



Uso de Tarjetas Inteligentes para un Control de Acceso Físico Seguro

Informe de la Smart Card Alliance Latin America (SCALA)

*Fecha de Publicación: julio 2003
Número de Publicación: ID-03003
Fecha de Modificación: octubre 2006*

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

Acerca de la Smart Card Alliance Latin America (SCALA). (Alianza de Tarjetas Inteligentes para América Latina)

La Smart Card Alliance Latin America (SCALA) es la asociación sin fines de lucro, líder, no partidaria con múltiples miembros de la industria trabajando para acelerar la amplia aceptación 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; la Alianza mantiene a sus miembros conectados con los líderes de la industria y el pensamiento innovador. La Alianza es la voz unificada de la industria de tarjetas inteligentes, liderizando 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

Copyright 2003 Smart Card Alliance, Inc. Todos los derechos reservados. La reproducción o distribución de está publicación de cualquiera forma, queda prohibido sin el permiso previo de la Smart Card Alliance. La Alianza ha hecho el mejor de sus esfuerzos para asegurar, sin embargo, no puede garantizar, que la información descrita en esté 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 esté 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) claves de la Smart Card Alliance en su web site para información sobre los derechos de reproducción y distribución para miembros

Miembros de la Smart Card Alliance: Los miembros podrán acceder a todos los informes sin costo alguno. Favor de Consultar la sección de (login) claves de la Smart Card Alliance en su web site para información sobre los derechos de reproducción y distribución para miembros.

Tabla de Contenido

Sobre la Smart Card Alliance Latin America (SCALA).....	2
Tabla de Contenido.....	3
Resumen Ejecutivo.....	5
Introducción.....	7
Panorámica del Sistema de Control de Acceso Físico.....	9
Componentes del Sistema de Control de Acceso.....	9
Proceso del Control de Acceso.....	11
Credencial de Identidad	12
Lector de Puerta de acceso	13
Panel de Control.....	14
Servidor del Control de Acceso.....	14
Formatos de Datos del Sistema de Control de Acceso	15
Radio de Acción Operacional.....	15
Consideraciones de Seguridad.....	16
Seguridad de la Tarjeta	15
Protección de Datos	16
Autenticación de la tarjeta y de los datos.....	17
Comunicación entre la tarjeta y el lector de tarjeta.....	18
Comunicación entre el lector de tarjeta y el panel de control ...	18
Implicaciones de Tendencias Recientes en la Arquitectura del Sistema .	19
La Tarjeta de Identificación Inteligente: El Papel de las Tarjetas Inteligentes en Los Sistemas de Acceso Físico Seguro.....	19
Consideraciones Claves para la Implementación de Sistema de Identificación Acceso Físico Seguro	23
Tecnologías Candidatas de Tarjetas Inteligentes.....	23
Tecnología de Tarjeta Inteligente sin Contacto	26
Tecnología de Tarjeta Inteligente De Contacto.....	26
Requerimientos y aspectos de interfase con el usuario	26
Facilidad de Uso Vs. Desempeño y Seguridad.....	27
Impacto de Americanos Descapacitados.....	27
Consideraciones a Nivel del Sistema.....	27
Sistemas Centralizados Vs. Distribuidos.....	28
Sistemas Abiertos Vs. Propietarios.....	28
Interoperabilidad.....	28
Administración del Ciclo de Vida.....	31

Tarjetas de Acceso de Aplicación Unica.....	31
Tarjetas de Acceso de Aplicación Múltiple.....	31
Costos y Beneficios.....	32
Tendencias del Mercado.....	33
Gubernamental.....	34
Comercial.....	35
Tecnologías Emergentes.....	35
Migración Hacia un Sistema de Identificación de Acceso Físico Basado en Tarjetas Inteligentes.....	37
Consideraciones Claves para la Migración.....	37
Tarjetas de Tecnología Múltiples.....	39
Tarjetas de Aplicaciones Múltiples	39
Lectores de Tecnología Múltiples	39
Cableado del Sistema de Control de Acceso.....	40
Formatos de Datos para Control de Acceso... ..	40
Nuevas Aplicaciones Permitidas por los Sistemas de Tarjetas Inteligentes	
Aplicaciones de control de acceso lógico.....	42
Protección por medio de un PIN/ clave.....	43
Respaldo PKI.....	43
Respaldo de llave Simétrica (claves de un solo uso).....	44
Respaldo Biométrico.....	44
Respaldo de Pagos.....	44
Almacenaje Seguro de Datos.....	46
Conclusión.....	47
Referencias y Recursos.....	49
Reconocimientos.....	50
Apéndice A: Definición de Términos y Siglas.....	52

RESUMEN EJECUTIVO

Hace sentido usar Tarjetas Inteligentes para controlar el acceso físico de forma segura.

Las tarjetas inteligentes están teniendo cada vez más aceptación como la credencial de preferencia para controlar el acceso físico con seguridad. Las tarjetas de identificación inteligentes basadas en estándares pueden ser usadas para fácilmente autenticar la identidad de una persona, determinar el nivel de acceso adecuado y admitir físicamente al portador de la tarjeta a un servicio, a un establecimiento. A través, del uso adecuado de tecnología de tarjetas inteligentes de contacto o sin contacto, en el diseño general de sistemas de acceso físico, los profesionales de seguridad pueden implementar las políticas de seguridad más altas posibles para cualquier situación.

Más de una aplicación de acceso puede ser realizada en una tarjeta única de identificación inteligente, permitiendo a los usuarios tener acceso a recursos físicos y lógicos sin la necesidad de portar múltiples credenciales. La seguridad puede cambiar dinámicamente los derechos de acceso, dependiendo del nivel de amenaza percibido, la hora del día o cualquier otro parámetro que sea adecuado. La Tecnología de Informática (IT) puede registrar y actualizar privilegios desde una localización central. Recursos Humanos (HR), puede procesar empleados que entran y que salen rápidamente, dando o retirando todos los derechos de acceso de una sola vez, en una sola transacción. La organización como un todo incurrirá en costos de mantenimiento más bajos.

Flexibilidad y Estándares Maduros son la Marca Registrada de la Tecnología de Tarjetas Inteligentes

El respaldo dado por las tarjetas inteligentes para múltiples aplicaciones, permite a las organizaciones expandir el uso de las tarjetas para proveer a la empresa un sólido caso de negocios. Las tarjetas inteligentes no solo aseguran acceso a los recursos físicos o lógicos, como pueden almacenar datos sobre el portador de la tarjeta, pagar una cuota o tarifa, si fuese requerido, certificar transacciones y rastrear las actividades del portador de la identificación para propósitos de auditoría. Debido a que los componentes que respaldan el sistema pueden ser colocados en red, las bases de datos compartidas y la comunicación entre computadoras; permiten que áreas separadas funcionalmente dentro de una organización puedan intercambiar y coordinar información automáticamente e instantáneamente distribuir información veraz a través de una amplia área geográfica.

La tecnología de tarjetas inteligentes está basada en estándares maduros (de contacto y sin contacto). Las Tarjetas que cumplen con

estos estándares son desarrolladas comercialmente y tienen una presencia establecida en el mercado. Múltiples vendedores son capaces de suplir los componentes basados en estándares, necesarios para implementar sistemas de acceso físico sin contacto, brindando a los compradores equipo interactivo y tecnología a un costo competitivo.

La Implementación debe ser Guiada según los Requerimientos de las Aplicaciones y de la Organización

Las organizaciones deben considerar muchos factores cuando se implementa un nuevo sistema de control de acceso físico, incluyendo: Que requerimientos de interfase de usuario, de desempeño y de seguridad son necesarios; cual es el nivel de integración necesario con otras aplicaciones de la empresa, como implementar una arquitectura del sistema que cumpla con los requerimientos de seguridad de forma costo efectiva; que tecnología debe ser usada para satisfacer los requerimientos de la organización; como será manejado el ciclo de vida de la credencial de identidad; como hará la organización para migrar hacia una nueva tecnología, y al mismo tiempo sacar provecho de los sistemas preexistentes de control de acceso.

Las tarjetas inteligentes son flexibles, brindando un camino para la migración donde los requerimientos de la organización, y no la tecnológica de la tarjeta, son la fuerza motora del proceso. Las tarjetas inteligentes de tecnología múltiple pueden respaldar tecnologías de control de acceso, preexistentes, a la vez que incluyen nueva tecnología de chips de contacto o sin contacto. Cuando se planifica la migración cuidadosamente, las organizaciones pueden implementar nuevas funciones, mientras se acomodan los sistemas preexistentes en la medida en que esto sea requerido.

Sobre Este Informe

Este informe fue desarrollado por la Smart Card Alliance, para brindar un documento base sobre sistemas de identificación de acceso físico basado en tarjetas inteligentes. Este informe da respuesta a preguntas frecuentemente hechas sobre el uso de las tarjetas inteligentes para accesos físico, tales como:

- © ¿Cómo funciona el sistema de control de acceso físico?
- © ¿Que papel juegan las tarjetas inteligentes en un sistema de control de acceso físico?
- © ¿Cuáles son los temas centrales que deben ser considerados cuando se implementa un sistema de control de acceso físico en base a las tarjetas inteligentes?
- © ¿Qué otras aplicaciones pueden ser combinadas con los sistemas de acceso físico basados en tarjetas inteligentes?
- © ¿Cuales son las opciones de migración para organizaciones que están moviéndose hacia sistemas de acceso físico basados en tarjetas inteligentes?

Introducción

El manejo de acceso a recursos esta adquiriendo una importancia cada vez mayor para organizaciones en todas partes del mundo, desde pequeñas compañías hasta grandes empresas corporativas y cuerpos gubernamentales de todos los tamaños. Hasta la organización más neutral ahora reconoce el peligro de fallas en la seguridad

La administración de acceso a recursos significa controlar tanto el acceso físico como el acceso lógico, ya sea como un esfuerzo independiente o a través de un abordaje integrado. El control de acceso físico protege contra robo o usurpación tanto de bienes tangibles como intelectuales. El control de acceso lógico permite a las empresas y organizaciones limitar el acceso a los datos, a las redes y las estaciones de trabajo solamente para aquellos que están autorizados para tener dicho acceso.

Antecedentes

La coordinación de personas y privilegios tradicionalmente ha dependido del uso de una tarjeta de identidad tal como de una licencia de manejar, una tarjeta de biblioteca, una tarjeta de crédito, una tarjeta de membresía, o una tarjeta de identificación del empleado. Tales tarjetas demuestran para una persona (tal como un guardia) o para un dispositivo (tal como un lector electrónico) que el portador tiene ciertos derechos y privilegios. En respuesta a la necesidad de una mayor seguridad, la industria ha desarrollado tecnologías (tales como las cintas magnéticas, códigos de barras y chips de proximidad) que pueden ser incluidos en una tarjeta. La tarjeta puede luego pasarse a través de un lector de cinta magnética, escaneado por un lector de código de barra o presentado a un lector electrónico con una antena de radio frecuencia (RF) para autorización de acceso automático. Un número de identificación personal (PIN) puede ser ingresado en un teclado para adicionar otro factor de autenticación que ayuda a verificar que el portador de la tarjeta es de hecho, el dueño de la tarjeta. Sin embargo, mientras esas tecnologías reducen costos y aumentan la misma conveniencia, ellos no garantizan que el usuario es de hecho la persona autorizada.

Cambios en la fuerza laboral hacen que el problema de identificación y autenticación de individuos se haga cada vez mayor. Los días de una fuerza laboral estable y reconocible básicamente se han terminado. Actualmente, muchas corporaciones están experimentando una rotatividad cada vez mayor de los empleados y tienen dificultad de llenar ciertas asignaciones y por lo tanto frecuentemente usan contratistas externos. Esta situación da como resultado la presencia de personal nuevo no reconocido que tiene acceso a los bienes e información de la corporación. Mientras la rotatividad de empleados generalmente no es un problema mayor para las organizaciones gubernamentales, la rotación de personal y el enorme tamaño y complejidad de tales organizaciones crean una

situación similar con el potencial de que, personas no autorizadas obtengan acceso a recursos.

El escenario está montado para la introducción de sistemas de identificación de acceso basado en una tarjeta de identidad u otra credencial de identidad que incluya inteligencia integrada. Tal credencial podría respaldar múltiples aplicaciones seguras para el procesamiento de información de identificación personal, privilegios y derechos de acceso, así como incluir protección criptográfica de la información. La aparición de credenciales inteligentes dio origen a un modelo completamente nuevo de control de acceso que logra procesamiento rápido, autenticación personal y mitigación de riesgo. Este modelo representa la base para un sistema de identificación segura que resuelve el problema fundamental de control de acceso como asociar de forma veraz a los individuos con sus derechos y privilegios en el local donde la decisión de acceso debe ser tomada. Tal tarjeta de identificación "inteligente" puede incluir una cinta magnética, una cinta Wiegand, un código de barra, un dispositivo de radio frecuencia (RF), un chip de tarjeta inteligente y otras tecnologías de seguridad.

Sistemas de Control de Acceso Físico Basados en Tarjetas Inteligentes

El sistema de control de acceso físico es una red coordinada de tarjetas de identificación, lectores electrónicos, bases de datos especializadas, software y computadoras diseñadas para monitorear y controlar el tráfico a través de puntos de acceso.

Los sistemas de control de acceso físico basados en tarjetas inteligentes son una herramienta de seguridad poderosa, eficiente para proteger los bienes de una empresa. A cada empleado o contratista se le emite una tarjeta de identidad inteligente que muestra la información de la empresa y diseños impresos, tanto para limitar la posibilidad de falsificación como para identificar que la tarjeta es oficial. Generalmente, la tarjeta muestra una foto de su portador. Cada tarjeta almacena información protegida sobre la persona y sobre los privilegios de esta persona. Cuando la persona se registra inicialmente y acepta la tarjeta, estos privilegios son diseminados (populated) a través de todo el sistema de forma veraz y segura (Si tales privilegios cambian, la nueva información puede ser inmediatamente actualizada de manera segura a través de la red). Cuando la tarjeta es colocada dentro o cerca de un lector electrónico, el acceso se brinda o se niega de forma segura y precisa a todos los espacios adecuados (por ejemplo, un campo, un garaje de estacionamientos, un edificio o una oficina). Cuando un empleado deja la organización, todos los privilegios de acceso físico son removidos de una sola vez. Cualquier tentativa futura por esta persona de reingresar al establecimiento usando una tarjeta expirada

o revocada, puede ser negada y este hecho registrado automáticamente.

Tanto las empresas privadas como las agencias de gobierno están implementando cada vez más los sistemas de control de acceso basados en tarjetas inteligentes. En el Apéndice A se incluyen algunos sumarios de la implementación de tarjetas inteligentes en: Sun Microsystems, Microsoft, American Express y el Departamento de Estado de los Estados Unidos. También se incluye en el Apéndice la descripciones de programa de tarjetas inteligentes planificadas en el U.S. Department of Homeland Security, National Aeronautics and Space Administration (NASA) Transportation Security Administration (TSA).

Oportunidades Adicionales

Idealmente, un sistema de control de acceso brinda protección tanto para el acceso físico como lógico de forma simultánea. La credencial usada para el acceso físico puede también permitir acceso a la red de computadoras e ir a una infraestructura de clave pública (PKI –Public Key Infrastructure) (incluyendo el uso de acceso remoto seguro, correo electrónico seguro, firma digital y red privada virtual segura (VPN- Virtual Privated Network)). La meta de protección simultánea puede ser alcanzada por la mezcla o por compartir bases de datos seguras dedicadas a cada tipo de aplicación, permitiendo tanto un control administrativo centralizado como el análisis de cualquier tentativa de acceso no autorizada. Al combinarse la información de monitoreo tanto del sistema físico como lógico, permitirá que las políticas de seguridad puedan ser cumplidas e investigadas a todos los niveles. La información recolectada puede ser invaluable en el análisis de riesgo del conjunto de la empresa.

La adopción de sistemas de control de acceso basados en tarjetas inteligentes puede también resultar en otras ventajas para la organización, incluyendo:

- Eliminación o reducción de la necesidad de múltiples tarjetas, PINs, o códigos de acceso.
- Apuntalar sistemas preexistentes, de una forma costo –eficiente, incluyendo la re-utilización de algunos componentes del sistema de acceso físico, mientras se logra un aumento significativo en seguridad
- Eliminación de la necesidad de reemplazar las tarjetas cuando los derechos o privilegios cambian.
- Administración centralizada, permitiendo a la organización mantener o aumentar la seguridad mientras se ahorra tiempo, logrando una distribución más completa de la información, manejando cambios globales para privilegios de acceso a partir de un único punto y reduciendo las complejidades involucradas en la sincronización de sistemas múltiples.

-
- Flexibilidad para respaldar múltiples funciones dentro de la organización, (por ejemplo seguridad de los establecimientos e Informática) para manejar y controlar aplicaciones separadas en una única tarjeta de identidad inteligente de aplicación múltiple.

