nombre del portador y derechos de acceso. Cuando esta clase de tarjeta es presentada a un lector, el número es transmitido a un anfitrión, el cual permite o niega el acceso, basándose en el número de acceso de ese registro en la base de datos. La entrada del banco de datos para ese número.

El método tradicional puede seguir siendo usado por las tarjetas inteligentes de hoy día, pero una nueva alternativa está disponible. La alternativa es almacenar todas las credenciales del tarjeta habiente de manera segura en la propia tarjeta inteligente. Cuando la tarjeta es presentada al lector, este permite el acceso sin necesidad de estar conectado a un sistema del organizador (host system). Puesto que hoy las tarjetas inteligentes tienen mayor capacidad de almacenamiento, las actuales transacciones de acceso pueden estar escritas en la tarjeta y ser recogidas más tarde cuando el tarjeta habiente presenta la tarjeta a un lector las transacciones actuales de la tarjeta pueden ser y ser recogidas más tarde cuando el tarjeta habiente presenta la tarjeta a un lector en línea.

Otra forma en la cual las aplicaciones de acceso físico pueden tomar ventaja de la creciente capacidad de almacenamiento de la tarjeta es usando información biométrica como un factor de autenticación. La tarjeta inteligente puede almacenar de forma segura información biométrica del tarjeta habiente. Cuando la tarjeta es presentada a un lector biométrico, la información biométrica es retrotraída de la tarjeta, y comparada a la del tarjeta habiente para validar la identidad de éste. Si la aplicación usa una de las tarjetas inteligentes más poderosas con un microcontroladores incluyendo, los datos biométricos pueden compararse y pueden emparejarse en la tarjeta. Un "pareo en la tarjeta asegura un alto grado de privacidad. Los datos biométricos nunca dejan la tarjeta, y la tarjeta puede destruirse cuando el portador deja una organización.

Números crecientes de organizaciones tanto en el sector público como en el sector privado están adoptando tarjetas inteligentes para respaldar acceso físico y lógico que usa una sola tarjeta. Por ejemplo, el nuevo distintivo empleado por Microsoft no sólo abre puertas que usan una interfase sin contacto, también respalda el logon de la red seguro que usa una aplicación que reside en el chip de contacto incrustado en la tarjeta.

Un acceso físico y lógico combinado de la tarjeta inteligente permite acceso físico a la verificación de identidad rápida a los edificios, entrega un usuario robusto y una tarjeta de identificación autenticada (usando firmas digitales, datos biométricos, y tecnologías de contraseña/PIN), permite no-repudiación de transacciones, y correo electrónico cifrado. Si una organización busca que cosas así beneficien como parte de un plan de seguridad de red global, los beneficios pueden cuantificarse y pueden incorporarse en la propuesta comercial global para la adopción de tecnología de la tarjeta inteligente.

Actualmente, un obstáculo mayor al desarrollo del mercado para tarjetas de ID que apoyan acceso físico y " lógico es la separación histórica de seguridad física

y seguridad de la red. Estas dos funciones generalmente son manejadas por dos partes diferentes de una organización, cada uno con una misión separada, presupuesto y la infraestructura técnica. Sin embargo, cuando la tecnología de la tarjeta inteligente está disponible más ampliamente en una variedad de formas (ej., de contacto, sin contacto, USB), más organizaciones están desarrollando una propuesta comercial que integra estas dos funciones de seguridad para lograr economías del costo y mejorar ampliamente la seguridad de la organización.

Pagos

Las tarjetas inteligentes respaldan transacciones de pago a través tanto de los interfaces de contacto como sin contacto. Por ejemplo, el Washington la Autoridad de Tránsito de Aéreo Metropolitana (WMATA) emite a los pasajeros la tarjeta inteligente sin contacto que llamó la tarjeta de SmarTrip®. Los pasajeros cargan una cantidad de la tarifa hacia una tarjeta, entonces usa la tarjeta para acceder al metro a través de los torniquetes de la entrada que simultáneamente deducen la cantidad de la tarifa de la cantidad guardada en la tarjeta.

Al usar la tecnología de tarjetas inteligentes sin contacto para pagos fueron los pioneros para el pago en el sector del transporte, donde la combinación de pago seguro y el acceso físico rápido es un requisito crítico. Los pagos con-tarjetas-respalda los pagos y están empezando a aparecer de manera general al detal. American Express, MasterCard y Visa todos tienen programas que usan tecnología sin contacto para llevar a cabo las transacciones de pago de tarjetas de crédito seguras.

Las aplicaciones de pago también pueden ser respaldadas por un chip de contacto incrustado en el mismo cuerpo de la tarjeta como un chip sin contacto usado para acceso físico. Actualmente, el de chip de contacto respalda una ancha variedad de aplicaciones de pago, tales como colectas electrónicas que guardan valor monetario al crédito convencional y transacciones de débito. La especificación de EMV global permite tarjetas inteligentes para respaldar chips basados en crédito transacciones de débito así como las tarjetas de cintas magnéticas que hacen hoy.

Una tarjeta inteligente que se piensa que respalda inicialmente el control de acceso lógico puede incluir una aplicación que respalda una amplia variedad de funciones de pago. La combinación de estas funciones puede producir un caso comercial más complejo para la adopción de tecnología de la tarjeta inteligente. Por ejemplo, el banco de una empresa puede proporcionar una tarjeta inteligente corporativa a empleados que incluyen la aplicación del pago del banco y un chip de contacto para acceso físico a las facilidades. La empresa beneficia al no tener que ejecutar dos tarjetas con programas separados, y el banco puede suscribir algún costo por manejar el programa de acceso físico.

