



Tarjetas Inteligentes y Sistemas de Identificación Seguros: Construyendo una Cadena de Confianza

Un informe de la Smart Card Alliance Latin America (SCALA)

Fecha de Publicación: julio 2005

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) .

La Smart Card Alliance Latin para América Latina (SCALA) es la asociación sin fines de lucro, líder, 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, acceso físico, transportación, tecnología, servicios de salud, industria de venta al detal 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 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

Reconocimientos

Este informe está basado en el contenido del reporte de la Smart Card Alliance Latin America, (Alianza de Tarjetas Inteligentes), "Sistemas de Identificación Seguros: Construyendo una Cadena de Confianza," que fue desarrollado por los miembros del equipo de trabajo del Sistema de Identificación Personal Segura de la Smart Card Alliance (Alianza de Tarjetas Inteligentes), publicado en marzo del 2004. La publicación de ese informe por Smart Card Alliance (Alianza de Tarjetas Inteligentes), no implica endoso de ninguna de las organizaciones miembros de la Alianza.

La Smart Card Alliance (Alianza de Tarjetas Inteligentes), desea agradecer a los miembros del equipo de trabajo del departamento de Sistema de Identificación Personal Segura de la Smart Card Alliance, por sus contribuciones. Participantes de 23 organizaciones estuvieron involucrados en el desarrollo del reporte original, entre los cuales se encuentran: ActivCard, Alegria Technologies, AOS Hagenuk, ASSA ABLOY ITG, Atmel Corporation, Gemalto, BearingPoint, Datakey, Datatrac Information Services, Inc, EDS, eID Security, Gemplus, IBM, Identix, Infineon Technologies, LaserCard Systems, Lockheed Martin, MartSoft Corporation, Northrop Grumman Information Technology, Philips Semiconductors, Smart Commerce, Inc., Unisys, U.S. General Service Administration.

Copyright © 2005 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, pero 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.

Introducción

Seguridad es actualmente uno de los requerimientos de mayor demanda en nuestra sociedad. El desafío es simple: como proteger lo que le pertenece a usted. "Usted puede ser un administrador, agencia gubernamental, o una persona particular. Lo que le pertenece puede ser un bien tangible, como un objeto físico, o un bien intangible, como información, derechos o privilegios. Pero en todos los casos, tales bienes tienen un valor significativo para sus propietarios.

Prácticamente todo aquello contra lo cual un bien requiere ser protegido involucra a las personas. Los ataques físicos y digitales son todos creados y ejecutados por personas. Por lo tanto, es esencial ser capaz de identificar con claridad y con exactitud aquellas personas que deban tener acceso a las cosas que le pertenecen a usted y permitirle solo a éstas el acceso. Todos los demás deben ser rechazados. Tal capacidad de identificación es ejecutada por medio de un sistema de identificación (ID) seguro.

Esencial para la seguridad de un sistema de identificación es la cadena de confianza. Confianza en los procesos, personas, arquitectura y tecnología es vital para construir y lograr la credibilidad en un sistema de identificación que sea seguro. La cadena de confianza garantiza la autenticidad de las personas, organizaciones emisoras, dispositivos, equipamiento, redes y todos los otros componentes del sistema de Identificación seguro. La cadena de confianza, debe también asegurar que la información dentro el sistema sea verificada, autenticada, protegida y usada correctamente.

El uso de equipos inteligentes de Identificación, especialmente en el formato de tarjetas inteligentes, ofrece ventajas; tanto para la seguridad física, como lógica. Las tarjetas inteligentes son un vínculo vital en la cadena de confianza. Ellas proveen seguridad y exactitud en la verificación de la identidad y cuando es combinada con otros sistemas tecnológicos de identificación (tales como certificados biométricos y digitales), pueden aumentar la seguridad del sistema y proteger la privacidad de la información en el sistema.

El poder y la portabilidad de la tarjeta inteligente, con un buen diseño del sistema y procedimientos operativos estrictos, se combinan para formar una cadena confiable y controlable, logrando sistemas de identificación seguros.

Lo que hace que un Sistema de Identificación sea Seguro

Un sistema de Identificación seguro, está diseñado para atender un requerimiento fundamental, que es el de verificar que un individuo realmente es quién reclama ser. Cuando es adecuadamente diseñado, el sistema de identificación implementa una cadena de confianza, asegurando a todos y cada uno de los involucrados que el individuo que presentó la tarjeta de identificación es el propietario de las credenciales que están en la tarjeta y que dichas credenciales son válidas. (El término “credencial” en este informe se refiere a la información almacenada en la tarjeta que representa el documento de identidad del individuo y sus privilegios). Un sistema de identificación seguro, le brinda a los usuarios credenciales que son de entera confianza y que pueden ser usadas para una amplia gama de aplicaciones, desde permitir acceso a facilidades o redes, hasta proveer autorización para servicios o realizar transacciones en línea.