Este informe fue diseñado para dar una panorámica educativa a personas que toman decisiones y planificadores de seguridad, en el se describe la arquitectura de un sistema de acceso físico, ofrece orientación sobre consideraciones claves de implementación, describe tecnologías de tarjetas inteligente usadas para acceso físico y lógico, discute consideraciones de migración al moverse de sistemas de acceso físico preexistentes hacia sistemas basados en tarjetas inteligentes e ilustra otras aplicaciones que pueden ser combinadas con sistemas de acceso físico seguro basados en tarjetas inteligentes.

Visión General del Sistema de Control Acceso Físico

Para el usuario, un sistema de control de acceso está compuesto de tres elementos:

- Una tarjeta o ficha (una credencial de identidad) que se presenta al lector de la puerta de acceso.
- Un lector de puerta de acceso que indica si la tarjeta es válida y se autoriza la entrada.
- Una puerta de acceso o portón, que es destrabado cuando se autoriza la entrada.

Detrás de la escena existe una red compleja de datos, computadoras y software que incorporan una funcionalidad robusta de seguridad. Esta sección describe la operación y componentes de un sistema típico de control de acceso físico basado en tarjetas inteligentes. Él brinda un contexto para entender como tecnologías de tarjetas inteligentes de contacto y sin contacto son usadas en una aplicación de control de acceso.

Componentes del Sistema de Control Acceso

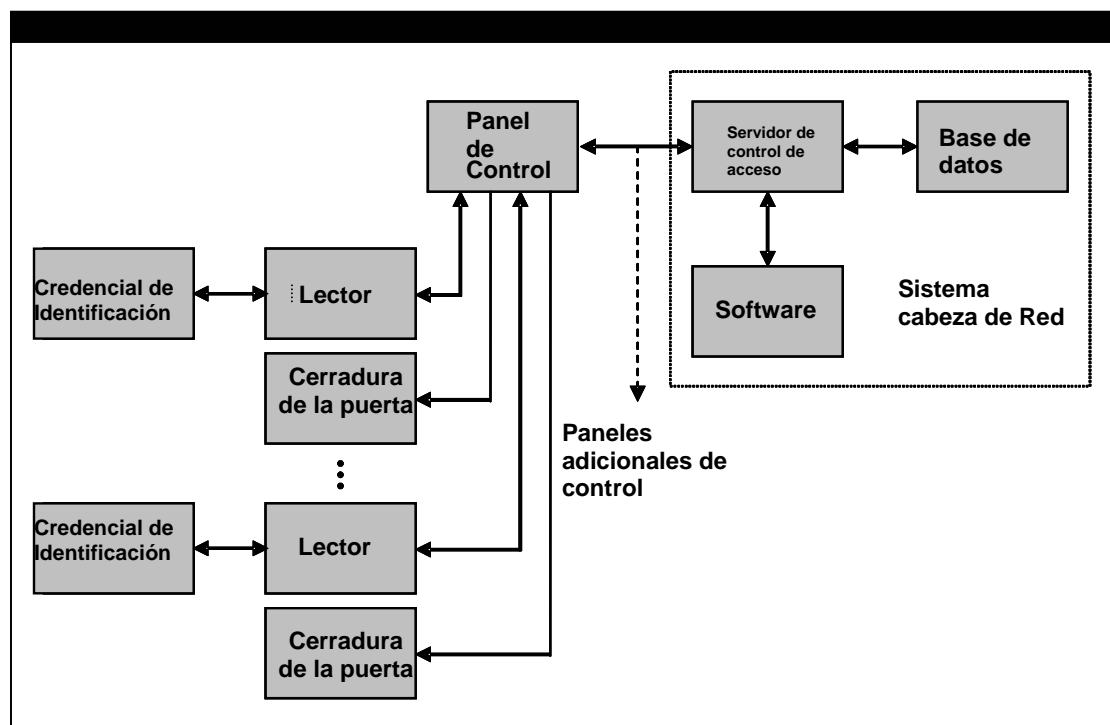
Un sistema de control acceso típico está compuesto de los siguientes componentes.

- Una credencial de identificación (tarjeta inteligente).
- Un lector de puerta de acceso (lector de tarjeta inteligente¹))
- Cerradura de Puerta
- Panel de Control
- Servidor de control de acceso
- Software
- Base de Datos

¹Los “ Lectores” de tarjetas inteligentes pueden tanto leer como escribir en la tarjeta inteligente.

La figura 1 ilustra como estos componentes básicos están interconectados. Cada componente será descrito en las siguientes secciones.

Figura 1: Esquema de un Sistema de Control de Acceso



Proceso de Control de Acceso

Los procesos de control de acceso empiezan cuando un usuario presenta la credencial² (típicamente la insignia o identificación de tarjeta inteligente del empleado) al lector, que normalmente está montado próximo a la puerta o portal de entrada. El lector extrae los datos de la tarjeta, los procesa y los envía al panel de control.

En primera instancia el panel de control valida el lector y luego acepta los datos transmitidos por el lector. Lo que ocurre luego depende si el sistema es centralizado o distribuido.

En un sistema centralizado, el panel de control transmite los datos al servidor de control de acceso. El servidor de control de acceso compara los datos recibidos de la tarjeta con la información sobre el

² Este informe utiliza el término “credencial” para referirse a la identificación general del dispositivo (tanto el dispositivo físico como los datos que él porta). Este es comúnmente referido como “la ficha de identificación” en el sistema de control de acceso físico.

usuario que está almacenado en la base de datos. El programa de control de acceso determina los privilegios de acceso del usuario y su autorización, la hora, la fecha y la puerta a la que se va a ingresar y cualquier otra información que la compañía pueda requerir para asegurar su seguridad. Cuando se autoriza el acceso, el servidor de control de acceso envía una señal al panel de control para abrir la puerta: el panel de control envía dos señales, una a la cerradura de la puerta correspondiente, que abre la puerta y una al lector de la puerta, que emite un sonido audible u otro tipo de señal que indica al usuario que puede entrar.

En un sistema distribuido, el panel de control permite o niega la entrada. El servidor de control de acceso periódicamente provee datos al panel de control, que habilita al software del panel de control a determinar si el usuario está autorizado o no para tener acceso. El panel de control, entonces, realiza las funciones del servidor de control de acceso descrito arriba y toma la decisión de permitir o negar la entrada. El habilitar el panel de control para realizar la función de decisión tiene la ventaja de requerir menor comunicación entre los paneles de control y el servidor de control de acceso central, mejorando el desempeño y la confiabilidad del sistema como un todo.

Si una función biométrica o un PIN se incorpora al sistema, el lector típicamente autentica estos datos. La validez puede ser determinada por el lector o desde dentro de la misma tarjeta inteligente al comparar el dato con un patrón biométrico o un PIN almacenado en la tarjeta. (En algunos casos los datos biométricos pueden ser enviados al panel de control para su procesamiento). Si la información adicional es válida, el lector envía el número de identificación de la credencial al panel de control. Si la información no es válida, entonces el lector de la tarjeta indica que la entrada es negada.

La respuesta a una tarjeta inválida es definida por la política y procedimiento de seguridad de la compañía. El servidor de control de acceso o panel de control pueden ignorar el dato y no enviar un código para abrir el controlador o la cerradura de la puerta. Él puede enviar una señal para que el lector emita un sonido diferente, para indicar que el acceso fue negado. Él podría notificar y activar otro sistema de seguridad (por ejemplo circuito cerrado de televisión, alarmas), indicando que una tarjeta no autorizada está siendo presentada al sistema.

Cada componente de un sistema de control de acceso en este proceso se describe con mayor detalle abajo.

La Credencial de Identificación

Una amplia gama de tecnología de identificación está actualmente siendo usado para control de acceso: cintas magnéticas, cintas

Wiegand, Bariun Ferrite, tecnología de proximidad de 125KHz³, las tarjetas inteligentes de contacto y sin contacto. Esas tecnologías pueden ser empaquetadas en diferentes formatos- desde un llavero o una insignia del empleado o incluso formas más exóticas, como un reloj de pulso o un anillo. Sin embargo, todas las credenciales operan básicamente de la misma forma: ellos almacenan datos que autentican la credencial y/ o el usuario.

Algunas tecnologías de credencial son solamente para lectura. La información está registrada permanentemente en la credencial, y cuando la credencial se presenta al lector la información es enviada al sistema. Ese tipo de credencial solo valida que la información misma es autentica. Pero no confirma que la persona que está presentando la credencial es la persona autorizada a poseerla, o que la credencial misma es legítima.

La tecnología de tarjeta inteligente de contacto definido, por ISO/IEC 7816 y la tecnología de tarjeta inteligente sin contacto definido, por ISO/IEC 14443 e ISO/IEC 15693, tienen capacidad tanto para leer como escribir y almacenar datos. Las credenciales que usan estas tecnologías son dispositivos inteligentes. Ellos pueden almacenar privilegios, autorizaciones y registros de asistencia. Ellos pueden almacenar los PINs y los patrones biométricos, ofreciendo una capacidad de autenticación de dos o tres factores simultáneamente. La credencial ya no es solo un portador de un número único; pero pasa a ser también, cargador seguro y portátil de datos.

El Lector de la Puerta de Acceso

El lector de la puerta de acceso puede tener una o más interfaces, acomodando algún tipo de combinación tanto de las tarjetas inteligentes de contacto como sin contacto e incluyendo un teclado de PIN y un lector biométrico. Como el lector responde va a depender del tipo de credencial presentada y de la política de seguridad de la organización.

Cuando el lector es usado con una tarjeta inteligente sin contacto, él actúa como un pequeño transmisor y receptor de radio de baja frecuencia, constantemente transmitiendo o un campo de radio frecuencia (RF) o un campo electromagnético que es llamado campo de recepción. Cuando la tarjeta sin contacto está dentro del radio de acción del campo de recepción, la antena interna de la tarjeta convierte la energía del campo en electricidad la cual le provee energía al chip que está en la tarjeta. El chip entonces usa la antena para transmitir los datos al lector.

Cuando el lector es usado con una tarjeta inteligente de contacto, el lector incluye una ranura que contiene un contacto de tarjeta inteligente. La tarjeta y el conector (connector) dentro del lector

³ Tecnología de proximidad de 125KHz es comúnmente referido como un “prox”.

deben hacer contacto (contact) físico.

Los lectores que incluyen un teclado de PIN o un lector biométrico (típicamente una huella digital o un lector geométrico de mano), generalmente se respaldan en una autenticación de dos o tres factores, según sea requerido. Por ejemplo, un establecimiento puede requerir solamente la presentación de una tarjeta sin contacto cuando el riesgo de seguridad es bajo, pero puede pasar a requerir datos biométricos también cuando aumenta el nivel de amenaza. Cuando el riesgo de seguridad es alto, puede ser necesario presentar una tarjeta inteligente de contacto, usar un lector biométrico y el teclado de PIN. Estos lectores de factores múltiples pueden ser usados cuando se desea cambiar los insumos requeridos según la hora del día, el día de la semana o la localización. Los requerimientos para los factores adicionales de autenticación han de ser establecidos por la política de seguridad de la organización.

Cuando el lector ha recibido todos los datos requeridos, él típicamente procesa la información en una de dos formas. O la información es enviada inmediatamente al panel de control o el lector analiza los datos antes de enviarlos al panel de control. Ambos métodos son ampliamente utilizados, cada uno tiene sus ventajas y desventajas.

Los lectores más sencillos envían los datos directamente al panel de control. Esos lectores no hacen nada para evaluar los datos o determinar la legitimidad de la credencial. Esos lectores son típicamente lectores de un solo factor y son genéricos, así que pueden ser almacenados en inventarios y fácilmente adicionados o intercambiados en un sistema de control de acceso.

Los lectores que analizan los datos deben estar integrados en el sistema de control de acceso. O sea, ellos deben interpretar y manipular la información enviada por la tarjeta y entonces transmitir los datos en un formato que pueda ser usado por el panel de control. Tal sistema puede ofrecer un nivel incrementado de seguridad. El lector puede determinar la legitimidad de la tarjeta (y la tarjeta puede determinar la legitimidad del lector) comparar los datos biométricos o la entrada de un PIN y manipular los datos de la credencial ya que lo que el lector envía al panel de control no es lo mismo que fue leído de la tarjeta. El proceso de autenticación de la tarjeta al lector y del lector a la tarjeta es llamado autenticación mutua. Autenticación mutua es una de las ventajas del sistema basado en tarjetas inteligentes.

Panel de Control

El panel de control (frecuentemente conocido como el controlador o simplemente el panel) es el punto central de comunicaciones para el sistema de control de acceso. El panel de control típicamente supe energía y establece interfases con múltiples lectores en diferentes puntos de acceso. El panel o controlador conecta con la cerradura electromecánica de la puerta de acceso necesario para físicamente

desatracar la puerta o el mecanismo para un portón de entrada (tal como un sistema rotatorio o un portón de estacionamiento o un elevador). El panel puede estar conectado a diferentes alarmas (por ejemplo, sirenas, digitalizadores automáticos, luces). Y finalmente, el panel de control generalmente está conectado a un servidor de control de acceso.

Dependiendo del diseño del sistema, el panel de control puede procesar datos del lector de tarjetas y del servidor de control de acceso y tomar la decisión última sobre autorización o él puede pasar los datos al servidor de control de acceso para que él tome esa decisión. Típicamente, el panel de control toma la decisión de desatracar la puerta, pasa los datos de esa transacción al computador base y envía una señal de desbloquear hacia el lector. Es importante que sea el panel de control (y no el lector) el que genere la señal de desatracar, ya que el panel de control está localizado dentro del establecimiento en un cuarto seguro, mientras el lector de la tarjeta está localizado en un área insegura o abierta.

Finalmente, el panel de control almacena información sobre los formatos de datos. Esa información identifica que porción del flujo de datos recibidos de una tarjeta es usada para tomar decisiones de control de acceso. Tarjetas y lectores con diferentes tecnologías pueden intercambiar datos en diferentes formatos. Sin embargo, el panel de control necesita saber cómo interpretar y procesar estos datos. Por ejemplo, si un lector envía 35 bits de data y el panel de control está diseñado para leer solamente 26 bits, el panel debe rechazar los datos o truncar 9 bits. El formato de los datos controla cómo el panel interpreta los datos recibidos.

El Servidor de Control de Acceso

El sistema de cabeza de red (también conocido como sistema de "back end", sistema huésped "Host system") incluye el servidor de control de acceso, el software y una base de datos. La base de datos contiene información actualizada sobre los derechos de acceso de los usuarios.

En un sistema centralizado, el servidor de control de acceso recibe los datos de la tarjeta del panel de control. El Software correlaciona los datos de la tarjeta con los datos en la base de datos, determina los privilegios de acceso de la persona, e indica si la persona puede o no ser admitida. Por ejemplo, si una persona está autorizada a ingresar a un edificio solamente entre las 8:00 a.m. y 5:00 p.m. y son las 7:45 a.m., esa persona no puede ser admitida. Sin embargo, si son las 8:01 a.m, entonces el computador debe responder al panel de control, indicando que la puerta puede ser abierta.

La mayoría de los sistemas son descentralizados. En un sistema descentralizado, el servidor de control de acceso periódicamente envía información de control de acceso actualizada a los paneles de control y les permite operar independientemente, tomando la decisión

de autorización para las credenciales presentadas basadas en los datos almacenados en el panel.

Las características operacionales en los sistemas centralizados o descentralizados, son determinadas por los requerimientos específicos de implementación de control de acceso de la organización.

Formato de Datos del Sistema de Control de Acceso

El formato de los datos de un sistema de control de acceso es un elemento crítico del diseño. El formato de datos se refiere al patrón de bits (dígitos binarios) que el lector transmite al panel de control. El formato especifica cuantos bits forman el flujo de datos y que representan estos bits. Por ejemplo, los primeros bits pueden representar el código del establecimiento los siguientes bits son un número de identificación de la credencial única, los siguientes pueden ser de paridad y así sucesivamente.

Muchos vendedores de sistemas de control de acceso han desarrollado sus propios formatos, haciendo que la codificación de los vendedores sea única, así como el patrón de dientes de una llave de puerta, los formatos se mantienen en secreto para evitar que una persona o compañía no autorizada puedan duplicar la tarjeta. Los formatos de sistemas de control de acceso instalados pueden ser considerados cuando se definen los requerimientos para la implementación de nuevas tecnologías para sistemas de control de acceso físico.

Radio de Acción Operacional

Una característica importante de la operación del sistema del control acceso es la distancia del lector en la cual la credencial es efectiva (llamado radio de acción operacional). Esta característica puede afectar la percepción final del usuario sobre la conveniencia de utilizar el sistema. Para los sistemas que utilizan las tarjetas inteligentes de contacto, el radio de acción operacional no es un problema; ya que la tarjeta se inserta dentro del lector y el contacto es físico.