Otro escenario (y uno que ya se ha llevado a cabo en varios organizaciones) es la llamada "tarjeta del campus". La tarjeta del campus tarjetas inteligentes de múltiples aplicaciones que puede usarse como una tarjeta de ID (incluso un cuadro) y también puede usarse para pagar por la comida y artículos en expendedores automáticos, abrir puertas del dormitorio, revisar libros de la biblioteca, y pagar por las llamadas telefónicas. Generalmente, estas tarjetas emplean una variedad de tecnologías, como cinta magnética, código de barra y un chip de tarjetas inteligentes, para respaldar una amplia gama amplia de aplicaciones. La mayoría de las aplicaciones respaldan el control de acceso físico en combinación con el pago y una variedad de aplicaciones adicionales de los cuales todas agregan valor a la tarjeta.

Almacenaje y Administración de Datos Seguro

Están usándose tarjetas inteligentes de varias maneras innovadoras para respaldar funciones que requieren almacenamiento seguro, almacenaje portátil de información sensible y no tan sensible. Por ejemplo, pueden guardarse archivos médicos en una tarjeta inteligente para que sólo el portador o el doctor del portador puedan acceder los archivos. Acceder tales archivos es típicamente protegido por un PIN

De manera similar, el Departamento de Defensa ha emitido más de 5.4 millones de Tarjetas de Acceso Comunes (Common Access Cards , CAC) para activar el personal militar, personal de la reserva seleccionado, empleados civiles, y personal del contratista seleccionado que incluye aplicaciones de almacenamiento seguras. El CAC puede guardar información relacionada a la historia médica u otros datos pertinentes a la misión del portador

Tarjetas sin contacto usadas para los sistemas de acceso físicos pueden guardar información que rastrea de manera segura el uso de la tarjeta. Por ejemplo, una tarjeta sin contacto puede usarse para grabar datos que describen acceso a un edificio particular (es decir, situación de la puerta, tiempo, la fecha) para la recuperación y interviniendo. Esta función puede ser manejada por la tarjeta o por un servidor central.

Acceso de la Red inalámbrica

Las tarjetas inteligentes permiten a las organizaciones controlar el acceso a las redes inalámbricas. Las tarjetas inteligentes pueden proporcionar una sólida y, autenticación de multi-factor, protección criptográfica de respaldo de volumen, y facilita la sesión clave de gerencia. Adicionalmente, las tarjetas inteligentes permiten movilidad del obrero dentro de las organizaciones y respaldan tanto la re-autenticación como la configuración de la gerencia. Con una tarjeta inteligente, un PIN, y las credenciales de acceso apropiadas, usuarios inalámbricos con una gama variante de requisitos de información (empleados, clientes, los compañeros) puede identificarse de manera única a redes o aplicaciones.

Instalación de la Aplicación

Cuando una tarjeta inteligente se usa para llevar aplicaciones múltiples, las aplicaciones pueden cargarse antes o después de que la tarjeta se emite. Hasta recientemente, los procedimientos de instalación de aplicación eran propietario. Sin embargo, en los últimos 2 años Global Platform ha creado normas por personalizar tarjetas y las aplicaciones cargantes. Las normas de Global Platform permiten emisores de la tarjeta para combinar soluciones de las fuentes múltiples con confianza.

La instalación de la post-emisión requiere un poco más de esfuerzo que la instalación de la pre-emisión. La información sobre las tarjetas emitidas debe estar disponible, incluso la cantidad de memoria disponible en la tarjeta, se necesitan qué claves o certificados acceden a la tarjeta, y se necesitan qué claves o certificados instalen nuevas aplicaciones. Tal información está típicamente disponible a través de una tarjeta con el ciclo de vida del sistema gerencial. La instalación de la post-emisión también requiere que la tarjeta pueda conectar al organizador que proporciona la nueva aplicación. Por último, instalando aplicaciones después de que una tarjeta emita allí una relación entre el emisor de la aplicación y el emisor de la tarjeta. El emisor de la tarjeta debe permitir o debe tener disponible la aplicación terciaria para cargar a la tarjeta. Ambas partes necesitan información sobre lo que está en la tarjeta.

Ejemplos de la Aplicación múltiples

La Tabla 3 muestra ejemplos de cómo están usándose tarjetas del multi-aplicación actualmente en muchas aplicaciones. Puede encontrarse información detallada sobre cada aplicación en el Apéndice A.

Tabla 3: Aplicaciones del multi-aplicación

Organización	Aplicaciones de Tarjetas inteligentes
Boeing	<ul style="list-style-type: none"> • Distintivo de identificación del empleado • Acceso Físico • Acceso lógico • Windows 2000 logon con PIN, PKI y applets biométricos • Firma única Web • Contraseña de bolsillo "wallet" • Autenticación VPN • Otras aplicaciones planeadas: Data/e-mail electrónico cifrados, firmas electrónicas, pago de cafetería, almacenaje de datos personales, rol basado en acceso
Microsoft	<ul style="list-style-type: none"> • Distintivo de identificación del empleado • Acceso Físico • Acceso remoto y logon para redes corporativas usando PKI
Rabobank	<ul style="list-style-type: none"> • Acceso lógico a redes y aplicaciones usando PKI • Microsoft Windows logon • Firmas digitales
Shell Group	<ul style="list-style-type: none"> • Acceso físico • Acceso a red y escritorio usando PKI • Documento y correo electrónico y firma cifrado
Sun Microsystems JavaBadge	<ul style="list-style-type: none"> • Distintivo de identificación del empleado • Acceso Físico • Acceso a red y escritorio usando PKI • Acceso a red remota • Firma única Web • Documento, transacción y correo electrónico y firma cifrado • Pago "E-purse"
U.S. Department of Defense Common Access Card	<ul style="list-style-type: none"> • Distintivo de identificación del empleado • Acceso lógico a red y escritorio usando PKI • Documento y correo electrónico y firma cifrado • Otras aplicaciones planeadas: acceso físico, autenticación biométrica
U.S. Department of State	<ul style="list-style-type: none"> • Distintivo de identificación del empleado • Acceso Físico • Acceso físico usando PKI, incluyendo seguridad del escritorio y encriptación, e-mail seguro, y acceso VPN • Otras aplicaciones planeadas: biométricas, almacenaje de los datos seguros