El radio de acción operacional es determinado por múltiples factores, incluyendo, tanto las especificaciones del diseño del sistema como el ambiente en el cual el lector es colocado. Entre los factores que afectan el radio de acción operacional se incluyen la forma de la antena, número de vueltas de la antena, el material de la antena, los materiales que se encuentran a su alrededor, la orientación de la credencial en relación con el lector, los parámetros eléctricos del chip, características anti-colisión y la fuerza de campo del lector. Organizaciones gubernamentales (por ejemplo, la FCC, UL y CE) están involucradas en aprobar o especificar los radios de acción de frecuencia o los límites de transmisión de energía. El campo de

acción operacional puede ser incrementado reforzando la antena (por ejemplo, aumentando el número de espirales de la antena, el tamaño de la antena, o la energía transmitida por la antena).

La localización del lector puede afectar el campo de acción operacional de un lector sin contacto. Por ejemplo, la proximidad del lector al metal puede distorsionar el campo de recepción e inclusive bloquearlo de la tarjeta. Si el lector es montado sobre una sólida placa de metal, próximo a una puerta hecha totalmente de metal o puesto dentro de una cajilla de metal (para protegerlo de actos vandálicos), puede que tenga un campo de acción operacional muy corto.

El campo de acción operacional de la credencial de identidad, para muchas tecnologías sin contacto es una decisión crítica de diseño para un sistema de control de acceso físico. El campo de acción operacional adecuado será determinado, como parte de la política de seguridad general de la organización de la arquitectura de seguridad y de sus requerimientos.

Consideraciones de Seguridad

Para mitigar los riesgos contra accesos no autorizados o ataques deliberados, la seguridad de todo el sistema de control de acceso debe ser tomada en cuenta. Eso comienza con el proceso inicial de emisión de las tarjetas, incluye los componentes del sistema (tal como la red, la base de datos, software, cámaras, lectores, tarjetas) los procesos del sistema (por ejemplo los procedimientos para los guardias) y la protección de los datos dentro de los componentes del sistema y durante la transmisión. El diseño del sistema debe considerar que características de seguridad son necesarias para ser implementadas, dado el ambiente del sistema y de la probabilidad real de un ataque.

SEGURIDAD DE LA TARJETA

Las tarjetas inteligentes pueden ayudar a detener la falsificación o impedir la manipulación, con una tarjeta de identificación y prevenir el uso de una tarjeta no autorizada. Las tarjetas inteligentes incluyen una variedad de capacidades de hardware y software que detectan y reaccionan ante intentos de manipulación y pueden contrarrestar posibles ataques, incluyendo: sensores de voltaje, frecuencia; luz y temperatura; filtros de reloj; memoria barajada (scrambled); fuentes constantes de energía, diseños del chip para resistir análisis por inspección visual, micro sondeos o manipulación del chip. Donde las tarjetas inteligentes se han de utilizar para verificación de identidad manual, características de seguridad pueden ser adicionadas al cuerpo de la tarjeta inteligente tales como, fuentes únicas, color de tinta, y arreglos multicolores, micro impresiones, tinta ultravioleta de alta calidad en la frente o en la parte de atrás de la tarjeta, imágenes fantasmas,(una fotografía secundaria del portador en una

localización alternativa de la tarjeta) y hologramas de múltiples planos, incluyendo imágenes tridimensionales⁴.

Cuando son adecuadamente diseñadas e implementadas, las tarjetas inteligentes son casi imposibles de falsificar o duplicar, y los datos en el chip no pueden ser modificados sin una autorización adecuada (por ejemplo, con palabras claves, con autenticación biométrica o con llaves de acceso criptográfico). En la medida que los sistemas de implementación tengan una política de seguridad efectiva e incorporen los servicios de seguridad necesarios, ofrecidos por las tarjetas inteligentes organizaciones y portadores de identidad pueden tener un alto grado de confianza en la integridad de la información de identidad y de su uso autorizado seguro

PROTECCION DE DATOS

Uno de los argumentos más fuertes para el uso sistemas basados en tarjeta inteligentes para control de acceso físico es su capacidad de usar mecanismos para mezclar datos (data Scrambling) o criptografiar para proteger la información tanto en el chip como durante la transmisión. La seguridad y confiabilidad de la información requerida para la identificación de una persona y sus derechos y privilegios es clave para el éxito del sistema de control de acceso físico.

Las tarjetas inteligentes pueden respaldar algoritmos criptográficos simétricos⁵, que aseguran una protección sustancial y tiempos de procesamiento excelentes. La criptografía de llave simétrica es ampliamente usada para control de acceso físico y utiliza la misma llave para la incryptación y la decriptación, haciendo que sea extremadamente rápido y confiable. Cuando un sistema de control de acceso incluye acceso lógico y privilegios PKI y cuando el tiempo de procesamiento no es problema, los algoritmos criptográficos asimétricos pueden ser usados⁶. Múltiples llaves pueden ser almacenadas en un chip único para tender las necesidades de seguridad para uso en múltiples aplicaciones, brindando de está forma mayor seguridad para la creciente complejidad de los sistemas de hoy.

Autenticación de Tarjeta y Datos

Un sistema de acceso físico seguro debe asegurarse de forma imparcial que tanto la tarjeta de identificación presentada al lector

⁴ Reporte del Gran Jurado a Nivel de Estado: Robo de Identidad en Florida

⁵ Los algoritmos de llave simétrica más comunes actualmente usados DES (Data Standard) Triple DES (ya sea con un formato de dos o tres factores) IDEA (International Data Encryption Standard) AES (Advance Encryption Standard) y MIFAREtm.

⁶ Los algoritmos criptográficos asimétricos utilizados con mayor frecuencia son RSA, ECC (Elliptic Curve Cryptography) y DISA (Digital Signature Algorithm).

como los datos que él contiene son auténticos. En algunos casos, es importante verificar que el es autentico también (como es determinado por la tarjeta) para prevenir terminales falsificadas que puedan extraer los datos.

Aparte del uso de un PIN y/o sistema biométrico para activar la tarjeta o autenticar la persona, las tarjetas inteligentes tienen la capacidad única de ofrecer una autenticación interna, basada en el chip que usa mecanismos criptográficos simétricos o asimétricos, para ofrecer soluciones altamente confiables para demostrar que la tarjeta y los datos son genuinos. Para una autenticación segura de la tarjeta, las tarjetas inteligentes tienen la capacidad única de usar técnicas criptográficas activas para responder a una señal del lector probando que la tarjeta posee una contraseña secreta que puede autenticar la validez de la tarjeta.

Comunicaciones Entre Tarjetas y Lectores de Tarjetas

Como sucede con cualquier proceso que envuelve señales electrónicas, los datos transmitidos entre componentes también pueden ser monitoreados. Esta posibilidad debe ser considerada en el diseño de seguridad del sistema en términos del ambiente (por ejemplo, esta área está bajo observación o podría alguien físicamente insertar otro dispositivo o colocar un dispositivo de monitoreo dentro del radio de acción de la señal) y la probabilidad real de que tal ataque o esfuerzo se realice.

Dependiendo del ambiente y del perfil de riesgos, una organización puede estar preocupada de que la información enviada por una tarjeta de identificación de contacto o sin contacto hacia un lector de tarjeta pueda ser monitoreada, permitiendo que se efectúe una entrada ilegal, si una tarjeta o un dispositivo furtivo pudiese duplicar los datos. Las tarjetas inteligentes respaldan técnicas de encriptación y seguridad estandarizados establecidos al nivel de la industria; que aseguran tanto comunicaciones entre la tarjeta y el lector así como permiten métodos de autenticación entre la tarjeta y el lector.

Las claves de seguridad usadas tanto para encriptar como autenticar son guardadas en fichas seguras (módulos de tarjetas inteligentes) tanto en la tarjeta como en el lector y son altamente resistentes a los ataques.

Comunicaciones entre el Lector de Tarjeta y el Panel de Control

Cuando un lector de tarjetas está localizado en un punto de acceso que no tiene un sistema de cableado físicamente seguro, la organización puede estar preocupada de que un invasor pueda remover el lector de tarjeta de su montura y leer el flujo de datos que este envía al panel de control o colocar una computadora personal u otro dispositivo; en estos alambres y mimetizar la inserción de una tarjeta válida para ganar autorización de acceso. La mayoría de las tarjetas de los lectores de tarjetas actualmente transmiten datos al panel de control usando uno de dos formatos: Wiegand o cinta

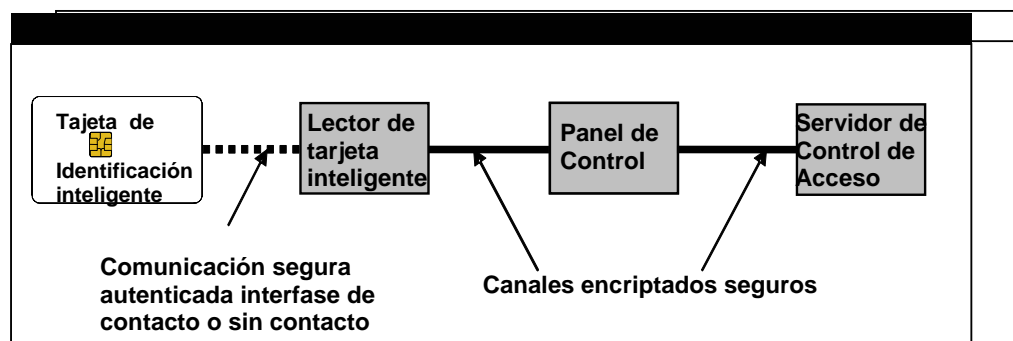
magnética. El formato Wiegand utiliza dos líneas de señales: D0, para transmitir “cero” pulso de datos; D1, para transmitir pulsos de un dato. El formato de cintas magnéticas utiliza dos líneas de señales – una para datos y otra para el reloj. Estas cintas de datos no son consideradas seguras.

El proveer un canal seguro desde la tarjeta hacia el lector y del lector hacia el panel de control, sobrelleva esta amenaza potencial a la seguridad. El proveer canales seguros se neutraliza la mayoría de las amenazas serias porque el lector y la tarjeta son los dos elementos que están expuestos y disponibles físicamente a alguien que desea atacar el sistema.

El canal de comunicación del lector hacia el panel de control puede ser asegurado de una forma similar a la que se usa para un canal seguro entre la tarjeta y el lector. Los datos intercambiados entre los dos dispositivos pueden ser encriptados para mayor seguridad y el lector y el panel pueden ser autenticados durante la transacción.

Debido a que la conexión entre el panel de control y el sistema de control de acceso es interna en un edificio o localizada en un cuarto seguro, normalmente no es tan susceptible a ser atacado. Sin embargo, si así se desea, esta conexión también puede ser asegurada usando las técnicas descritas en esta sección, de forma que todo el sistema tiene un canal de datos seguros de punta a punta. La figura dos ilustra un ejemplo de como un sistema de control de acceso físico basado en tarjetas inteligentes puede brindar una seguridad de punta a punta.

Figura 2: Ejemplo de una seguridad de punta a punta en un sistema de acceso físico basado en tarjetas inteligentes.



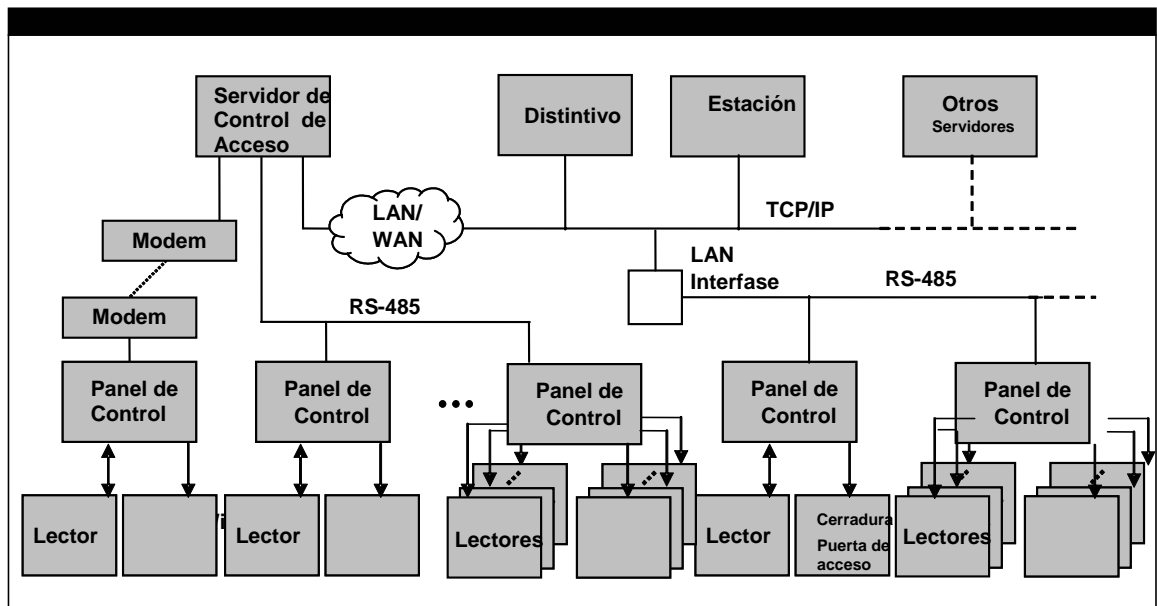
Implicaciones de las Tendencias Recientes en la Arquitectura de Sistemas

Los sistemas de control de acceso físico tradicionalmente han sido controlados por el departamento de seguridad corporativa. Sin embargo, con el advenimiento de sistemas corporativos centralizados, basados en tecnología de internet y de TCP/IP, los sistemas de control de acceso han evolucionado a sistemas de red

que combinan muchas funciones e involucran múltiples departamentos. Sistemas modernos pueden incluir no solo funciones de control de acceso, sino también funciones corporativas tales como: manejo de credenciales y bases de datos personales. Tampoco los sistemas de control de acceso en redes han alcanzado sus límites funcionales: es fácil concebir un lector de tarjeta que actúe como un reloj que marca el tiempo de entrada y salida de los empleados, extendiendo así el sistema al departamento de recursos humanos y de pagos (figura 3) o una tarjeta de identificación que incluye una aplicación de pago para el sistema local de transporte.

Esta nueva arquitectura de múltiples aplicaciones en red, requiere el compromiso y la cooperación de varios departamentos, incluyendo seguridad, IT, Recursos Humanos y otros en la implementación de un sistema de control de acceso físico corpora

Figura 3. Ejemplo De un Sistema de Control de Acceso Físico en Red



La Tarjeta de Identificación Inteligente: El Papel de las Tarjetas Inteligentes en un Sistema de Acceso Físico Seguro

Originalmente, el distintivo del empleado era usado como una credencial de identidad visual. El acceso a los edificios y a las puertas era dado cuando un guardia reconocía el distintivo del portador de la tarjeta. Las tecnologías para automatizar el control de acceso (tal

como cintas magnéticas, códigos de barra y chip de proximidad) fueron desarrolladas para reducir los costos operativos, aumentar la seguridad e incrementar la conveniencia.

Mientras esas tecnologías reducen los costos de operación e incrementan la conveniencia, ellos no garantizan que el portador del distintivo es de hecho la persona autorizada a tener el distintivo. Otras tecnologías de identificación brindan poca o ninguna seguridad para redes de computadoras. El requerimiento de una credencial segura única para acceso físico y lógico y para protección de la información privada del individuo han llevado a la emergencia de la tarjeta de identificación inteligente: Una credencial de identificación en la cual tecnologías de tarjetas inteligentes de contacto y/o sin contacto, son integrados en una identificación corporativa que permite a los sistemas de acceso ser implementados con niveles adicionales de seguridad –autenticación, autorización y no rechazo.

La tarjeta de identificación inteligente le brinda a una persona (o dispositivo) un acceso seguro y autenticado tanto a recursos físicos como virtuales. El distintivo puede autorizar el acceso a edificios, a redes de computadoras, a archivos de datos o a la computadora personal del usuario. Además, estas mismas tarjetas pueden ahora incluir aplicaciones que permiten acceso a sistemas de transporte de masas, pagos de cuentas y otros datos seguros. El requerimiento común a todas estas aplicaciones es la identificación autenticada del usuario.

Muchas de las personas involucradas en la compra, implementación y uso de tarjetas inteligentes – desde el Director Ejecutivo (CEO) hasta (y más importante) el empleado, están dándose cuenta de los beneficios de estas tarjetas. Casi toda revista en seguridad incluye por lo menos un artículo, sino el artículo de portada, sobre la convergencia de acceso físico y lógico. Tales artículos describen las ventajas de seguridad, ROI, conveniencia y consideraciones de implementación..

Beneficios de las Tarjetas de Identificación Inteligentes

Para escoger una credencial de acceso se debe atender las preocupaciones de varias áreas funcionales de una organización. La gerencia ejecutiva necesita tanto acceso físico como de red seguros. Con presupuestos operativos cada vez más bajos, los Directores Ejecutivos (CEOs) y los Oficiales Jefes de Finanzas (CFOs) están demandando hacer un sólido caso de negocios y el planteamiento de soluciones que sean las más costo-efectivas . El Oficial Jefe de Seguridad (CSO) y el Oficial Jefe de Informática (CIO) tienen que ser notificados de cualquier falla de seguridad rápidamente, identificar y localizar el perpetrador y recoger toda evidencia forense que pueda ponerse en un caso en la corte. Los Recursos humanos quieren que los nuevos empleados lleguen al terreno operando inmediatamente,

para incrementar su eficiencia y la ganancia de la empresa. La legislación de gobierno requiere que la privacidad de las personas sea respetada. Y finalmente, los empleados necesitan una credencial de identificación que sea fácil y conveniente de utilizar. De otra forma, los empleados encontrarán formas de burlar la seguridad o los costos de las acreditaciones de los empleados aumenten tan significativamente que la compañía terminará abandonando el sistema.

Las tarjetas de identificación inteligentes son una solución costo-efectiva y flexible que atienden a los requerimientos a través de toda la organización. Una sola tarjeta de identificación inteligente puede incorporar múltiples tecnologías, acomodando tanto los sistemas de control de acceso nuevos como los sistemas preexistentes, como parte de un plan general de migración hacia las nuevas tecnologías de control de acceso. Los distintivos para empleados pueden respaldar una gama de perfiles de seguridad, dependiendo del nivel de acceso requerido por el empleado. Por ejemplo, algunos distintivos pueden brindar solo acceso limitado al establecimiento y acceso a la red, mientras otros distintivos pueden brindar acceso especial a áreas restringidas y usar chips de tarjetas inteligentes de contacto o sin contacto para respaldar: patrones biométricos que autentican el usuario ante la tarjeta; algoritmos seguros de señas y contraseñas que autentican la tarjeta y el lector unos a otros; y un protocolo con clave de manejo seguro que cambia cada vez que el distintivo es presentado al lector para prevenir la duplicación de la tarjeta y proteger la privacidad de la información.

Las nuevas especificaciones de software de integración de sistemas y productos, ayudan a identificar y analizar las fallas en seguridad. El vincular las bases de datos de acceso físico y de Informática ofrece el potencial de inmediatamente identificar cualquier actividad sospechosa. Por ejemplo, si un computador ha sido accedido por un empleado que ha abandonado el edificio, el departamento de Informática puede ser notificado inmediatamente e investigar la actividad. De forma similar, la seguridad puede ser notificada si un computador de un área restringida ha sido accedido por un empleado que no está autorizado para estar en esta área. La comunicación conjunta entre los sistemas de acceso físico y lógico permite a las compañías proteger datos confidenciales e identificar problemas de seguridad.

Los sistemas de control de acceso deben atender a las necesidades del empleador y del empleado y satisfacer los requerimientos legales. Hay tarjetas de identificación seguras disponibles que usan los protocolos más recientes de seguridad y de técnicas de prevención contra sondeos. La información de un empleado está disponible solamente para aquellos a quienes el empleador ha autorizado el acceso. Una organización puede querer usar un único proceso para manejar las autorizaciones de los empleados, accesos y privilegios. Al vincular las bases de datos de recursos humanos, Informática y de

acceso físico significa que el empleado puede hacer un solo viaje a un departamento y recibir un distintivo que contiene toda la información requerida. La base de datos de recursos humanos puede indicar que privilegios de acceso pueden ser asignados. El software de Informática puede verificar la base de datos de Recursos Humanos y asignar las palabras claves y certificaciones requeridas. Una huella digital biométrica y una foto digital se podrán tomar. Con esa información, una tarjeta en blanco puede ser luego insertada en una impresora de distintivos y toda la información requerida puede ser bajada a la tarjeta y la tarjeta puede ser impresa. El empleado recibe el distintivo dentro de pocos minutos y empieza a trabajar inmediatamente.

Las tarjetas de identificación inteligentes son convenientes y de fácil uso. Los empleados solo tienen que mantener un solo distintivo, de esta forma se reduce la probabilidad de que se pierda u olvide el distintivo o de que se dañe. Los empleados no tienen que buscar el distintivo correcto o sentir que están llevando consigo una gran cantidad de tarjetas.

CONCLUSION

Los Gobiernos, las corporaciones y las universidades están descubriendo que las tarjetas de identificación inteligente pueden satisfacer sus necesidades para aplicaciones tanto de acceso físico como lógico. Un sistema a base de tarjetas inteligentes brinda beneficios a través de una organización, mejorando la seguridad, la conveniencia del usuario, a la vez que reduce los costos generales de gestión y administración. La tecnología de tarjetas inteligentes brinda una plataforma flexible y costo-efectiva no solo para control de acceso físico sino también para nuevas aplicaciones y procesos que pueden beneficiar a la organización como un todo.

Consideraciones Claves para la Implementación de un Sistema de Identificación de Acceso Físico Seguro

La implementación de un sistema de identificación de acceso físico basado en tarjetas inteligentes requiere tomar en consideración algunos aspectos claves, comenzando por una consideración y análisis cuidadoso de los requerimientos operacionales.

Tecnologías Candidatas de Tarjetas Inteligentes

Cuando se considera la implementación de un nuevo sistema de acceso físico seguro, hay dos soluciones al problema de cómo una aplicación de seguridad física lee un credencial: de contacto y sin contacto. La decisión de adoptar una tecnología de tarjetas inteligentes de contacto o sin contacto depende de los requerimientos de la organización.

Tecnología de Tarjetas Inteligentes sin Contacto

La tecnología de tarjetas inteligentes sin contactos es más adecuada para acceso físico a través de portales de alto tráfico y es la mejor selección para usar en áreas donde el ambiente físico es hostil o en áreas que están expuestas al tiempo o a la intemperie. (Lectores de acceso de puertas que deben estar expuestas al viento, polvo, lluvia, nieve, hielo, ocasionalmente goma de mascar, papel, cenizas de cigarrillos y que debe ser protegido).

Dos estándares de tarjetas inteligentes sin contacto ISO/IEC14443 e ISO/IEC 15693, son buenos candidatos para el uso de aplicaciones de control de acceso físico. Nuevas implementaciones de sistemas de control de acceso deben considerar estos estándares de tarjetas inteligentes sin contactos para satisfacer nuevos requerimientos de aplicación para mayor seguridad (por ejemplo técnicas de autenticación biométricas y otras avanzadas), para acomodar múltiples aplicaciones en una sola tarjeta (por ejemplo acceso físico, acceso lógico, transacciones de pago) y para proteger la privacidad de la información del portador de la tarjeta.

ISO/IEC 14443 es una tecnología sin contacto de 13.56Mhz con un radio de operación de hasta 4 pulgadas (diez centímetros). El ISO/IEC 14443 fue diseñado originalmente para emisión electrónica de boletos y para aplicaciones financieras electrónicas. Para esas aplicaciones radios de acción operacional cortos y velocidades de transacción rápidas son críticos. Los mismos requerimientos de mercado llevaron el ISO/IEC 14443 a ser adaptados para transporte, pagos fuera de línea y transacciones de ventas. Como las aplicaciones que usan ISO/IEC 14443 generalmente requieren un valor almacenado en la tarjeta, el desarrollo de nuevos productos se enfoca en seguridad, donde está tecnología actualmente oferta memoria central segura y esquemas de encriptación sofisticada respaldados por varios co-procesadores de encriptación.

Los productos ISO/IEC 14443 son los que están ahora empezando a moverse en el mercado de control de acceso físico. Las credenciales de acceso físico que están de conformidad con ISO/IEC 14443 ofrecen soluciones que van desde tarjetas de memoria de bajo costo hasta tarjetas micropocesadoras altamente seguras. Tarjetas micropocesadoras ofrecen niveles de interactividad de seguridad de identificación a niveles ofrecidos por las tarjetas inteligentes de contacto. Debido a que tarjetas ISO/IEC 14443 pueden transferir grandes bloques de datos muy rápidamente, muchas de las llaves de acceso físico que son habilitadas de forma biométrica que están disponibles hoy, son usados con tarjetas de ISO/IEC 14443. Varios productos ahora apoyan la transferencia de datos hasta 848 Kilobits por segundo y una enmienda para modificar el estándar ha sido sometida a las organizaciones que formulan los estándares para incluir estas tasas de transferencia de datos más elevadas.

ISO/IEC 15693 es una tecnología de Radio Frecuencia pasiva de 13.56 MHz diseñado para operar en radios de acción hasta tres pies (un metro) a la vez que cumplen con los límites de salidas FCC establecidos en los Estados Unidos. Puede ser usada para control de acceso a establecimientos en edificios que leen radios de acción que pueden ser establecidos entre 4 a 6 pulgadas (10 a 15 centímetros) para las puertas del edificio. El ISO/IEC 15693 también es ideal para lotes de estacionamientos donde las tarjetas y los lectores pueden ser seteados para operar en radios de acción mayores, de forma que no sea necesario que el conductor extienda su brazo fuera de la ventana del carro.

La Tecnología de ISO/IEC 15693 fue desarrollado para operar en radios de acción de lectura y escritura muchos mayores. Las aplicaciones iniciales que usaron esa tecnología, incluyeron el seguimiento y la identificación de bienes que requerían radios de acción operacional más amplios y transmisión de mayores bloques de datos. Debido a las capacidades de esta tecnología está se transformó en una de las tecnologías preferidas para acceso físico. Los radios de acción operacionales mayores respaldan las capacidades que los usuarios esperan cuando ellos se acercan a una puerta. El almacenaje de lecto-escritura de patrones biométricos, datos e información personal también está llevando a la migración de 125KHz hacia tarjetas inteligentes sin contacto tipo ISO/IEC 15693.

Las tecnologías ISO/IEC 14443 e ISO/IEC han evolucionado con sus propias características y especificaciones. Las diferencias claves entre las dos tecnologías son sus radios de acción operacionales, velocidad (tasa de transferencia de datos) y la extensión y madurez de las características y aplicaciones que usan las tecnologías. La figura 4 resume las especificaciones y características claves que generalmente están disponibles para productos que respaldan los

dos estándares de tarjetas inteligentes sin contacto, a la fecha de la publicación de este informe⁷

Figura 4 Características y Especificaciones Claves de las Tarjetas Inteligentes sin Contacto

Features	ISO/IEC 14443	ISO/IEC 15693
Estándares	ISO/IEC 14443 ISO/IEC 7810	ISO/IEC 15693 ISO/IEC 7810
Frecuencia	13.56 MHz	13.56 MHz
Radio de acción operacional (ISO)⁸	Hasta 10 centímetros (~3-4 pulgadas)	Hasta 1 metr (~3.3 pies)
Tipos de Chips respaldados	Micro controlador con memoria lógica	Memoria lógica
Funciones de Encriptación y autenticación ⁹	MIFARE, DES/3DES, AES, RSA10,, ECC	Suplidores específicos, DES/3DES
Radio de acción de la capacidad de la memoria	64 a 64K bytes	256 y 2K bytes
Habilidad de lecto-escritura	Lecto-escritura	Lecto-escritura
Tasa de transferencia de datos (Kb/sec)	Hasta 106 (ISO) Hasta 848 (disponible)	Hasta to 26.6
Anti-colisión	Si	Si
Autenticación de la tarjeta al lector	Señal/contraseña	Señal/contraseña
Competente para una tarjeta híbrida	Si	Si
Respalda interfase de contacto	Si	No

Tecnología de Tarjetas Inteligentes de Contacto

Las tarjetas inteligentes de contacto que cumplen con el estándar ISO/IEC 7816 están siendo usadas actualmente en una amplia variedad de aplicaciones incluyendo acceso físico y lógico.

Las tarjetas inteligentes de contacto son típicamente usadas para entradas con bajo volumen y donde la velocidad para entrar no es un problema, tal como áreas internas o áreas de alta seguridad, donde el uso de múltiples factores mitiga la ventaja que las tarjetas sin contacto ofrecen para un acceso más rápido. Las tarjetas inteligentes

⁷ Para información adicional acerca de tecnología sin contacto, ver "Contactless Technologies for Secure Physical Access: Technology and Standards Choice" (Acceso Físico Seguro para Tecnologías Sin Contacto: Selección de Tecnologías y Estándares), informe Smart Card Alliance, octubre 2002.

⁸ Distancias especificadas por los estándares de ISO/IEC. La Implementación de Acceso Físico establecerían los radios de acción operacional específico típicamente hasta 15 centímetros (seis pulgadas).

⁹ Los estándares de ISO/IEC no especifican funciones de seguridad.

¹⁰ Encriptación basada en RSA pueden no estar disponible en todas las tarjetas debido a consumo de energía limitaciones en el tiempo de ejecución o a lo largo de la clave .

de contacto no son típicamente utilizadas para los sistemas de acceso físico que involucran un volumen alto de usuarios y millares de accesos por día, o que requieran ser resistentes a las inclemencias del tiempo o al vandalismo, o que necesitan que el acceso sea altamente conveniente para el usuario. Sin embargo la tecnología de tarjetas inteligentes de contacto es más y si ofrece una capacidad de avanzado que todavía no está disponible con tecnologías sin contacto (por ejemplo procesadores más avanzados, mayor capacidad de memoria, y sistemas operativos avanzados). Debido a esto, organizaciones que necesitan de tales características pueden requerir un abordaje con tarjetas inteligentes de contacto.

La selección de cual tecnología de tarjetas inteligentes es la adecuada para un nuevo sistema de acceso físico seguro debe ser guiada por las necesidades de corto y largo plazo de la organización. Al definir tanto los requerimientos inmediatos como futuros del sistema, las organizaciones pueden seleccionar las tecnologías que mejor respondan a sus necesidades globales de implementación.

La escogencia de cual tecnología de tarjeta inteligente es apropiada para un nuevo sistema de acceso físico seguro debe ser determinada por las necesidades organizacionales a corto y largo plazo. Al identificar los requerimientos inmediatos y futuros del sistema, las organizaciones pueden seleccionar las tecnologías que mejor satisfacen las metas generales de implementación.

Requerimientos y Problemas de Interfase del Usuario

El volumen de paso y facilidad de uso son consideraciones claves en un sistema de seguridad físico. Un establecimiento grande, con miles de empleados probablemente necesita brindar acceso en un corto período de tiempo. La tecnología sin contacto tiene obvias ventajas para volumen de paso sobre la tecnología de contacto o la inspección visual de distintivos. Sin embargo, ciertas compensaciones deben ser tomadas en cuenta.

Facilidad de Uso Vs. Desempeño y Seguridad

Cualquier decisión relacionada con un sistema de control de acceso y la credencial de identificación debe equilibrar la facilidad de uso para el portador de la tarjeta con el desempeño y la seguridad de la tarjeta y del documento de identificación. Una evaluación cuidadosa de estos y otros requerimientos de la organización constituyen el primer paso en la selección de una tecnología de contacto o sin contacto.

El ambiente sin contacto tiene obvias ventajas en términos de velocidad y facilidad de uso. Los problemas de tener que alinear una tarjeta con lector o insertar una tarjeta en un lector son eliminados consecuentemente el volumen de paso aumentan (a menos que exista un requerimiento para una autenticación por múltiples factores, tales como el uso de un PIN o de un factor biométrico). Sin embargo,

en algunos casos un ambiente de contacto puede ser considerado como un sistema más seguro, si existe preocupación de que señales de radio frecuencia de que tarjetas sin contacto pudiesen estar comprometidas (ya que la conexión física entre la tarjeta y el lector reduce el potencial que señales de radio frecuencia comprometan el sistema). Usando señal y contraseña y otras técnicas criptográficas en la implementación de tarjetas inteligentes sin contacto puede ayudar a minimizar este riesgo.

El radio de acción operacional de las tecnologías sin contacto es una consideración clave en lo que respecta la facilidad de uso. Los radios de acción operacional mayores pueden ser la solución preferida en situaciones donde el volumen de paso en el punto de acceso y la conveniencia para el usuario es la principal preocupación, o cuando se requiere acceso de manos libres. Los radios de acción operacional más cortos pueden ser preferidos cuando se requieren otros factores de autenticación.

Cualquier decisión para implementación debe tomar en cuenta la compatibilidad con las políticas y procedimientos generales de seguridad física.

El impacto del “Americans with Disabilities Act” (Legislación sobre las Personas con Impedimentos)

Los establecimientos públicos en los Estados Unidos actualmente están obligados a cumplir con la reglamentación impuesta por el “American Disabilities Act”. Este requerimiento puede influenciar la selección de una tecnología adecuada de seguridad física, ya que las organizaciones deben tomar en cuenta el problema de la destreza manual y otras limitaciones físicas. Para usuarios que pudieran estar confinados a sillas de ruedas o que de alguna forma necesiten asistencia para desplazarse, el requerimiento de para orientar una tarjeta para insertarlo en el lector puede ser un problema. Además, puede haber problemas con la presentación de la tarjeta al acercarse al lector. Puede ser necesario instalar los lectores más cerca del piso para facilitar el acceso a personas en sillas de rueda. Un radio de acción operacional mayor brinda ventajas para usuarios con discapacidades.