Propuesta de Negocio para Tarjetas inteligentes y Acceso Lógico

Muchas empresas están considerando hoy en día la utilización de as Tarjetas Inteligentes y el Acceso Lógico seguro .Un reciente estudio ¹¹ de U.S. Fortune a 500 compañías revelaron a lo siguiente:

- Todas las compañías inspeccionadas (100%) son conscientes de la tecnología de la tarjeta inteligente.
- Más del 63% de los ejecutivos o entrevistados han investigado o han estado investigando tarjetas inteligentes para seguridad de la red.
- Más del 39% de las compañías inspeccionó plan para usar tarjetas inteligentes para reforzar y fortalecer sus sistemas de seguridad corporativos dentro de los próximos 3 años.
- UN total de 30% de las compañías está usando actualmente o está probando tarjetas inteligentes dentro de sus sistemas de seguridad.

Para las tarjetas inteligentes la inversión de tecnología debe ser apoyada por la propuesta de negocio apropiada que requiere consideración de beneficios tangibles e" intangibles

Beneficios intangibles

Los negocios invierten en tecnología de autenticación sólida por dos razones principales:

- Complacencia o cumplimiento y Regulación
- Posicionamiento estratégico

Cumplimiento de las Regulaciones

A los negocios generalmente se les exige que mejoren sus procesos de autenticación para cumplir con requerimientos externos.

Esos requerimientos externos incluyen nuevas legislaciones o regulaciones (por ejemplo, HIPAA, Sarbanes-Oxley) y otros estándares gubernamentales o industriales. En tales casos, los negocios regularmente se les requiere que demuestren que ellos reúnen ciertos estándares prescritos. La falta de cumplimiento con estos estándares puede resultar en sanciones financieras.

El requerimiento de elevar los sistemas de información para ofrecer autenticaciones más sólidas es comúnmente visto por los gerentes seniors como el costo de hacer negocios en determinado sector o mercado. En adición, las violaciones a la privacidad pueden resultar en significativas sanciones.

Posicionamiento Estratégico.

Las tarjetas inteligentes forman parte de la columna vertebral de la seguridad de una empresa. En este respecto, no hay diferencia entre servidores de directorio, VPNs, sistemas de detección de intrusos o firewalls. Los negocios están empezando a reconocer que para mantener una ventaja competitiva ellos necesitan asegurar que sus activos intelectuales están bien defendidas.

¹¹ "Fortune 500 Companies' Preference for Corporate Security Applications," Frost & Sullivan, Feb. 17, 2003.

Ciertos negocios han establecido una posición Oficial Jefe de Seguridad (CSO) para asegurar que las preocupaciones relacionadas con la seguridad son atendidas y manejadas de manera integral. Para ser efectiva, el CSO regularmente reporta al CEO. Las tarjetas inteligentes son atractivas en este tipo de ambiente, puesto que ellas actúan como puentes entre los dominios de seguridad física y lógica.

Beneficios Tangibles

Es altamente probable que una organización que considere una tarjeta inteligente para el desplazamiento tenga una infraestructura preexistente, que por lo general incluye lo siguiente:

- Usuario –contraseña basada en autenticación local.
- Fichas OTP para acceso remoto seguro para proteger activos
- Infraestructura del distintivo de identificación de empleado con respaldo sistema de control de acceso físico

Las organizaciones a menudo consideran un sistema de acceso físico y lógico combinado basado en tarjetas inteligentes o smart cards. Estas tarjetas incluyen una interfase sin contacto para respaldar el acceso al edificio y una interfase con contacto para respaldar el acceso lógico. Históricamente, estos dos componentes han estado físicamente separados, pero ahora hay una creciente tendencia a que ambas funciones se respalden en un chip de interfase dual con significativa capacidad para procesamiento y almacenamiento de información.

Los beneficios de un sistema de esta índole incluyen lo siguiente:

- Simplificación en la administración del usuario.
- Eliminación de fichas de OTP y la infraestructura asociada (ej., servidores)
- Incrementar la productividad del usuario

Simplificación en la administración del usuario.

El gasto significativo es asociado con el mantenimiento de sistemas de la autenticación contraseña-basado en los sistemas tradicionales. Por ejemplo, el Aberdeen Group ha encontrado que el costo de configurar y mantener sistemas de contraseña para las compañías pequeñas promedia \$100 a \$150 por usuario por año. Costos para una compañía mediana- promedia en \$200, y una empresa grande gasta un promedio de \$300 a \$350.12 por usuario por año. De hecho, no es raro para el Departamento de Informática y las secciones establecer un cargo interior por manejo y mantenimiento de la contraseña. Los sistemas de dirección de tarjetas inteligentes ofrecen "de autoservicio" capacidades que pueden reducir lo administrativo sobre los aspectos principales del manejo de la contraseña. Mientras los secretos (comoPIN) todavía necesitan ser manejados, un sistema de dirección de tarjetas inteligentes incluye una capacidad de dirección de usuario desatendido que puede disminuir el gasto significativamente asociado con el mantenimiento de estos secretos típicamente establecidos.

¹² "Ask the Analyst: Passwords Are Gobbling Up your Profits," Jim Hurley, Aberdeen Group, May 1, 2003

Eliminación de Fichas de OTP

Las fichas de OTP son caras de adquirir y manejar y tienen una proporción de fracaso significativa. El costo típico para una ficha de OTP puede acercarse a los \$100 por año por usuario. Las tarjetas inteligentes ofrecen funcionalidad equivalente pero a un costo total reducido de propiedad.

Reducción de Infraestructura Global

Las aplicaciones de acceso lógicas y físicas combinadas en una sola ficha ofrecen la oportunidad de eliminar tecnología redundante a las organizaciones. Típicamente, pueden posicionarse sistemas basados en tarjetas inteligentes- como una versión revisada, en lugar de un reemplazo para, los sistemas de acceso físicos actuales.