· Nota del traductor: La mayoría de los países en América Latina están empezando a adoptar legislaciones similares al del American with Disabilities Act, para respetar los derechos de personas con discapacidad.

Consideraciones a Nivel de Sistema

La selección de un diseño de sistema y de la arquitectura de seguridad debe ser determinado según los requerimientos de desempeño e interfase con el usuario, así como los requerimientos para la integración con otros sistemas de seguridad o no (por ejemplo recursos humanos, controles internos de los edificios). Además, la funcionalidad de los varios componentes de los sistemas

(credenciales, lectores, paneles, servidor de control de acceso, base de datos), debe ser examinada para asegurar que el sistema se ha diseñado con la seguridad, flexibilidad y la incrementabilidad deseada (scalability)

Sistemas Centralizados Vs. Sistemas Distribuidos

Una consideración básica en el diseño de un sistema es la de establecer si el sistema debe ser centralizado o distribuido. Esta decisión será un factor determinante para la funcionabilidad del sistema. Se deben tomar decisiones sobre donde serán almacenados los PINs o patrones biométricos y que nivel de criptografía será incluida en una credencial. Almacenaje a nivel central vs. Almacenaje en la tarjeta tiene diferentes implicaciones en cuanto a vulnerabilidad de los datos a diferentes tipos de amenazas en cuanto a la protección de la información privada.

Sistemas Abiertos Vs. Sistemas Propietarios

Otro factor en el desarrollo de un sistema de acceso físico seguro es en que medida es deseable la integración con otros sistemas de seguridad. (La próxima sesión discute en mayor detalle la interoperabilidad). Estos otros sistemas pueden incluir dispositivos para detección de intrusos, cámaras de vigilancia, almacenaje de videos y controles de edificios. Cuando se requieren soluciones de interoperabilidad, el sistema debe ser diseñado para incorporar una arquitectura abierta y aplicaciones estándares de programación de interfases (APIs) abiertas al máximo grado posible.

De hecho, el mejor abordaje para definir los requerimientos de un sistema de acceso físico seguro es adoptar una visión de seguridad que abarque toda la empresa. Cuando se toman decisiones sobre soluciones y tecnologías de seguridad individuales a la vez que los encaja en un plan holístico de seguridad que abarca toda la empresa se pueden tomar decisiones que dan dividendos de largo plazo y eliminar medidas transitorias “stop gap” que resultan de la implementación de sistemas aislados y cerrados.

La tecnología que se va a usar debe ser escogida cuidadosamente. Escoger un sistema basado en una arquitectura abierta usando APIs abiertos tiene ciertas ventajas tales como mayor facilidad para integración con otros sistemas, flexibilidad de adquisición, facilidad de expansión e incrementabilidad. En el análisis final sistemas propietarios o cerrados pueden tener una ventaja a corto plazo de costos y de tiempo de implementación, pero a largo plazo sacrifican flexibilidad, incrementabilidad e integración.

Interoperabilidad

Interoperabilidad es un elemento clave en el diseño e implementación de una solución para control de acceso físico. El significado de “interoperabilidad” frecuentemente puede tener un significado diferente para varios negocios y organizaciones. Sin embargo, se

presenta abajo algunos puntos importantes que deben ser considerados:

- ¿Cómo se da la interoperabilidad de nuevas tecnologías con los sistemas de acceso físico y lógico preexistentes?
- ¿Cómo se da la interoperabilidad entre los productos sin contacto disponibles de múltiples vendedores entre sí?
- ¿Cómo afectan los sistemas de acceso físico y lógico la infraestructura y otras aplicaciones de una empresa?

Interoperabilidad debe ser considerada en el contexto de varias opciones tecnológicas disponibles para soluciones de control de acceso físico.

La tecnología de proximidad de 125KHz es ampliamente utilizada y típicamente será el sistema preexistente que está siendo incrementado o que debe ser integrado con el nuevo sistema. El mayor problema con los sistemas de 125KHz es que no están sujetos a ningún estándar oficial, sino más bien tienden a ser soluciones propietarias del vendedor o en el mejor de los casos, sujetas a estándares de facto . Ese problema es de particular importancia cuando una organización está integrando una nueva tecnología de tarjetas inteligentes. Puede que sea necesario (por ejemplo) planificar la implementación de múltiples tecnologías sin contacto hasta tanto se complete la migración de la infraestructura de la empresa a la nueva tecnología de tarjetas inteligentes sin contacto.

Los estándares de tarjetas inteligentes –ISO/IEC 7816, ISO/IEC 14443, ISO/IEC 15693 especifican como los componentes interaccionan a un determinado nivel, en la cual diferentes estándares respaldan funciones interoperativas a diferentes niveles. Los estándares no incluyen todos los comandos o características de seguridad necesarias para respaldar una implementación completa del sistema. Las tarjetas inteligentes que incluyen microprocesadores brindan mayor flexibilidad para la implementación de protocolos de interoperabilidad. Adicionalmente, la introducción del sistema de operación de tarjetas de “uso general” (general purpose) crea una plataforma genérica que puede ser usada por varias aplicaciones.

Solución de Tarjeta Vs. Solución de Lector El hecho de simplemente requerir que las tarjetas y los lectores estén de conformidad con un estándar ISO/IEC en particular no es suficiente para asegurar la interoperabilidad entre sistemas y dispositivos de diferentes fabricantes, proveedores o integradores de aplicaciones. La interoperabilidad a cierto nivel se puede lograr usando un lector interoperativo o una tarjeta interoperativa. Cada uno de estos abordajes va a incurrir en diferentes costos y tendrán diferentes ventajas y desventajas.

Muchos fabricantes de lectores están ofreciendo ahora lectores que pueden leer y escribir en tarjetas que cumplen tanto con el estándar

ISO/IEC 14443 como ISO/IEC 15963. Otros productos están disponibles que pueden comunicarse con tarjetas que satisfacen tanto el estándar ISO/IEC 14443 como el ISO/IEC 15963 utilizando un chip de lectura único.

Cuando se selecciona una tecnología de tarjeta inteligente de contacto o sin contacto los diseñadores del sistema deben revisar que nivel de interoperabilidad es respaldado y como los productos se acomodan a funciones no estandarizadas.

Para resolver el problema de la falta de seguridad y de estándares de aplicaciones interoperativos, las organizaciones usuarias pueden colaborar para desarrollar especificaciones para interoperabilidad con un enfoque de la industria. Por ejemplo:

-
- La especificación EMV fue desarrollado por la industria financiera para tarjetas inteligentes de contacto usado con aplicaciones de pago de crédito y de débito.
- El Government Smart Card Interoperability Specification (GSC-IS) brinda soluciones a un gran número de problemas de interoperabilidad asociados con la implementación de tecnología de tarjetas inteligentes de contacto. Esto permite al programador de la aplicación a desarrollar aplicaciones para el cliente sin tener un conocimiento íntimo de las interfases de la tarjeta . La especificación fue definida para ofrecer la habilidad de desarrollar tarjetas inteligentes de identificación segura que pueden funcionar en múltiples agencias de gobierno o entre los gobiernos federal, estatal o local. Está en proceso de revisión del GSC-IS (dirigido por National Institute Of Standards and Technology (NIST)) que va a incluir definiciones de interoperabilidad para tecnología de tarjetas inteligentes sin contacto, brindando un recurso para la industria que puede ser usado para implementaciones con tarjetas inteligentes sin contacto.

Administración del Ciclo de Vida

Un punto crítico en la implementación de un sistema de acceso físico es la necesidad de rastrear cada tarjeta de acceso y cada aplicación en la tarjeta. Una función que es única de las tarjetas inteligentes es la capacidad de almacenar o modificar aplicaciones después que la tarjeta ha sido emitida (también llamado personalización post emisión (post issuance personalization)). Debido a que la información en la tarjeta inteligente puede ser modifica de forma dinámica es necesario rastrear el ciclo de vida de las aplicaciones en la tarjeta y el ciclo de vida de la tarjeta. La administración del ciclo de vida¹¹ rastrea y en algunos casos administra todos los cambios a los datos de la tarjeta

¹¹ Los siguientes documentos del Global Platform y Open Security Exchange ofrecen una revisión más completa de los problemas de gestión de ciclo de vida de la tarjeta: "A Primer to the Implementation for Smart Card Management and Related Systems," disponible en www.globalplatform.org; "Physical Security Bridge to IT Security," disponible en www.opensecurityexchange.com

inteligente, independientemente de que la información en la tarjeta sea una nueva versión de una aplicación, una nueva tecnología de chip, o una información actualizada sobre el portador de la tarjeta.

En su expresión más simple la administración del ciclo de vida puede concebirse como una base de datos vinculada a una aplicación de control de acceso específica. La base de datos registra información sobre transiciones y datos en el estado del ciclo de vida como las siguientes:

- El tipo de tarjeta, como una tarjeta de empleado de contratista, o visitante.
- Información solicitada y autorización en la tarjeta
- Información personalizada en la tarjeta, incluyendo:
 - La versión del sistema operativo y los datos del chip
 - Datos personalizados, incluyendo elementos visibles como una foto, firma o códigos de barra.
 - Vínculos de la base de datos
- Información de gestión de la aplicación incluyendo:
 - El estado de los privilegios (los emitidos o actualizados).
 - Información de expiración, reemplazo o re-emisión de la tarjeta.
 - Activación, suspensión y reactivación de la aplicación (bloquear y desbloquear reversible)
 - Aplicaciones post emisión.

El inventario de tarjetas de control de acceso debe ser rastreado y auditado para proteger contra la emisión no autorizada de tarjetas. La administración del inventario de las tarjetas incluye contar todas las tarjetas recibidas y distribuidas a los centros de emisión. El ciclo de vida de la tarjeta comienza con un registro del número de serie del chip brindado por el proveedor de la tarjeta la administración del ciclo de vida subsecuentemente rastrea todas las adiciones o cambios a los datos almacenados en cada tarjeta individual, y simplifica el proceso de re-emisión de las tarjetas asegurando que la nueva tarjeta tiene el mismo conjunto de aplicaciones y de valores de parámetros de aplicación incluidos en la tarjeta original.

Tarjetas de Acceso de Aplicación Única

Las tarjetas de aplicación única vinculan una aplicación a la tarjeta. Para tales tarjetas, la aplicación y la tarjeta son administradas como un ciclo de vida. Para muchos sistemas de control de acceso los administradores pueden controlar cambios a la aplicación requiriendo que los portadores de las tarjetas traigan sus tarjetas a un local específico para que sean actualizadas, eliminando la necesidad de sustituir tarjetas cuando cambian privilegios o aplicaciones en este caso, la aplicación controla cualquier cambio en la tarjeta y la base de datos es actualizada.

La administración de la tarjeta puede ser automatizada vinculando la base de datos del portador de la tarjeta a la aplicación de acceso

incluyendo reglas de decisión sobre privilegios de acceso. En este caso, el sistema de administración de la aplicación asegura que la información es consistente entre las bases de datos, ofreciendo un camino de auditoría completo que rastrea la emisión, actualizaciones y expiración o revocatoria.

Organizaciones que tienen múltiples localizaciones pueden usar un sistema automatizado de manejo de las aplicaciones para asegurar la integridad de los datos de la aplicación y mejorar la seguridad del sistema, asegurando (por ejemplo) que una tarjeta emitida en una localización es válida en todas las localizaciones, o que un cambio en el estado de la aplicación en un establecimiento es inmediatamente implementado en todas las localizaciones. El nivel de seguridad para controlar las actualizaciones a los datos de las tarjetas o a la base de datos es controlado en este caso por la aplicación.

Tarjetas de Aplicación Múltiple

La tecnología de tarjetas inteligentes brinda la oportunidad de incluir múltiples aplicaciones en una tarjeta. (Para ejemplos ver una sección posterior en la página 35 Nuevas Aplicaciones Habilitadas por Sistemas de Tarjetas Inteligentes). Cada aplicación puede ser manejada por un grupo diferente dentro de la organización o hasta por un proveedor externo (por ejemplo, una bolsa electrónica para terceros para uso de una cafetería). A pesar de que esto requiere una coordinación organizacional más compleja, la implementación de múltiples aplicaciones puede hacer más fuerte un caso de negocios en apoyo a la adopción de tarjetas inteligentes. La tecnología de tarjetas inteligentes permite el uso de herramientas basadas en el web que permite a los usuarios adicionar, modificar o eliminar aplicaciones de forma segura sin que se necesite de un administrador para hacer dichos cambios. En estos casos la administración del ciclo de vida debe controlar y rastrea el estado de cada aplicación almacenada en cada tarjeta.

El manejo del ciclo de vida de una aplicación es fundamentalmente diferente del manejo del ciclo de vida de una tarjeta. El área funcional que emite la tarjeta (por ejemplo el departamento de infraestructura) puede estar completamente separado del área funcional que maneja una aplicación (por ejemplo informática o recursos humanos). La administración centralizada del ciclo de vida de la tarjeta requiere que la entidad que emite las tarjetas sea responsable por la producción inicial de la tarjeta y de brindar una interfase a los otros proveedores de aplicaciones para almacenar, personalizar y actualizar aplicaciones.

Una vez que las tarjetas son emitidas hacer cambios a los datos o a una aplicación puede realizarse a nivel central o de forma remota, usando comunicaciones seguras. Un ambiente híbrido brinda la mayor flexibilidad, combinando los mejores elementos de una gestión tanto centralizada como distribuida. Cuando se utiliza el Internet para personalización posterior a la emisión, se requieren controles

adecuados para verificar el portador de la tarjeta y asegurar la integridad y encriptación de los datos. Esto requiere un almacenador de aplicación seguro que este bajo el control del proveedor de la aplicación.

Cuando se consideran múltiples aplicaciones para una tarjeta de acceso un sistema de gestión del ciclo de vida de la tarjeta basada en un conjunto de reglas de negocio puede manejar varios tipos de tarjetas y de aplicaciones. Este sistema puede brindar las siguientes funciones:

- Administración centralizada para emisión de tarjetas, con una interfase para cada aplicación, para almacenaje de aplicación y personalización.
- Administración centralizada de tarjetas y aplicaciones, aplicando decisiones o reglas de autorización para añadir, modificar, bloquear o desbloquear aplicaciones y roles administrativos.
- Implementación de cambios a una aplicación basados en eventos, tales como bloquear privilegios para una tarjeta perdida o bloquear una aplicación si se da un uso sospechoso a una tarjeta.
- Un proceso para atender solicitudes del usuario para añadir aplicaciones o modificar privilegios y para personalización de tarjetas de forma segura después que han sido emitidas.
- Una auditoria central para transiciones en del status del ciclo de vida de una aplicación
- Respaldo y acceso del usuario a los datos del status del ciclo de vida.

Otras consideraciones

Generación y administración de claves son funciones críticas. La generación de claves en par y los certificados digitales asociados deben ser controlados durante los procesos de emisión y actualización. Esquemas de seguridad deben proteger sesiones claves, comenzando con el uso de las claves de transporte del fabricante de la tarjeta y durante todos los cambios del ciclo de vida en la tarjeta. El proceso de preparación inicial de los datos (preparación de los conjuntos de datos, escritura (script) y claves únicas), siguen siendo una función del proveedor de la aplicación. El emisor brinda la infraestructura que permite que las tarjetas de identificación segura sean “verificadas en el futuro”(future proofed) asegurando que aplicaciones y nuevas funciones pueden ser implementadas con seguridad después que la tarjeta ha sido emitida.

Costos y Beneficios

Es un desafío cuantificar con precisión los beneficios potenciales de un sistema de seguridad. Las iniciativas de seguridad son parte de una estrategia general de reducción de riesgo y los costos de mitigación deben ser sopesados contra los riesgos. Cuando es posible, el sistema debe ser diseñado para beneficiar tanto la

seguridad como las operaciones. Por ejemplo, una credencial segura puede incrementar tanto seguridad como el volumen de paso. Además, si la credencial es usada para múltiples propósitos los costos administrativos pueden ser reducidos.

Una consideración importante en el diseño e implementación de cualquier solución de negocio es determinar quien paga por el sistema. Un sistema de seguridad físico puede ser considerado como responsabilidad del departamento de seguridad. Sin embargo, si el sistema es considerado como otro sistema de informática, el puede ser considerado entonces como parte de la red de informática. Además, como la seguridad es una función a nivel de toda la organización, puede haber varios dueños del sistema, incluyendo seguridad, administración del edificio, recursos humanos o gerencia ejecutiva.

La habilidad de las tarjetas inteligentes de respaldar múltiples aplicaciones pueden ayudar en hacer una propuesta comercial (business case) para la implementación de un nuevo sistema. Múltiples organizaciones o departamentos pueden implementar aplicaciones y compartir el costo de la una nueva tarjeta de identificación segura y de su infraestructura. Una vez que este establecida la infraestructura del sistema de control de acceso basado en tarjetas inteligentes, el costo incremental para adicionar nuevas aplicaciones o funciones es menor.

El compartir la carga de planificación, diseño y costo de un sistema de seguridad físico permite que la toma de decisiones resulte en una solución flexible e incrementable para seguridad física. El proceso debe incluir la evaluación de los requerimientos para una arquitectura abierta con la meta de conseguir un sistema integrado que maneje múltiples aplicaciones.

Tendencias de Mercado

Tanto gobiernos como industrias están actualmente involucrados en la implementación de aplicaciones basadas en tecnología de tarjetas inteligentes. Muchas de estas aplicaciones usan tarjetas inteligentes para acceso a edificios y establecimientos. Aplicaciones en otros mercados verticales, tales como instituciones financieras y de venta al detal, tienen el potencial de vincularse con una tarjeta de acceso físico en el futuro. Para facilitar escenarios de aplicaciones múltiples, los desarrolladores de tecnología están introduciendo tarjetas con una variedad de tipos de interfases sin contacto y con contacto.

Gobierno

En los Estados Unidos, el gobierno federal está apoyando el uso de tecnología de tarjetas inteligentes para millones de tarjetas de identificación de empleados federales.

La Administración de Servicios Generales (GSA) desarrolló una especificación para tarjetas inteligentes de aplicación múltiple (GSC-IS), y varias agencias están planificando usar tarjetas que cumplan con esa especificación para accesos físicos.

El Departamento de Estado (DoS) está implementado un sistema de control de acceso para sus establecimientos en Washington D.C.. Los empleados y contratistas del Departamento de Estado recibirán tarjetas inteligentes de contacto para acceso físico y lógico.

El Departamento de Defensa (DoS) está emitiendo credenciales de tarjetas inteligentes a millones de personal militar, empleados civiles, y contratistas como parte de un programa de tarjeta de acceso común (CAC). Esas tarjetas actualmente ofrecen una plataforma común para PKI, acceso lógico e identificación que cumpla con los requerimientos de la Convención de Ginebra y que brindará acceso físico en el futuro.

La Administración de Seguridad del Transporte (TSA) está probando diferentes tecnologías para acceso físico y lógico bajo el Programa de Credencial de Identificación del Trabajador del Transporte (TWIC). Este programa puede resultar en una extensión hacia trabajadores del transporte del sector público y privado a nivel nacional.

Muchas agencias de transporte público que ya han introducido la tecnología de tarjetas inteligentes sin contacto para el pago de pasajes, ahora están explorando el uso de la misma tecnología para acceso a establecimiento y equipo. La Autoridad de Transporte del Area Metropolitana de Washington (WMATA), está usando la tecnología de la tarjeta de pasaje inteligente (SmarTrip™) para el acceso de sus empleados a las oficinas WMATA. Además, WMATA y el Departamento de Educación de Estados Unidos (DoE) han hecho una demostración usando una tarjeta inteligente sin contacto para identificación de empleado de DoE que es usado tanto para acceso a establecimientos como para pagos de pasaje. La Autoridad de Tránsito de Chicago ha introducido tecnología de tarjeta inteligente sin contacto para pago de pasaje y ha usado tarjetas de proximidad para acceso a establecimientos y equipo como cajeros en los buses.

Una revisión de la especificación de tarjetas inteligentes de la Administración de Servicios Generales (GSA) que incluye tecnología de tarjetas inteligentes sin contacto será lanzado en el verano del 2003. Demostraciones de tecnología sin contacto para acceso físico están siendo planificadas por el Departamento del Interior y del Tesoro de los Estados Unidos. Tarjetas con tecnología sin contacto

pueden ser evaluadas para uso en puertos y otros establecimientos de transporte donde sea esencial un rápido volumen de paso.

Comercial

Industrias comerciales están empleando aplicaciones de tecnologías de tarjetas inteligentes. Una cantidad de empresas comerciales, Sun Microsystems, Microsoft, Schlumberger, Shell, Boeing y Proctor & Gamble¹², están planeando la implementación de tarjetas de identificación inteligentes para acceso lógico y/o físico

Tarjetas inteligentes están siendo usadas para pagos en todo el mundo, incluyendo iniciativas desarrolladas por American Express, JCB, Master Card y VISA Internacional para probar o extender el uso de tarjetas inteligentes para pagos sin contacto. Por ejemplo, en Orlando, Florida, Master Card y varios bancos han emitido miles de tarjetas inteligentes sin contacto en la prueba piloto conocida como MasterCard® Pay Pass™. En esta prueba piloto tarjetas inteligentes sin contacto están siendo usados en almacenes de venta al detal y en restaurantes de comida rápida, donde la velocidad de la transacción y la conveniencia para el usuario son considerados de gran beneficio.

En la medida que la tecnología sin contacto emerge en varias industrias crece el potencial para tarjetas de aplicaciones múltiples que pueden ser usadas para identificación, acceso físico, pagos y otros propósitos. Actualmente, varios gobiernos extranjeros están emitiendo este tipo de tarjeta de aplicación múltiple. En algunos lugares como Hong Kong, el uso de tecnología sin contacto para pago del pasaje del transporte público está siendo expandido para respaldar otros tipos de pagos y otras funciones. Ya existe la tecnología que respalda estos programas. El desafío está en vincular programas del gobierno y del sector privado y de resolver problemas de administración del programa, compartir costos y privacidad.

Tecnologías Emergentes

Nuevos productos están siendo introducidos que facilitaran el uso de tecnologías de tarjetas inteligentes sin contacto para control de acceso físico. Sistemas de control de acceso físico que aceptan tarjetas que cumplen con ISO/IEC 14443 que simplemente tocan a un lector, tarjetas con ISO/IEC 15693, con un radio de acción operacional expandido o tarjetas inteligentes de contacto que son insertadas en un lector, están siendo incorporados.

Las organizaciones tienen muchas opciones de selección con tecnología de tarjetas de identificación inteligentes, incluyendo tarjetas de múltiples tecnologías, tarjetas híbridas y tarjetas de interfase dual. Para permitir acceso a establecimientos por personas de diferentes organizaciones se están desarrollando sistemas de control de accesos con tarjetas y lectores de tarjetas que pueden

¹² Building Blocks of the U.S. Smart Card Market, "Card Technology, may 2003

respaldar múltiples tecnologías de identificación. Por ejemplo, una tarjeta inteligente sin contacto o de contacto puede incluir tecnologías preexistentes como cintas magnéticas o códigos de barra. Ya están disponibles, tarjetas de tecnología múltiples que pueden combinar tanto tecnologías sin contacto de estándar ISO/IEC con tecnología de proximidad de 125KHz, permitiendo que las tarjetas operen tanto en sistemas de acceso físico preexistentes como con nuevos sistemas que cumplen estándares ISO/IEC.

Se están introduciendo tarjetas de interfase dual que incorporan tanto interfases de contacto como sin contacto en una sola tarjeta con un solo chip. Tarjetas inteligentes híbridas están disponibles que incluyen dos chips – uno de contacto y otro sin contacto. Esos productos permiten que las organizaciones puedan combinar aplicaciones de acceso físico sin contacto con aplicaciones que requieren una interfase de contacto, tales como acceso lógico a computadoras y redes. Dicha integración de acceso físico y lógico puede brindar beneficios de alta seguridad. Las organizaciones pueden vincular privilegios de acceso físico y lógico para incrementar la seguridad (por ejemplo, el requerimiento de usar la tarjeta para abandonar un establecimiento puede reducir el acceso no autorizado a las computadoras de los empleados y mejorar la respuesta administrativa de emergencia en el caso de una catástrofe en el establecimiento). Ese tipo de integración programática puede reducir los costos de emisión y administración de tarjetas y brindar a los usuarios la conveniencia de portar una sola credencial de identificación de acceso.

Para proveer factores adicionales de autenticación, se puede incluir en las tarjetas inteligentes múltiples factores biométricos. Los patrones biométricos pueden ser almacenados en la tarjeta o en otros componentes del sistema de control de acceso.

Nuevos sistemas de control de acceso físico basados en tarjetas inteligentes pueden brindar mayor flexibilidad a las organizaciones. Tales sistemas incluyen componentes programables, que permiten que los privilegios de acceso sean modificados sobre la marcha para responder a requerimientos cambiantes y condiciones de amenaza. Además, componentes basados en TCP/IP están listos para uso en redes, permitiendo el monitoreo centralizado de establecimientos ubicados en diferentes localizaciones.

Migración hacia Un sistema de Identificación de Acceso Físico Basado en Tarjetas Inteligentes

Una organización puede moverse a un sistema de identificación de acceso físico basado en tarjetas inteligentes por una variedad de razones – por ejemplo, para mejorar la seguridad, implementar procesos de identificación más eficientes, reducir el número de tarjetas de identificación portadas por el personal, ofrecer acceso a nuevas localizaciones o añadir nuevas aplicaciones. Independientemente de la razón que sea, la implementación de dicho sistema requiere que se tome en consideración si el nuevo sistema reemplazará a los viejos sistemas o si necesita integrarse y ser compatible con los sistemas preexistentes. Aunque la solución ideal pudiese ser reemplazar todos los sistemas viejos inmediatamente, moverse a un nuevo sistema basado en tarjetas inteligentes puede lograrse de forma incremental – lo que requiere un plan para hacer la mudanza de un sistema a otro al menor costo e interrupción de actividades posibles. Dicho plan, llamado un plan de migración, debe tomar en cuenta todos los componentes del sistema de control de acceso físico y desarrollar una estrategia que responda a los nuevos requerimientos, mientras se obtiene el mayor provecho de la inversión existente y se maneja la experiencia de los portadores de las identificaciones durante el proceso de migración.

Algunas preguntas claves que deben ser tomadas en cuenta cuando se planifica la migración, pueden incluir:

-
- ¿Cuál es el margen de tiempo deseado para reemplazar los sistemas preexistentes? ¿Cuántos sistemas preexistentes están instalados? ¿Hay diferentes sistemas preexistentes en diferentes localizaciones? ¿Hay nuevas localizaciones que deben ser tomadas en cuenta?
- ¿Cuáles puntos de acceso requieren nuevos lectores? ¿Son algunos o todos los puntos de acceso que requieren nuevas funciones (por ejemplo, biométricos o teclado de PIN) o si nuevas funciones solo son requeridas en algunos sitios seleccionados? ¿Qué tecnologías de identificación son necesarias para atender los requerimientos de seguridad en los puntos de acceso?
- ¿Cuáles empleados requieren nuevas funciones en la tarjeta de identificación? ¿Es conveniente reemplazar todas las tarjetas de identificación para mejorar la seguridad y añadir funciones a través de la organización o si solo se requieren nuevas tarjetas de identificación para un grupo de empleados?
- ¿Se cambiará el esquema de numeración o el formato de datos del sistema de identificación? ¿Cómo serán modificados los sistemas preexistentes para acomodar dichos cambios?
- ¿Hay nuevos requerimientos de seguridad que implicarán el reemplazo o actualizaciones de la arquitectura o de los componentes del sistema de acceso físico?

Consideraciones Claves de Migración

Algunas de las decisiones claves para la migración son con respecto a la selección de tecnologías de nuevas tarjetas y lectores y como deben ser manejados los sistemas de los formatos de información preexistentes.

Tarjetas de Tecnología Múltiple

Las tarjetas de identificación se componen de variados elementos, cada uno específica una circunstancia en particular, tales como:

- Impresión de la foto del portador
- Impresión del nombre del portador
- Código de Barra(s)
- Cinta magnética
- Cinta de débito
- Tecnologías múltiples sin contacto (125 KHz, 13.56 MHz)
- Tecnología de tarjeta inteligente de contacto
- Cinta óptica
- Relevo (embossing)
- Marcas de Seguridad¹³
- Panel de firmas
- Logo y dirección de la autoridad emisora de la tarjeta

El uso de tarjetas de tecnología múltiple puede ser parte de una estrategia de migración o la solución total. Al considerar una tecnología múltiple de tarjeta inteligente de identificación, es importante recordar que combinar un número pequeño de tecnologías de identificación compatibles puede ser una solución práctica, mientras otras combinaciones pueden ser imposibles o poco prácticas de implementar.

Las tarjetas de tecnología múltiple proveen una solución potencial en la medida que las tecnologías nuevas y preexistentes puedan cohabitar. Por ejemplo, un nuevo chip de proximidad preexistente de 125MHz puede cohabitar con un chip de tarjeta inteligente sin contacto de 13.56 MHz y las tecnologías no interferirán una con otra. La tecnología de tarjetas múltiples que respaldan tanto la tecnología 125KHz como una tecnología de 13.56 MHz las cuales están actualmente disponibles. De manera similar, las tecnología de tarjeta inteligente de contacto puede cohabitar con las tecnologías sin contacto de 125KHz y de 13.56 MHz.

¹³ Las marcas de seguridad pueden ser utilizadas para detener la manipulación y falsificación. Tecnologías tales como bordes ornamentales, micro texto, textos ultravioleta, hologramas, quinegramas, imágenes múltiples de láser y grabados con láser, son algunos ejemplos. A pesar de que incrementan los costos, las marcas de seguridad son requeridas si el riesgo de manipulaciones o falsificaciones son reales o percibidas como una amenaza.

Las tecnologías sin contacto (125KHz y 13.56 MHz) y tecnología de tarjeta inteligente de contacto pueden cohabitar con otras tecnologías de identificación, tales como, cintas magnéticas, códigos de barra y cintas ópticas. Tal tarjeta de tecnología múltiple puede ofrecer al usuario una credencial de identificación sencilla que es compatible con los sistemas instalados, a la vez que permite añadir nuevas tecnologías que estén disponibles.

Mientras sea posible mezclar varias tecnologías en una tarjeta, se deberá considerar con mucho cuidado su impacto general. Entre las limitaciones de las tarjetas de tecnología múltiple, se encuentran:

- Inclusión de múltiples tecnologías sin contacto que operan en la misma frecuencia. En general, las tarjetas no pueden incluir tecnologías múltiples sin contacto (125 KHz o 13.56 MHz) que operen en la misma frecuencia, porque interferirán entre si.
- Espesor de la tarjeta El estándar ISO/IEC 7810 define el espesor máximo permitido para una tarjeta. Las tarjetas de tecnologías múltiples deben cumplir con las especificaciones de espesor máximo. Caso contrario, los lectores de contacto que requieren que las tarjetas tengan cierto espesor, no podrán leer tarjetas de mayor espesor.
- Ubicación de relevo. Si el relevo es requerido, la localización del chip, la espiral de la antena, el alambre Wiegand o la localización de los datos ópticos debe ser tomada en cuenta, para que éstas no sean dañadas por el proceso de relevo. Los estándares ISO/IEC proveen soluciones para estos problemas potenciales.
- Costo de la tarjeta En teoría, las compañías pueden diseñar tarjetas para respaldar cualquier combinación de tecnologías sin contacto u otras. Sin embargo, en la práctica el costo y la complejidad de tales tarjetas pueden limitar la aceptación en el mercado. Las tarjetas de tecnologías múltiples complejas cuestan, invariablemente, más que la suma de sus partes.
- Fabricación y Disponibilidad de las tarjetas: Tarjetas de tecnología múltiples no estandarizadas podrán ser fabricadas, sin embargo, puede haber un largo periodo de espera hasta que el diseño del cuerpo de la tarjeta se cualifiquen los procesos de la tarjeta en conformidad con los procesos ISO/IEC. Si múltiples fabricantes están involucrados en suplir diferentes tecnologías puede haber problemas en las garantías de los fabricantes.
- Tasa de Fallas de la Tarjeta. Cada tecnología tiene el potencial de introducir posibles defectos (cosméticos o funcionales) durante la manufactura de la tarjeta, incrementando el riesgo de tener que deshacerse de la tarjeta. Además, cuanto mayor sea el número de tecnologías que tenga una tarjeta, mayor será el potencial de que la tarjeta tendrá una mayor tasa de fallas después de haber sido emitida. Una corta vida tiene un impacto en el costo total, que incluye no solamente el costo de reemplazo de la tarjeta, sino también los costos operacionales de la re-emisión de las tarjetas.

La combinación de un pequeño número de tecnologías de identificación compatibles dentro de una tarjeta sencilla es fácil y puede ser más costo-eficiente que combinar muchas tecnologías. Mientras las tarjetas de tecnologías múltiples pueden proveer soluciones para acomodar los sistemas de control de acceso preexistentes, las organizaciones deben considerar cuidadosamente la mayor complejidad de la implementación y mantenimiento de las múltiples

Tarjetas de Múltiple Aplicación

Las organizaciones pueden preferir la utilización de una tarjeta inteligente de una sola tecnología que pueda dar respaldo tanto a las tecnologías preexistentes como a las aplicaciones. Una tarjeta inteligente de aplicación múltiple puede permitir que cada tecnología de aplicación preexistente diferente almacene la información en su propia área, con sus propias claves de seguridad. Por ejemplo, un chip de una tarjeta inteligente de identificación sin contacto puede comunicarse con el lector usando 13.56 MHz, pero seguir utilizando los formatos y datos requeridos por el sistema de control de acceso de 125 KHz. Una tarjeta inteligente sencilla de contacto y sin contacto puede ser altamente deseada porque reduce los costos e incrementa la conveniencia.