Incrementando la Productividad

La introducción de tarjetas inteligentes normalmente coincide con otras iniciativas diseñadas para simplificar el flujo de trabajo comercial, por eso la creciente y eficaz productividad del empleado. La autenticación sólida generalmente aumenta la eficacia de varios servicios internos y externos y rinde una in mensurable rentabilidad. Pueden multiplicarse tales mejoras si los compañeros comerciales también usan el mismo software o softwares interoperables.

Inversión

Las tarjetas inteligentes y los sistemas asociados de tarjeta inteligente representan una inversión. El nivel de inversión depende de varios factores, incluyendo la infraestructura actual de la organización y la técnica de la autenticación que están llevándose a cabo. Los gastos descritos abajo se requieren para adquirir y desplegar tarjetas inteligentes basadas en un sistema de autenticación.

Fichas de la tarjeta inteligente. Tarjetas inteligentes son más caras por si mismas que las tarjetas de ID preexistentes. Un premio de \$5 a \$10 por la tarjeta es típico para las tarjetas inteligentes.

Lectores de la tarjeta inteligentes. No es raro ahora para las computadoras ser entregado con lectores integrados en la tarjeta inteligente. Para los sistemas preexistentes, un lector de la tarjeta inteligente externo típico que puede ser adjuntado al puerto de USB de una computadora puede adquirirse por aproximadamente \$15 (en volumen). Las tarjetas inteligentes basadas en fichas de USB pueden ser conectadas directamente en el puerto USB de una computadora y no requiere ninguna inversión del hardware adicional.

Middleware. Para habilitar el proceso de autenticación de tarjetas inteligentes, deben instalarse middleware en las estaciones de trabajo de cada usuario. Los costos van de \$2 a \$10 por asiento y dependen de la técnica de la autenticación a implementarse.

Sistema de Administración de Tarjetas inteligentes. Un sistema de Administración de tarjetas inteligentes respalda la emisión y el ciclo de vida de la administración de las tarjetas inteligentes y las credenciales guardadas en ellos. Los sistemas varían en la capacidad y complejidad que dependiendo de la técnica de la autenticación respaldadas y pueden ir de \$5 a \$50 por usuario.

Infraestructura de la Técnica de Autenticación. Cuando se usa para acceso lógico, las tarjetas inteligentes implementan la técnica de la autenticación seleccionada de una organización o combinación de técnicas. Las técnicas pueden incluir contraseñas de varios tipos, claves simétricas basadas en autenticación, claves asimétricas basadas en autenticación, y biométricas. El costo de la infraestructura para respaldar la técnica de la autenticación escogida necesita ser considerada. Las tarjetas inteligentes proporcionan una ventaja. Su habilidad de respaldar técnicas de autenticación múltiples en una sola tarjeta de ID permite a la organización implementar una sólida autenticación exigida para conocer los requisitos de seguridad de la organización. La habilidad de agregar aplicaciones a las tarjetas inteligentes después de la emisión inicial permite a las organizaciones comenzar a usar tarjetas inteligentes con una contraseña sencilla almacenada y agregar técnicas de autenticación sólidas como deseasen, sin reinvertir en tarjetas y lectores.

Otros Costos del Proyecto. Desplegando un nuevo sistema de administración de identidad puede ser un proyecto de gran escala. La inversión requerirá de procesos de administrativos de re-ingeniería, utilizando entrenamiento y se apoyará, así como para la configuración del sistema inicial y despliegue y dirección del proyecto.

Tabla 4 resume los beneficios potenciales claves, ahorros y costos que deben ser considerados al implementar una solución de tarjetas inteligentes basado en accesos lógico

Tabla 4: Sistema de Tarjetas inteligentes con Acceso Lógico – Ahorros y Costos

Beneficios y Ahorros Claves	Costos
<ul style="list-style-type: none"> - Simplificación de la administración de la contraseña del usuario - Incrementando la conveniencia del usuario. • Eliminación de Fichas de OTP • Reducción de los costos de la infraestructura combinando funciones múltiples en indistintivo de • Legislación y regulaciones de cumplimiento • Mejoramiento de la productividad del usuario y reducción de costos de operaciones. <ul style="list-style-type: none"> - Fácil acceso a los recursos de la red. - Mejoramiento de los procesos administrativos (ejemplo firma de documento) • Reducción de los riesgos de ruptura de seguridad y los costos resultantes (ejemplo, aspectos financieros, productividad, ventas, posicionamiento del mercado, exposiciones legales) • Habilidad para migrar a técnicas sólidas u otras sin reinvertir en tarjetas y lectores 	<ul style="list-style-type: none"> • Costo de la ficha de la tarjeta inteligente • Costo del lector de tarjetas inteligentes (si es utilizado con tarjeta de fábrica) • Middleware del cliente • Sistema de administración de la tarjeta inteligente. • Costos de infraestructura y respaldo de la técnica de autenticación seleccionada (ejemplo biométricos, PKI, claves simétricas) • Costos de los proyectos de IT: proyectos administrativos, entrenamiento del usuario, procesos administrativos de reingeniería, sistema de configuración y desplazamiento.

Conclusiones

Virtualmente cada día una nueva noticia destaca la importancia de la seguridad en las redes corporativas son quebrantadas, sistemas de información son accesados por individuos no autorizados y las identidades son robadas y usada para realizar transacciones fraudulentas. Como resultado de ello, tanto los negocios como los gobiernos están evaluando o implementando nuevos sistemas de administración/manejo de identidades para proveer un acceso lógico más seguro.

Una sólida autenticación para acceso lógico requiere del uso de múltiples factores de autenticación. La tecnología de tarjetas inteligentes – por lo regular es usada en conjunto con un PIN para abrir la tarjeta – es usada cada vez más para ofrecer el segundo o tercer factor crítico de autenticación que hace el acceso lógico más seguro.