Lectores de Tecnología Múltiple

El uso de un lector de tecnología múltiple es otro aporte a la migración. Lectores de tecnologías múltiples pueden leer más de una tecnología al mismo tiempo. El lector puede ser sencillo o complejo, dependiendo si las tecnologías pueden cohabitar. La interfase y el protocolo físico del lector hacia el panel de control es típicamente la misma tecnología para ambas tecnologías, pero los datos y el contenido no lo son.

Los Sistemas de control de acceso físico que usan múltiples tecnologías de radio frecuencia que operan en la misma frecuencia pueden ser combinadas de forma costo-efectiva en un solo lector. Por ejemplo, actualmente están disponibles lectores y chips de lector de tecnología múltiple que respaldan tanto ISO/IEC 14443 como ISO/IEC 15693.

Generalmente, lectores de tecnología múltiple que combinan tecnologías que usan diferentes radio frecuencias no son las soluciones ideales, debido a los elevados costos de los lectores y su limitada disponibilidad. Adicionalmente, como un nuevo lector tiene que ser instalado de cualquier forma, generalmente es más simple instalar el lector con la nueva tecnología y emitir nuevas tarjetas o usar tarjetas de tecnología múltiple que pueden tener interfase con ambos lectores. Sin embargo, dependiendo del número de tarjetas y lectores involucrados, hay escenarios de migración en que resulta práctico usar lectores que respaldan una variedad de tecnologías.

Cableado del Sistema de Control de Acceso

Un componente en los costos de migración que frecuentemente no se toma en cuenta es el reemplazo del cableado o los requerimientos para nuevos cableados. Muchos sistemas de control de acceso actuales usan una tecnología de solo lectura que requiere poco alambrado entre el lector y el panel. Si, nuevas funciones de control de acceso requieren un protocolo de comunicación de dos vías (por ejemplo, RS-232, RS-485 o TCP/IP) entre el lector y el panel, se necesitará un tipo diferente de cableado (por ejemplo, cableado categoría 5 o similar). Pasar un nuevo alambrado a través de un edificio puede ser costoso y, en algunos casos, imposible sin realizar mayores modificaciones al edificio.

Formatos de los Datos de Control de Acceso

Mover datos de la tarjeta de identificación de acceso físico con la vieja tecnología hacia la nueva tarjeta basada en chip, puede ser una consideración clave, dependiendo de cuantas tarjetas están involucradas y o si los portadores están geográficamente esparcidos. Un abordaje para mover datos es duplicar los datos de una tarjeta 125KHz a una tarjeta inteligente. Esta solución es particularmente atractiva porque los lectores de tarjetas inteligentes están disponibles con la misma interfase de salida como de los lectores de 125 KHz, así que los paneles del sistema de control de acceso no necesitarán ser reemplazado.

Nuevos sistemas de control de acceso pueden tener datos nuevos o nuevos formatos de datos que son incompatibles con los viejos sistemas preexistentes. Esto requerirá una estrategia de migración que emita nuevas tarjetas e incorpore nuevos lectores, paneles y funciones de servidores de control de acceso, que puedan entender el nuevo formato, pero que también consideren como los formatos preexistentes pueden ser respaldados durante la migración.

Conclusión

Esto es critico para una organización definir los objetivos a largo plazo para un nuevo sistema de identidad de acceso físico y desarrollar una cuidadosa estrategia y planificación de migración que implementa el sistema de forma lógica, conveniente, oportuna y costo-efectiva. La migración hacia una nueva tecnología de control de acceso puede ser económica y relativamente sin rodeos, si la mudanza es bien planificada.

Nuevas Aplicaciones Habilitadas por el Sistema de Tarjetas Inteligente

El usar tarjetas inteligentes permite a un sistema de control de acceso incluir aplicaciones que hacen más que autorizar el acceso físico. Tomando ventaja de las capacidades del chip de la tarjeta inteligente, las organizaciones pueden realizar una propuesta de negocio para la implementación de un nuevo sistema de control de acceso físico seguro e incrementar la habilidad de ese sistema para manejar futuras necesidades.

Esta sección describe tres aplicaciones que frecuentemente son implementadas en tarjetas inteligentes de aplicación múltiple, junto con control de acceso físico:

- Aplicaciones de control de acceso lógico (por ejemplo, para autenticación de computadoras o de red)
- Aplicaciones de pago
- Aplicaciones de almacenamiento de datos seguros

Aplicaciones de Control de Acceso Lógico ¹⁴

Así como las necesidades para una seguridad física se han incrementado, ha habido un incremento simultáneo en el requerimiento de una alta seguridad cibernética (por ejemplo, acceso seguro a recursos de la red de informática). Las noticias están repletas de ejemplos de rupturas de seguridad en la red, particularmente en el Internet, donde transacciones fraudulentas se han realizado e identidades han sido robadas por los “hackers”, quienes accesan bases de datos que contienen información personal. Una clara amenaza existe para la seguridad, tanto de redes corporativas como gubernamentales.

Para minimizar el riesgo del ataque de los “hackers” y rupturas de seguridad, ha habido un incremento en la implementación del diseño de tecnología para proveer un acceso seguro a los recursos de la red. Tales tecnologías pretenden ayudar a los operadores de red a controlar el acceso, haciéndolo disponible solamente para aquellos individuos a quienes el operador de la red desea dar dicho acceso. El acceso a la red es controlado por dos procesos: autenticación y autorización.

Autenticación es el proceso por el cual un individuo prueba que él o ella es la persona para quien la credencial fue emitida originalmente, por una tercera entidad de confianza, la cual confirma la identidad del individuo en primera instancia. Por ejemplo, si una identificación con fotografía es emitida a John Doe, luego John Doe se autentica, demostrando que su rostro corresponde con el rostro de la fotografía.

¹⁴ Los casos estudiados ilustrando el uso de tarjetas inteligentes para acceso lógico pueden ser encontrados en el web site de la Smart Card Alliance, www.smartcardalliance.org

La autenticación prueba que una persona es el individuo identificado por la credencial.

Autorización es el proceso por el cual se brinda acceso a los recursos a un individuo debidamente autenticado. Los derechos de acceso pueden ser otorgados de acuerdo a las jerarquías de los individuos dentro de la organización o los derechos de acceso pueden ser otorgados por el operador de la red.

La tecnología de tarjeta inteligente permite una variedad de mecanismos para respaldar la autenticación.

Protección a través de PIN/ Clave

Un esquema común para obtener autenticación involucra almacenar un PIN o clave en una tarjeta inteligente. Cuando un usuario desea obtener acceso a los recursos de la red (una computadora local, servidor, aplicación basada en Web o aplicaciones de una intranet/extranet), el usuario da entrada al PIN. El PIN introducido es comparado con el PIN almacenado en la tarjeta inteligente. Si él corresponde, el usuario es autenticado y puede acceder al recurso deseado. El servicio de control de acceso por PIN utiliza dos factores de autenticación para brindar un mecanismo relativamente simple para asegurar que la persona correcta está accediendo al recurso.

Para respaldar el servicio de control de acceso por PIN, paquetes de software están disponibles para permitir al usuario el manejo del PIN almacenado en la tarjeta. Por ejemplo, este software (algunas veces llamado "middleware") puede permitir que el PIN sea cambiado varias veces, inhabilitar el PIN en caso de que sea introducido de manera incorrecta una cierta cantidad de veces y desbloquear el PIN si es inadvertidamente inhabilitado.

Respaldo del PKI

Otras metodologías para habilitar la autenticación del usuario es usar certificados digitales que son emitidos como parte del PKI para proveer un identificador digital único (pasaporte digital) para cada usuario de manera individual.

Estos certificados y las llaves de las cuales ellos se derivan (que están almacenados en la memoria del chip de la tarjeta inteligente) pueden ser usados para realizar la operación de firma digital (después del proceso de registro diseñado para probar la identidad exacta de la persona a quién se está emitiendo el certificado). La operación, a través de criptografía, vincula a la persona portadora de la tarjeta inteligente con el certificado. Generalmente, el portador de una tarjeta de identificación inteligente usará un PIN o un factor biométrico para desbloquear la tarjeta para realizar la operación de firma digital solicitada.

Cada vez más los certificados están siendo usados para respaldar la autenticación a las redes del computador, donde el PKI está siendo

implementado. Por ejemplo, Windows ® 2000, Windows® (XP) y Windows® NT proveen un respaldo interno para un “logon” seguro por vía de certificados, (como emitidos por la “Microsoft Certificated Authority”). El Departamento de Defensa (DoD CAC) utiliza certificados separados para respaldar el “logon” a la red y la firma digital para el no rechazo (non-repudiation) de las transacciones.

Un chip de tarjeta inteligente puede almacenar claves privadas de forma segura. Las claves privadas son la mitad de los pares de llaves públicas-privadas que han sido creadas para proveer la función criptográfica que habilita las aplicaciones PKI, tales como las firmas digitales y los correos electrónicos encriptados. Además, algunos chips son diseñados para generar pares de llaves dentro de la propia tarjeta inteligente. Generar los pares de llaves dentro de la tarjeta agrega un nivel de seguridad a las llaves privadas, debido a que no tendrá que ser importada a la tarjeta desde otra fuente. La llave pública es enviada a la autoridad de certificación, donde el certificado es creado para distribución y enviada de vuelta a la tarjeta inteligente para su almacenaje seguro. .

Respaldo de Llave Simétrica (Claves de un solo uso “One Time Passwords

Algunas organizaciones pueden justificar la inversión a un sistema PKI, a una escala completa, no obstante, requieren un robusto proceso de autenticación para acceder a los recursos de la red. Se puede lograr una autenticación robusta con la utilización de llaves simétricas y manejo, dinámicas o estáticos de claves (password). En este escenario, un PIN es combinado criptográficamente con una llave secreta compartida (y potencialmente con otros datos tales como la hora o una fecha) para crear un código digital. El código es luego comparado con el código generado por el proveedor de servicio de red de un modo similar. Sí, los dos códigos concuerdan, el usuario autenticado.

Una tarjeta inteligente es capaz de almacenar de forma segura una llave secreta que puede ser usada para autenticar al usuario cuando la llave es comparada con la llave secreta que tiene el operador de la red. Este sencillo pareo de uno-a-uno provee cierto nivel de seguridad, ya que la tarjeta del usuario solo podrá contener la llave secreta cuando está es emitida por el operador de la red. La debilidad de este esquema es que si la llave secreta es comprometida, el usuario puede fácilmente ser despersonalizado. La efectividad de las llaves estáticas o claves (password) depende de la natural resistencia a la falsificación del chip de la tarjeta inteligente para proteger de los hackers la llave o la clave. Algunas organizaciones usan esquemas de “la rotación de llaves” o “versificación de llaves” (key versioning) para hacer más difícil que el sistema sea comprometido.

Un esquema auxiliar consiste en generar de forma dinámica una llave o clave. En este esquema, toda transacción tiene una llave diferente, la cual puede ser usada por ambos lados de la transacción para

garantizar la seguridad. Las tarjetas inteligentes pueden respaldar este proceso, usando el poder de computación del chip para crear la llave o clave dinámica..

Respaldo Biométrico

Otro uso de creciente importancia de la tarjeta inteligente es respaldar la autenticación basada en factores biométricos¹⁵. La tarjeta inteligente almacena información biométrica para un individuo, ante el cual el individuo es autenticado en tiempo real. Los chips de la tarjeta inteligente, dependiendo del tamaño de su memoria, pueden almacenar prácticamente cualquier tipo de información biométrica, ya sea como patrones digitales comprimidos (por ejemplo, huellas digitales en miniatura) o como una representación digital completa de la característica biométrica (una imagen digital).

Una autenticación biométrica requiere que el individuo provea características particulares biométricas únicas al dispositivo de lectura o escaneo. El dispositivo captura los factores biométricos y los compara con los factores biométricos almacenados dentro de la tarjeta. Si ellos hacen juego o pareo, el individuo es considerado autenticado.

El adicionar autenticación biométrica basada en tarjetas inteligentes puede elevar considerablemente el nivel de seguridad. Las tarjetas inteligentes respaldan autenticación de tres factores, aprovechándose de algo que el usuario tiene (la credencial de la tarjeta inteligente), algo que el usuario conoce (un PIN o una clave) y algo que el usuario es (una o más características biométricas). En algunos casos una característica biométrica puede ser usada para un proceso de autenticación de dos factores que brindan acceso más seguro a los datos en la tarjeta.

Los sistemas de acceso físico más recientes usan técnicas de pareo en la tarjeta (match on card), donde el lector captura una característica biométrica y la envía a la tarjeta. La tarjeta entonces compara la característica biométrica adquirida con la que está almacenada en la tarjeta y le dice al lector si la característica biométrica concuerda. Esto mejora aún más la seguridad de un sistema debido a que la característica biométrica original nunca queda expuesta y consecuentemente no puede ser capturada.

Resumen de Acceso Lógico

Una tarjeta inteligente de acceso físico puede ofrecer una autenticación robusta del usuario y de la tarjeta de identificación (usando firmas digitales, datos biométricos y tecnologías de clave/PIN), permitiendo el no rechazo de transacciones y correos

¹⁵ Para más información acerca de del uso de factores biométricos con tarjeteas inteligentes, ver Smart Card Alliance report, "Smart Cards and Biometrics in Privacy-Sensitive Secure Identification Systems," publicado en mayo del 2002.

electrónicos encriptados. Si esos beneficios son buscados por una empresa, como parte de su plan general de seguridad en red, los beneficios pueden ser cuantificados e incorporados en la propuesta de negocio (business case) general para adopción de tecnología de tarjetas inteligentes para respaldar tanto acceso físico como lógico.

Un creciente número de empresas tanto e el sector Público como privado están adoptando tarjetas inteligentes que respaldan acceso físico y lógico en una tarjeta. Por ejemplo, Microsoft está emitiendo un distintivo de empleado que no solamente abre puertas usando una interfase sin contacto, pero también respalda el “logon” más seguro a la red, usando una aplicación que se ubica en el chip de contacto inmerso en la tarjeta.

Actualmente, el mayor obstáculo para el desarrollo del mercado de tarjetas de identificación que respaldan tanto acceso físico como lógico es la separación histórica de seguridad física y seguridad en la red. Estas dos funciones generalmente se manejan en dos partes claramente diferentes de la organización, cada uno con una misión, presupuesto e infraestructura técnica separada. Sin embargo, en la medida que la tecnología se ha hecho más ampliamente disponible en una variedad de formas (por ejemplo, contacto, sin contacto, USB), más empresas están desarrollando propuestas de negocios que requieren la integración de estas dos funciones de seguridad para lograr ahorros de costos y mejorar la seguridad en toda la empresa.

Respaldo de Pagos

Una tarjeta inteligente que habilita control de acceso físico puede respaldar transacciones de pago, sea a través de una interfase de contacto o sin contacto. Un ejemplo es la tarjeta “SmarTrip”, una tarjeta inteligente sin contacto usada por el sistema de transporte WMATA. Los pasajeros cargan a la tarjeta una suma para pasajes, luego usan la tarjeta para tener acceso al subterráneo por sus entradas “turnstiles”, que simultáneamente deduce el monto del pasaje del monto almacenado en la tarjeta.

A la vez que está aplicación de la tecnología de tarjetas inteligentes ha sido introducida como pionero en el ambiente del transporte, donde la combinación de pago seguro con control de acceso físico rápido son requerimientos claves, pagos respaldados por tarjetas sin contacto están comenzando a aparecer en el sector general de venta al detal en los Estados Unidos. Los programas pilotos de Master Card PayPass y American ExpressPay usan tecnología sin contacto para realizar transacciones seguras de pago con tarjeta de crédito.

Los pagos pueden ser respaldados por un chip de contacto dentro del cuerpo de la misma tarjeta en que está el chip sin contacto usado para acceso físico. Actualmente chips de contacto pueden respaldar una gran variedad de aplicaciones de pago, desde bolsas

electrónicas en la cual un valor monetario puede ser almacenado hasta transacciones convencionales de crédito y débito. Una especificación global llamada EMV ha sido creada para que tarjetas inteligentes puedan respaldar transacciones de crédito y de débito basadas en chips de la misma forma que tarjetas con cintas magnéticas lo hacen actualmente.

Una aplicación de tarjetas inteligentes, que originalmente fue diseñada para respaldar control de acceso físico, también puede incluir una aplicación adicional para respaldar una amplia gama de funciones de pago. La combinación de estas funciones podría resultar en una propuesta de negocios más convincente para la adopción de tecnología de tarjetas inteligentes. Por ejemplo, el banco de una empresa podría proveer una tarjeta inteligente corporativa a sus empleados que podría incluir la aplicación de pago del banco, así como un chip sin contacto usado para acceso físico a los establecimientos de la empresa. En este caso, la empresa podría potencialmente obtener beneficios financieros por no tener que correr dos programas de tarjetas separadas, y el banco podría potencialmente asumir parte del costo de manejar el programa de acceso físico.