La tecnología de Smart card está disponible en múltiples formas (tarjeta plástica, dispositivo USB, o teléfonos móviles con SIM chip) y respalda cualquiera o todas las técnicas de autenticación comúnmente usadas para asegurar acceso lógico. Los dispositivos de tarjetas inteligentes son seguros, resistente a la falsificación y fáciles de usar. Las tarjetas inteligentes pueden respaldar múltiples aplicaciones, permitiendo a una sola ID card realizar múltiples funciones. Por ejemplo, la misma tarjeta inteligente de identificación puede permitir a un individuo entrar seguro a un edificio, conectarse en una red corporativa segura, firmar documentos de manera segura, cifrar correos electrónicos y transacciones y pagar su almuerzo en la cafetería de la organización. Esta flexibilidad facilita a la organización desarrollar una sólida propuesta de negocio para tarjetas inteligentes basadas en los sistemas de control de acceso.

La Smart Card Alliance urge a las organizaciones quienes están evaluando una nueva administración de identidad y de control de acceso lógico seguro a implementar un sistema sólido de autenticación basado en la tecnología de tarjetas inteligentes. La tecnología de tarjetas inteligentes provee las bases para aplicaciones de acceso lógico de privacidad, confianza y seguridad. La combinación de tecnología de tarjetas inteligentes y multifactor de autenticación mejora la seguridad, aumenta la conveniencia del usuario y conlleva fuertes beneficios comerciales.

Para mayor información acerca de las tarjetas inteligentes y el pape que ellas juegan en una identificación segura y otras aplicaciones, favor visitar The Smart Card Alliance web site en www.smartcardalliance.org o contacte directamente a the Smart Card Alliance al 1-800-556-6828.

Referencias y Fuentes

"2004 E-Crime Watch™ Survey Shows Significant Increase in Electronic Crimes," CSO Magazine survey conducted in cooperation with the United States Secret Service and Carnegie Mellon University Software Engineering Institute's CERT® Coordination Center, May 25, 2004 (http://www.csoonline.com/releases/052004129_release.html)

"Ask the Analyst: Passwords Are Gobbling Up your Profits," Jim Hurley, Aberdeen Group, May 1, 2003

"The Boeing Company Chooses Siemens to Enhance Physical and Information Security with Identity Management System," Siemens and Boeing press release, Sept. 8, 2003, http://www.siemens.com/index.jsp?sdc_p=cs4uo1093899pnflm

"Boeing SecureBadge Program," Sharon Lindley, SecureBadge Program Director, Boeing, Smart Card Alliance Annual Conference presentation, Oct. 16, 2003

Department of Defense Personal Identity Protection (PIP) Program, DoD Directive Number 1000.25, July 19, 2004 (<http://www.dtic.mil/whs/directives/corres/html2/d100025x.htm>)

Electronic Authentication Partnership (EAP), <http://www.eapartnership.org>

"Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology," NIST Computer Security Division, NIST Special Publication 800-63, Version 1.0, June 2004

"Endpoint Security Management: Maximizing Best of Breed," IDC report, March 4, 2004

"Fortune 500 Companies' Preference for Corporate Security Applications," Frost & Sullivan, Feb. 17, 2003

"FTC Releases Survey of Identity Theft in U.S. 27.3 Million Victims in Past 5 Years, Billions in Losses for Businesses and Consumers," FTC press release, Sept. 3, 2003, <http://www.ftc.gov/opa/2003/09/idtheft.htm>

Global Platform (<http://www.globalplatform.org>). Industry association that is creating and advancing interoperable technical specifications for smart cards, acceptance dispositivos and systems infrastructure.

"Government Smart Card Handbook," February 2004, available at <http://www.smartcardalliance.org>

"HIPAA Compliance and Smart Cards: Solutions to Privacy and Security Requirements," Smart Card Alliance report, September 2003, available at <http://www.smartcardalliance.org>

Initiative for Open Authentication (OATH), <http://www.openauthentication.org>

International Civil Aviation Organization (ICAO) Machine Readable Travel Documents (MRTD), <http://www.icao.int/mrtd/Home/Index.cfm>

MUSCLE Project (<http://www.musclecard.com>). MUSCLE is a project to coordinate the development of smart cards and applications under Linux.

NIST Personal Identity Verification (PIV) Project (<http://csrc.nist.gov/piv-project/index.html>)

Liberty Alliance, <http://www.projectliberty.org>

“One Card Fits All,” Boardroom Minutes: Technology Intelligence for Business Executives, available at <http://www.sun.com/software/sunone/boardroom/newsletter/0603solutions.html>

OpenCard Consortium, <http://www.opencard.org>

Open Security Exchange (OSE), <http://www.opensecurityexchange.com>

PC/SC Workgroup (<http://www.pcscworkgroup.com>). Industry group who developed the PC/SC specification, which defines how to integrate smart card readers and smart cards with the computing environment and how to allow multiple applications to share smart card dispositivos.

“Phishing Victims Likely Will Suffer Identity Theft Fraud,” Gartner press release, May 14, 2004, http://www3.gartner.com/5_about/press_releases/asset_71087_11.jsp

“Privacy and Secure Identification Systems: The Role of Smart Cards as a Privacy-Enabling Technology,” Smart Card Alliance white paper, February 2003, available at <http://www.smartcardalliance.org>

“Secure Identification Systems: Building a Chain of Trust,” Smart Card Alliance report, March 2004, available at <http://www.smartcardalliance.org>

“Securing the Enterprise,” Albert Leung, Group Marketing Manager, Java Card Technology, Sun Microsystems, Smart Card Alliance Annual Conference presentation, October 16, 2003

Smart Card Alliance Smart Card Reader Catalog, available at http://www.smartcardalliance.org/industry_info/catalog.cfm

“Smart Card Case Studies and Implementation Profiles,” Smart Card Alliance report, December 2003, available at <http://www.smartcardalliance.org>

“Smart Card Deployment at Microsoft,” Microsoft white paper, March 11, 2004, available at <http://www.microsoft.com/technet/itsolutions/msit/security/smartcrd.mspx>

USB Implementer’s Forum, <http://www.usb.org>

“Using Smart Cards for Secure Physical Access,” Smart Card Alliance report, July 2003, available at <http://www.smartcardalliance.org>

Reconocimientos de la Publicación

Este informe fue desarrollado por la Smart Card Alliance para discutir sobre los resultados con autenticación individual para acceso lógico y para definir los beneficios que la tecnología de tarjetas inteligentes provee. La publicación de este documento por la Smart Card Alliance no implica el endoso por parte ninguna organización miembro de la Alianza.

La Smart Card Alliance desea agradecer a los miembros del Grupo de Trabajo de Identificación Personal Segura por sus comentarios y contribuciones. Se involucraron en el desarrollo de este informe participantes de 22 organizaciones, tanto públicas como privadas, incluyendo: ActivCard, AOS-Hagenuk, Axalto, CardLogix, Datakey, Gemplus, Honeywell Access Systems (OmniTek), IBM, Identix, Litronic/SAFLink, Lockheed Martin, MartSoft Corporation, Northrop Grumman Information Technology, OTI America, SCM Microsystems, Smart Commerce, Inc., Sun Microsystems, U.S. Department of Defense, VeriFone, VeriSign, Visa USA, XTec, Incorporated.

Agradecimiento especial a las personas que escribieron, revisaron y/o editaron este informe.

David Asay, IBM

David Berman, VeriSign

Kirk Brafford, Litronic/SAFLink

Yuh-Ning Chen, Ph.D., MartSoft Corporation

Michael Davis, Honeywell Access Systems (OmniTek)

Patrice Erickson, Identix

Nick Hislop, Gemplus

Mansour Karimzadeh, Smart Commerce, Inc.

Colleen Kulhanek, Datakey

Kevin Kozlowski, XTec Inc.

Albert Leung, Sun Microsystems

Mark McGovern, Lockheed Martin

John McKeon, IBM

Cathy Medich, Consultant & Task Force Chair

Yahya Mehdizadeh, Axalto

Bob Merkert, SCM Microsystems

Neville Pattinson, Axalto

Dwayne Pfeiffer, Northrop Grumman Information Technology

Bruce Ross, CardLogix

Nick Stoner, Lockheed Martin

Shawn Willden, IBM

Derecho de Autor (Copyright Notice)

Copyright 2004 Smart Card Alliance, Inc. Todos los derechos reservados

Marcas Registradas (Trademark Notices)

Todas las marcas registradas, son de propiedad de sus respectivos dueños:

Apple, Macintosh y Mac OS son marcas registradas de Apple Computer, Inc., registrada en los U.S. y/u otras ciudades.

BSD es una marca registrada de Berkeley Software Design, Inc.

Cosmologic es una marca registrada de Oberthur.

Entelligence es una marca registrada de Entrust.

IRIX es una marca registrada de Silicon Graphics, Inc., en los U.S. y/u otras ciudades.

Mediametric es una marca registrada de XTec, Incorporated.

Microsoft, Windows, Windows NT, Win32, Outlook son marcas registradas o marcas de Microsoft Corporation en los U.S. y/u otras ciudades

MIFARE es una marca registrada de Philips Semiconductors.

Netscape es una marca registrada de Netscape Communications.

OS/2 es una marca registrada de IBM Corporation.

SecurID es una marca registrada de RSA Security Inc. en los U.S. y/u otras ciudades.

S/KEY es una marca registrada de Bell Communications Research.

SmarTrip es una marca registrada de WMATA.

Sun, Sun Microsystems, Sun Ray, Java, Java Card and Solaris es una marca registrada o marcas registradas de Sun Microsystems, Inc. en los U.S. y otras ciudades.

Unix es una marca registrada de The Open Group.

Apéndice A: Definición de Términos y Siglas

API

Aplicación del programa de interfase. Formal especificación de una colección de procedimientos y funciones disponibles para un programador de aplicaciones. Estas especificaciones describen los comandos disponibles, argumentos (o parámetros) que pueden ser proveídos cuando un comando es llamado y el tipo de valor del entorno cuando la ejecución del comando es completada.

Claves Asimétrica

Dos claves relacionadas, una clave pública y una clave privada, que son utilizadas para realizar operaciones complementarias, tales como encriptación y desencriptación o generación de firmas y verificación de firmas.

Biométrico(a)

Tecnologías biométricas son definidas como métodos automatizados de identificación y o autenticación de identidad de una persona viva basado en características fisiológicas o

Patrones Biométricos

Registros almacenados de imágenes biométricas de un individuo. Generalmente, escaneadas de atributos biométricos individuales trasladados a través de un algoritmo específico dentro de un registro digital que puede ser almacenado en una base de datos o en una tarjeta inteligente. Los registros digital formateados usados para almacenar los atributos biométricos generalmente se refieren a patrones biométricos.

BSD

Una versión de Unix desarrollada por la Universidad de California, Berkeley.

Autoridad de Certificación o Certificate authority (CA)

Un componente de la infraestructura de clave Pública que es responsable de emitir y revocar certificados digitales. Los certificados digitales pueden contener claves públicas o información pertinente a la clave pública

Verificador de suma (Checksum)

Valores computarizados que dependen de los contenidos de los mensajes. EL verificador de suma es transmitido con el mensaje. La parte que recibe puede recomputarizar la verificación para verificar que el mensaje no fue interrumpido durante la transmisión.

Texto no cifrado o Cleartext

Datos o información que no está cifrada.

Chip

Componente electrónico que realiza funciones lógicas de procesamiento y o memoria.

Tarjetas inteligentes de Contacto

Una tarjeta inteligente que se conecta al dispositivo de lectura a través de contacto físico directo entre el chip de la tarjeta inteligente y el lector de la tarjeta inteligente (ver ISO/IEC 7816).