Un escenario más probable (y uno que ya ha sido implementado en varios colegios y compañías) es lo que se ha llamado “tarjeta de campus” (campus card). La tarjeta de campus es una tarjeta inteligente de aplicación múltiple que puede ser usada como una tarjeta de identificación (incluyendo una foto) y también usada para pagar por comida y máquinas vendedoras, abrir puertas del dormitorio, retirar libros de la biblioteca y pagar llamadas telefónicas. Generalmente estas tarjetas utilizan una variedad de tecnologías como cintas magnéticas, código de barras y un chip de tarjeta inteligente que respalda una amplia gama de aplicaciones funcionales. La mayoría de las implementaciones respaldan control de acceso físico en combinación con aplicaciones de pago y una variedad de otras aplicaciones, las cuales le añaden valor a la tarjeta.

Almacenamiento seguro de Datos

Cuando se junta la habilidad de la tecnología de tarjetas inteligentes de ofrecer almacenamiento de datos seguros y portátiles con la capacidad de computación del chip, el resultado final es un dispositivo portátil y distribuido de computación que puede respaldar una amplia variedad de aplicaciones con seguridad. Las únicas restricciones técnicas son el tamaño físico del chip y la cantidad de memoria disponible.

Por esta razón, las tarjetas inteligentes están siendo usadas en una cantidad de formas innovadoras, respaldando funciones que envuelven almacenamiento portátil seguro de información sensible y no sensible. Por ejemplo, registros médicos pueden ser almacenados en una tarjeta inteligente de tal forma que solo el portador de la

tarjeta o el médico del portador de la tarjeta pueden tener acceso a los registros. El acceso a los registros es típicamente protegido con algún tipo de lógica de control de acceso como un PIN.

De forma similar, la tarjeta CAC del Departamento de Defensa (DoD CAC) que está siendo emitida para el personal militar, incluye varias aplicaciones de almacenamiento seguro que guarda información personal sobre cada portador. La tarjeta CAC puede almacenar potencialmente información relacionada a la historia médica u otros datos relevantes a la misión de la persona.

Las tarjetas sin contacto usadas para sistemas de acceso físico pueden almacenar con seguridad información que rastrea el uso de la tarjeta. Por ejemplo, una tarjeta sin contacto puede ser usada para registrar cuando el portador de la tarjeta entra a un edificio en particular (por ejemplo, la localización de la puerta, la hora, la fecha) para luego ser recobrada y auditada. Esa función puede ser manejada por la tarjeta o por un servidor central, dependiendo de los requerimientos o infraestructura de la empresa.

Sumario

La propuesta de negocio en apoyo a la adopción de tarjetas inteligentes para control de acceso físico puede ser dramáticamente reforzada por la identificación de características y funciones adicionales respaldadas por una plataforma de tarjetas inteligentes. La funcionalidad adicional puede usar una interfase sin contacto que respalde acceso físico, un chip e interfase adicional sin contacto dedicado a una aplicación diferente, o un chip de contacto adicional incluido en el cuerpo de la tarjeta inteligente.

Por lo tanto, cualquier desarrollo de un programa de tarjetas inteligentes debe incluir un análisis de otras funciones que pueden apuntalar la inversión en tarjetas inteligentes. Con este proceso una empresa puede descubrir beneficios adicionales de migración hacia una tecnología de tarjetas inteligentes que podrían resultar en un ahorro general para la empresa a la vez que aumentaría la conveniencia para el usuario y simplifica los procesos del negocio..

Conclusión

Actividades significativas están siendo desarrolladas tanto por el gobierno como por la industria para implementar nuevos sistemas de control de acceso para verificar la identidad y los privilegios de una persona antes de brindarle acceso físico (hacia un edificio o lugar) o acceso lógico (a información u otros recursos en línea). Son requerimientos claves para estos sistemas tener un control de acceso más seguro, una mejor conveniencia para el usuario, procesos de verificación de identidad más simples y menores costos generales de gestión y administración.

Muchas agencias del Gobierno Federal están implementando sistemas de control de acceso físico y lógico basados en tarjetas inteligentes, cuyos esfuerzos están enfocados a la implementación de tecnología con base en estándares. Como parte de este esfuerzo, iniciativas a través de varias agencias de gobierno manejadas por el GSA y NIST han guiado la definición de especificaciones para interoperabilidad entre las implementaciones del gobierno. Empresas comerciales, como Sun y Microsoft, están ahora implementado sistemas de control de acceso basados en tarjetas inteligentes para manejar el acceso global de los empleados a los recursos corporativos.

El diseño de un sistema de acceso físico seguro incluye consideraciones que van más allá de la selección del credencial y del lector. El diseño de un sistema adecuado requiere una definición completa de los requerimientos del sistema, incluyendo la funcionalidad requerida y la política de seguridad, y debe tomar en cuenta factores como costo, los requerimientos para integrarse y migrar de sistemas preexistentes y el efecto de la implementación sobre los usuarios y la organización.

Tecnologías de tarjetas inteligentes sin contacto y de contacto están siendo usados en sistemas de control de acceso. La tecnología de tarjetas inteligentes ofrece muchos beneficios a un sistema de control de acceso

- Alta velocidad de acceso y costos de mantenimiento reducidos para control de acceso físico sin contacto.
- Seguridad robusta respaldando autenticación de múltiples factores y una variedad de técnicas de autenticación e encriptación.
- Flexibilidad para incorporar múltiples aplicaciones y apoyar múltiples tecnologías de tarjetas y lectores.
- Establecimiento de soluciones basadas en estándares ofreciendo una solución de componentes interoperativos y disponibilidad de tarjetas y lectores de múltiples vendedores.

La convergencia de las necesidades del gobierno y del sector comercial y la disponibilidad de soluciones seguras de tarjetas

inteligentes basadas en estándares están llevando a la implementación de sistemas de control de acceso basadas en tarjetas inteligentes. La tecnología de tarjetas inteligentes permite que el sistema de control de acceso pueda implementar mecanismos de verificación de identidad más seguros tanto para acceso físico como lógico y brindar una plataforma tecnológica para añadir nuevas aplicaciones que mejoren aún más la conveniencia del usuario y simplifique los procesos del negocio.

Para mayor información sobre tarjetas inteligentes y el papel que tienen las aplicaciones de identificación segura y otras, favor visitar el sitio web de la Smart Card Alliance en www.smartcardalliance.org o contactar directamente al Smart Card Alliance al 1-800-556-6828.

Referencias y Recursos

"Access Control Technologies for the Common Access Card," a study by the Security Equipment Integration Working Group (SEIWG), April 2002

"Amex Opts for Biometric RFID Card," *RFID Journal*, February 17, 2003

"Building Blocks of the U.S. Smart Card Market," *Card Technology*, May 2003

"California Independent System Operators (CalISO) secures access to electric power grid control with smart cards and PKI," Smart Card Alliance case study

"Contactless Smart Card Technology for Physical Access Control," Avisian, Inc. report, April 1, 2002

"Contactless Technology for Secure Physical Access: Technology and Standards Choices," Smart Card Alliance report, October, 2002

"Department of Defense to issue 13 million Common Access Cards," Smart Card Alliance case study

"Dutch bank deploys 33,000 smart cards to authenticate internal users and secure online transactions," Smart Card Alliance case study

"Federal Deposit Insurance Corporation deploys smart cards and PKI to internal staff and field agents," Smart Card Alliance case study

"Microsoft employees to use smart card access controls," Paul Roberts, *IDG News Service/Boston Bureau*, www.idg.net, September 23, 2002

"Navy's DENCAS system centralizes dental records and secures access with smart cards and PKI," Smart Card Alliance case study

"A Primer to the Implementation for Smart Card Management and Related Systems," Global Platform, www.globalplatform.org

"Physical Security Bridge to IT Security," Open Security Exchange, www.opensecurityexchange.com

"Schlumberger/SEMA deploys 89,000 smart cards and PKI to protect corporate and customer data," Smart Card Alliance case study

"Shell Group's info security centers around 85,000 smart cards with PKI and single sign-on for smart card-enabled PKI," Smart Card Alliance case study

“Smart Cards and Biometrics in Privacy-Sensitive Secure Identification Systems,” Smart Card Alliance report, May, 2002

Reconocimientos

Este informe fue desarrollado por la Smart Card Alliance para brindar un manual sobre sistemas de identificación de acceso físico seguro y para discutir como estos sistemas están migrando hacia la tecnología de tarjetas inteligentes. La publicación de este documento por la Smart Card Alliance no implica el endoso de 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. Participantes de 28 organizaciones, tanto públicas como privadas se involucraron en el desarrollo de este informe incluyendo: ACI Worldwide, ActivCard, ASSA ABLOY ITG, Bell ID, Datacard Group, eID Security, EDS, Gemplus, Hitachi America Ltd., Honeywell Access Systems (OmniTek), IBM, ISR Solutions, LaserCard Systems, MasterCard International, MGM Security Consulting, NASA, Northrop Grumman Information Technology, SC Solutions, Schlumberger, SCM Microsystems, Smart Commerce Inc., Transportation Security Administration, Unisys, U.S. Dept. of Defense, U.S. Dept. of Homeland Security, U.S. Dept. of State, U.S. Dept. of Transportation/Volpe Center, XTec Incorporated.

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

Tim Baldrige, NASA	Bob Merkert, SCM Microsystems
Dovell Bonnett, ASSA ABLOY ITG	Dwayne Pfeiffer, Northrop
Kirk Brafford, ActivCard	Grumman Information Technology
Joe Broghamer, U.S. Dept. of Homeland Security	Tate Preston, eID Security
Mike Davis, Honeywell Access Systems (OmniTek)	J. C. Raynon, SCM Microsystems
Mike Dinning, U.S. Dept. of Transportation/Volpe Center	James Russell, MasterCard International
Kevin Kozlowski, XTec Incorporated	James Sharp, Transportation Security Administration
Lolie Kull, U.S. Dept. of State	Randy Vanderhoof, Smart Card Alliance
Philip Lee, SC Solutions	Mike Vermillion, EDS
Mark McGovern, MGM Security Consulting	Tim Weisenberger, U.S. Dept. of Transportation/Volpe Center
John McKeon, IBM Ltd.	Chuck Wilson, Hitachi America Ltd.
Cathy Medich, Consultant and Task Force Chair	.

Derecho de Autor (Copyright Notice)

Copyright 2003 Smart Card Alliance, Inc Todos los derechos reservados

Marcas Registradas (Trademark Notices)

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

Apéndice A: Definición de Términos y Siglas

Formato de sistema de control de acceso

El formato de sistema de control de acceso se refiere al patrón bit que el lector transmite al panel de control. El formato especifica cuantos bits forman el flujo de datos y lo estos bits representan. Por ejemplo, los primeros bits pueden transmitir el código del establecimiento los siguientes un número de identificación único, los próximos paridad, y así en adelante.

AES

Advanced Encryption Standard. (Patrón avanzado de criptografía)

Barium ferrite

Tecnología magnética que usa barium ferrite en la composición de la credencial de identificación para almacenar datos y hacer que los datos estén disponibles para el dispositivo de lectura.

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 de comportamiento únicas.

CCTV

Closed Circuit Television.(Circuito cerrado de Televisión)

Chip

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

Cohabitar

Es la habilidad de que múltiples tecnologías residan en la misma tarjeta y no interfieran una con la otra (por ejemplo, una tarjeta de tecnología múltiple).

Tarjeta Inteligente 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).

Tarjeta Inteligente 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.

Panel de Control

Es el componente del sistema de control de acceso que se conecta a todos los lectores de puerta de acceso, cerraduras de puerta y el servidor de control de acceso. El panel de control valida el lector y acepta los datos. Dependiendo del diseño general del sistema, el panel de control puede enviar los datos al servidor de control de

acceso o puede tener suficiente inteligencia local para determinar los derechos del usuario y dar la autorización final de acceso. El panel de control puede ser llamado de controlador o panel

Credencial

El dispositivo de identificación general (tanto el dispositivo físico como los datos contenidos en él). Comúnmente se le conoce como la “ficha de identificación” (ID token) en los sistemas de control de acceso físico.

DES

Data Encryption Standard. (Patrón de Criptografía de Datos)

Lector de puerta de acceso

Es el dispositivo en cada puerta que se comunica con una tarjeta o credencial de identificación y envía datos de la tarjeta al panel de control para decidir sobre los derechos de acceso.

Cerradura Electrónica (Door strike)

Cerradura electrónica en cada puerta que está conectada al panel de control.

DSA

Digital Signature Algorithm. (Algoritmo de firma digital)

Tarjeta de interfase dual

Una tarjeta de identificación que tiene un único chip de tarjeta inteligente con dos interfase - un interfase de contacto y un interfase de contacto - usando memoria y recursos del chip compartido.

Campo de recepción

Es el campo de radio frecuencia o electromagnético transmitido constante por el lector de puerta sin contacto. Cuando una tarjeta sin contacto está en el radio de acción del campo de recepción, la antena interna de la tarjeta convierte el campo de energía a electricidad que da energía al chip. El chip entonces usa la antena para transmitir datos al lector.

ECC

Elliptic Curve Cryptography. (Criptografía de curva elíptica)

EMV (Europay MasterCard Visa.)

Especificaciones desarrolladas por Europay, MasterCard y Visa que define un conjunto de requerimientos que aseguran la interoperabilidad entre tarjetas con chip de pago y los terminales.

FCC

Federal Communications Commission. (Comisión Federal de Comunicación)

FIPS

Federal Information Processing Standard. (Patrón Federal de Procesamiento de Información)

GSA

General Services Administration. (Administración de Servicios Generales)

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

Una próxima revisión del GSC-IS (manejada por el NIST) incluirá definiciones de interoperabilidad para tecnologías de tarjetas inteligentes sin contacto.

Sistema de cabeza de Red (Head-end system)

Es el servidor de control de acceso, el software y las bases de datos usados en un sistema de control de acceso físico.

Tarjeta Híbrida (Hybrid card)

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

IDEA

International Data Encryption Standard. (Patrón Internacional de Criptografía de Datos)

IEC

International Electrotechnical Commission. (Comisión Internacional Electro Técnica)

Circuito Integrado

Ver chip.

ISO

Organización Internacional de Estándares

ISO/IEC 14443

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

ISO/IEC 15693

Estándar ISO/IEC para "Tarjetas de Identificación – Tarjetas con Circuitos Integrados sin contacto- Tarjetas de Vecindario (Vecinity Cards)".

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).

MCU

Ver microcontrolador.

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.

Migración

Es el movimiento planificado e incremental de un sistema de control de acceso físico existente hacia un sistema basado en tarjetas inteligentes.

Tarjeta de Aplicación Múltiple

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

Lector de Múltiples Factores

Es un lector de tarjetas inteligentes que incluye un teclado de PIN, un lector biométrico o ambos para permitir autenticación de múltiples factores.

Tarjeta de Tecnología Múltiple

Es una tarjeta de identificación que tiene dos o más tecnologías de identificación que son independientes y que no interaccionan o que no interfieren uno con el otro. Un ejemplo es una tarjeta que contiene un chip de tarjeta inteligente y una cinta magnética.

Lector de Tecnología Múltiple

Es una tarjeta de lecto/escritura que puede acomodar más de una tecnología de tarjeta en el mismo lector (por ejemplo, tecnologías de tarjetas sin contacto tanto ISO/IEC 14443 como ISO/IEC 15693 o tecnologías sin contacto tanto de 13.56 MHz como 125 kHz).

NIST

National Institute of Standards and Technology. (Instituto Nacional de Patrones y Tecnología)

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).

Radio de acción operacional (Operational range)

Es la distancia del lector en el cual la credencial de identificación sin contacto es efectiva.

PC

Personal computer.

Acceso Físico

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

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.

PKI

Public Key Infrastructure. (Infra estructura de llave Pública).

RF

Radio frecuencia.

RFID

Radio Frequency Identification. (Identificación de Radio Frecuencia)

RSA

Se refiere a la tecnología de encriptación de llave pública/privada que utiliza un algoritmo desarrollado por Ron Rivest, Adi Shamir y Leonard Adleman y que es propiedad y bajo licencia de RSA

Tarjeta Inteligente

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 interaccionar inteligentemente con el lector de tarjeta inteligente.

Tarjeta de Identificación Inteligente (Smart ID card)

Una tarjeta de identificación que es una tarjeta inteligente.

3DES

Triple DES.

UL

Underwriters Laboratories. (Laboratorios Suscritos)

USB

Universal Serial Bus. (Barra Serial Universal)

Tecnología Wiegand

Tecnología Wiegand es ampliamente usada para aplicaciones de acceso físico e incluye una interfase, una señal, un formato de 26 bits, un efecto electromagnético y una tecnología de tarjeta. Una cinta Wiegand es la implementación de la tecnología Wiegand.

Lógica Cableada (Wired logic)

Es una tarjeta sin contacto que tiene un circuito electrónico que esta diseñada para una función específica (por ejemplo, seguridad, autenticación) sin un MCU.