Tarjetas inteligentes sin Contacto

Una tarjeta inteligente cuyo chip se comunica con el lector usando radio frecuencia y no requiere contacto físico con el lector de la tarjeta.

DES

Estándar de Datos Cifrados.

DSA

Firma Digital Algoritmo.

Tarjeta interfase dual

Tarjetas inteligentes que tiene un solo chip de tarjeta con dos interfaces- interfase de contacto y sin contacto -usando una memoria compartida y recursos del chip.

EMV

Europay MasterCard Visa .Especificaciones desarrolladas por Europay, MasterCard, y Visa que definen el conjunto o requerimientos para una interoperabilidad entre los chips de tarjeta de pago y las terminales.

Gramm-Leach-Bliley

La Financial Services Modernization Act of 1999 (también conocida como el Acta de Gramm-Leach-Bliley), facilita la afinidad entre bancos, firmas de seguridad y compañías de seguro. El acta incluye provisiones para proteger la información financiera personal del consumidor guardadas por instituciones financieras.

GSC-IS

Government Smart Card Interoperability Specification. El GSC-IS fue definido para brindar la habilidad de desarrollar tarjetas inteligentes de identificación \segura que puedan operar a través de múltiples agencias del gobierno o entre los gobiernos Federal, Estatal y Local y ofrece soluciones a varios problemas de interoperabilidad asociados con la implementación de tecnología de tarjetas inteligentes de contacto

GSM

Global System for Mobile Communications

Hash algorithm

Software de algoritmo que computa al valor (hash) de un dato de una unidad en particular de una forma que permita la detección intencional/no autorizada o no autorizada/accidental de datos modificados por el receptor.

HIPAA

Health Insurance Portability and Accountability Act of 1996. HIPAA fue pasada para proteger el cubrimiento del seguro de salud para trabajadores y sus familiares y para animar el desarrollo de un sistema de información de salud estableciendo estándares y requerimientos para la transmisión electrónica segura de ciertas informaciones de salud. La HIPAA exige que el diseño y la implementación de los sistemas eléctricos garanticen la privacidad y la seguridad de la información obtenida del paciente como parte de la provisión de cuidados médicos.

Tarjeta Híbrida (Hybrid card)

Es una tarjeta de identificación que tiene dos chips de tarjetas inteligentes- tanto chip de contacto como sin contacto- que no están interconectados.

ICAO MRTD

International Civil Aviation Organization Machine Readable Travel Documents. ICAO establece los estándares internacionales para documentación de aviación. Una MRTD es un documento internacional de aviación (ejemplo, pasaporte o visa) contiene ojos y una máquina con datos disponibles .ICAO Document 9303 es el estándar internacional para MRTDs.

Circuito Integrado

Ver chip.

ISO

International Organization for Standardization.

ISO/IEC 14443

Estándar ISO/IEC para “Tarjetas de Identificación – Tarjetas con Circuitos Integrados sin contacto- Tarjetas de Proximidad”.

ISO/IEC 7816

Estándar ISO/IEC para tarjetas circuito integrado de contacto.

Acceso Lógico

Es el acceso a recursos en línea (por ejemplo, redes, archivos, computadoras, bases de datos).

Man-in-the-middle attack

Un atacante o un protocolo de autenticación en el cual el atacante es colocado entre la autenticación individual buscada y el sistema de verificación de autenticación. En este ataque el atacante atenta con interceptar y alterar los datos de viaje entre las partes.

MCU

Ver microcontrolador

MD5

Uno de los más populares algoritmos de hashing, desarrollado por el Profesor Ronald L. Rivestof MIT, el cual produce un hash de 128-bit desde cualquier entrada.

Microcontrolador (MCU)

Un chip de computador altamente integrado que contiene todos los componentes comprendidos en un controlador. Típicamente esto incluye CPU, RAM, alguna forma de ROM, puertos I/O y marcadores de tiempo. A diferencia de un computador de uso general un microcontrolador está diseñado para operar en un ambiente restringido.

Microsoft Crypto API

Red de seguridad de Microsoft que desarrolla usos para implementar funciones de seguridad para aplicaciones que corren en Microsoft Windows.

Tarjeta de Aplicación Múltiple

Es una identificación de tarjetas inteligentes que ejecuta múltiples aplicaciones- por ejemplo, acceso físico, acceso lógico, almacenamiento de datos y bolsa electrónica (electronic purse)- usando una única tarjeta.

NIST

National Institute of Standards and Technology.

No rechazo (Non-repudiation)

Es la habilidad de asegurar y tener la evidencia de que una acción específica ocurrió en una transacción electrónica (por ejemplo, que el creador de un mensaje no puede negar haber mandado un mensaje o que un participante en una transacción no puede negar la autenticidad de su firma).

NTFS

New Technology File System. Sistema de archivos propietarios de Windows

OTP

Contraseña de un solo uso son contraseñas que son utilizadas una sola vez y luego se descartan. Cada vez usuario se autentica al sistema, con una

contraseña diferente, después de lo cual la contraseña no tiene validez. La contraseña es computarizada quizás por el software en el logo de la computadora o en el hardware OTP, fichas en posesión del usuario que es coordinado a través de un sistema confiable.

PC

Computador personal

PC/SC

Computador personal/Tarjetas inteligentes. Las especificaciones PC/SC definen como integrar los lectores de tarjetas inteligentes con el medio computacional y como permitir múltiples aplicaciones para compartir dispositivos de tarjetas inteligentes.

PCSC Lite

Computador Personal/Smart Card Lite. PCSC Lite es un software con recurso abierto que implementa la especificación de PC/SC para Linux.

PGP/MIME

Pretty Good Privacy/Multipurpose Internet Mail Extensions. Protocolo para cambio de firma digitalizada y/o correo electrónico cifrado.

Acceso Físico

Es el acceso a establecimientos físicos (por ejemplo, edificios, cuartos, aeropuertos, depósito).

PIN

Personal Identification Number. (Número de identificación personal). Es un Código numérico que está asociado con una tarjeta de identificación y que añade un segundo factor de autenticación al proceso de verificación de identidad.

Public (asymmetric) key cryptography

El tipo de criptografía que es usado por pares matemáticos relaciona las claves criptográficas. Las claves públicas pueden ser hechas disponibles para cualquiera y pueden cifrar información o verificar firmas digitales. La clave privada es mantenida en secreto por su portador y puede descriptar información o generar firma digital.

PKI

Public Key Infrastructure. (Infraestructura de clave Pública).

La arquitectura de la organización, técnicas, prácticas y procedimientos que colectivamente respaldan la implementación y operación de las certificaciones basadas en los sistemas criptográficos de claves públicas. Además, la infraestructura de comunicación permite a los usuarios cambiar dinero o datos mediante el Internet en un ambiente seguro. Hay cuatro componentes básicos de PKI: Certificate Authority (CA) responsable de emitir y verificar los certificados digitales, el registro de autoridad (RA) el cual provee la verificación del CA para garantizar los certificados digitales, de uno o múltiples directorios para sostener los certificados (con claves públicas) y un sistema para administración de los certificados. También incluyen en un PKI los certificados de Políticas y acuerdos entre partes que documenten las reglas de la operación, políticas de procedimiento y la responsabilidad de las partes que operan sin PKI

PKCS #11

Estándar Criptográfico de Clave Pública #11. Este estándar define la interfase para operaciones criptográficas con fichas hardware..

Private key

La parte secreta de un par de clave asimétrica que es usada para crear firmas digitales y depender algunas veces de algoritmos, para describir mensajes o cifrar archivos (para confidencialidad) con la correspondiente clave pública.

Clave Pública

La parte pública de un par de clave asimétrica que es usado para verificar firmas creadas con sus correspondientes claves privadas. Dependiendo algunas veces de algoritmos, para describir mensajes o cifrar archivos (para confidencialidad) con la correspondiente clave privada.

Certificado de Clave Pública

Documento digital que es emitido y firmado digitalmente por clave privada de CA y que contiene el nombre del suscriptor de clave pública.

RF

Radio frecuencia.

RFID

Radio Frequency Identification. (Identificación de Radio Frecuencia)

RSA

Refiere a tecnología de encriptación de claves públicas/privadas que son usadas en algoritmos desarrolladas por Ron Rivest, Adi Shamir, y Leonard Adleman y que es propiedad bajo licencia de RSA Security.

Sarbanes-Oxley

El Sarbanes-Oxley Act of 2002, la cual introduce cambios en las regulaciones que aplican práctica financiera y gobernabilidad corporativa para compañías públicas. El acto de introducir nuevas reglas que pretenden "proteger a los inversionistas para incrementar la exactitud y confianza de lo manifestado para hacer mas persuasivas las leyes de seguridad.

Secure Hash Algorithm (SHA)

Uno de los hashing algoritmos más populares, diseñados para ser usados con la Digital Signature Standard por el National Institute of Standards and Technology (NIST) y el National Security Agency (NSA). SHA-1 produce un hash de 160-bit.

Seed

Una secuencia de bits que son usados en una criptografía algorítmica como conector para generar otro, mayores secuencias de bit pseudo aleatorias.

SIM

Subscriber Identity Module. SIM es una tarjeta inteligente que incluye en GSM (Global System for Mobile Communications) teléfonos móviles. SIMs son configurados con información esencial autenticar el GSM, que permite a un teléfono recibir servicio aunque el teléfono no tenga cobertura por una red.

Tarjetas inteligentes

Una tarjeta inteligente incluye un chip que puede ser un microcontrolador con memoria interna o un chip de memoria solamente. La tarjeta se conecta a un lector con contacto físico directo o con interfase electromagnética remota sin contacto. Con un microcontrolador las tarjetas inteligentes tienen la habilidad única de almacenar grandes cantidades de datos, ejecutar sus propias funciones en la tarjeta (por ejemplo, encriptación y firmas digitales) e interactuar inteligentemente con el lector de tarjetas inteligentes

Tarjeta de Identificación Inteligente (Smart ID card)

Una tarjeta de identificación que es una tarjeta inteligente.

S/MIME

Secure Multipurpose Internet Mail Extensions .Protocolo para cambiar firmas digitales y/o correo electrónico cifrado.

Sniffing

El acto de auditar o mirar tráfico de la red computarizada. Hackers pueden utilizar programas de olfatear para capturar datos que se están comunicando a través de la red.

SSL

Secure Sockets Layer.SSL es un protocolo usado para transmitir información en el Internet de forma cifrada. SSL también asegura que la información transmitida está solamente accesible por el servidor que es el que intenta recibir la información.

Autenticación Sólida

El uso de dos o tres factores de autenticación para proveer una identidad individual. Los factores incluirán alguna combinación de algo que usted sabe (una contraseña o número de identificación personal que solo usted conoce) algo que usted tiene (un objeto físico o ficha en su posesión) y algo que usted es (una cualidad física única o conducta que los diferencie de los otros individuos)

Claves Simétricas

Claves que son utilizadas para claves criptográficas simétricas (secreta).En un sistema criptográfico simétrico, la misma clave secreta es usada para realizar tanto la operación criptográfica como su inversa (por ejemplo cifrar y descifrar o para crear un mensaje codificado de autenticación para verificar el código).

TLS

Transport Layer Security protocol. El protocolo TLS provee comunicaciones seguras mediante el Internet.

Ficha (Token)

Un dispositivo hardware de seguridad que contiene las credenciales de identidad del usuario y las claves requeridas para usar la credencial, autenticación individual, y/o realizar transacciones seguras. Esto puede incluir claves privadas individuales, certificados de claves públicas, y de manera opcional otros certificados.

3DES

Triple DES.

USB

Bus de Serie Universal.

VPN

Red Virtual Privada.