La tarjeta de Identificación.¹ es un factor crítico para cualquier sistema de Identificación seguro. La tarjeta de identificación es usada como una representación portátil, confiable y verificable de la identidad del poseedor y de los derechos y privilegios que tiene dentro del sistema de identificación. Para que la tarjeta de identificación cumpla con estos requerimientos, el sistema de identificación debe asegurar que una autoridad legítima fue la que emitió la tarjeta y que el documento de identificación y credenciales que están contenidas en la misma, no son falsificadas, ni alteradas y que la persona que porta la tarjeta de identificación corresponde a la persona que está adscrita al sistema de información.

El Modelo de Confianza del Sistema de Identificación Seguro

Los Sistemas de Identificación seguros, pueden ser implementados para grupos en particular, para varios grupos dentro de una organización o empresa o para múltiples organizaciones o empresas. Independientemente, del número o tipo de entidades que se vean involucradas; para que sean, realmente seguros, los sistemas de identificación deben implementar un modelo de confianza. Este modelo confiable institucionaliza principios y políticas aceptadas universalmente: que las operaciones del sistema siempre tengan el mismo resultado, independientemente de donde sean realizados y todos los participantes involucrados pueden confiar de que el sistema verificará con precisión y seguridad su identidad. Antes de implementar cualquier sistema, todas las entidades participantes en un sistema de identificación deben definir y acordar un modelo de confianza.

Elementos de Diseño para hacer un Sistema de Identificación Seguro

El diseño de un sistema de identificación seguro requiere una serie de decisiones para seleccionar e implementar políticas, procedimientos, arquitectura, tecnología y personal idóneo. El diseño debe implementar el nivel deseado de seguridad y una adecuada cadena de confianza, con un proceso de autenticación que incorpora medidas de seguridad y tecnologías apropiadas para evitar personificación, falsificación y asegurar la privacidad de las credenciales que están en el documento de identificación.

¹ Este informe se refiere al dispositivo de Identificación física como un “ID” o una “Tarjeta ID”. Aunque los sistemas de identificación utilizan diferentes formatos físicos de identificación, las tarjetas plásticas que incorporan otras tecnologías usadas para aplicaciones de identificación (e.g., chip, códigos de barra, tiras magnéticas) es el formato prevaleciente para un sistema de identificación seguro.

El diseño de un sistema de Identificación seguro debe incluir lo siguiente:

- Un proceso de registro seguro que establezca la entidad de cada individuo y que determine que la persona está autorizada para utilizar los privilegios o servicios que están siendo brindados.
- Procedimientos para emitir tarjetas de identidad con seguridad y asegurar que los documentos de identidad sean emitidos solamente por organizaciones autorizadas para expedir dichas tarjetas y que solamente sean emitidos documentos de identidad para las personas correctas.
- Políticas y procedimientos para monitorear el uso de la Identificación.
- Procedimientos para manejar el ciclo de vida de la identificación
- Entrenamiento para usuarios y emisores de tarjetas.
- Políticas, procedimientos y tecnologías que protejan el acceso a la información acerca de los portadores de identidad en el sistema.
- Controles de seguridad que provean acceso a la información contenida en el documento de identificación solamente a observadores debidamente autorizados para ello.
- Un proceso de autenticación que implemente la cadena de confianza previamente establecida, verificando la identidad de los portadores de la identidad y la legitimidad de las tarjetas de identidad y sus credenciales.

Requerimientos de Privacidad para Sistemas de Identificación Seguro

Además de proteger los bienes de las organizaciones, los Sistemas de Identificación seguros, deben también proteger la privacidad de los individuos registrados en el sistema y salvaguardar su información personal. Los requerimientos de privacidad son un aspecto clave para la implementación exitosa de un Sistema de Identificación seguro. Para que un Sistema de Identificación sea considerado como habilitado para una adecuada privacidad debe cumplir los siguientes requisitos:

- Controlar la recolección, uso y liberación de la información personal.
- Proteger el derecho de cada individuo de controlar como su información personal es colectada y promulgada.
- Proteger contra robo de identidad y el uso de la información personal de un individuo para propósitos fraudulentos.
- Proteger la confidencialidad, integridad y disponibilidad de la información que identifica o de otra forma describe a un individuo.

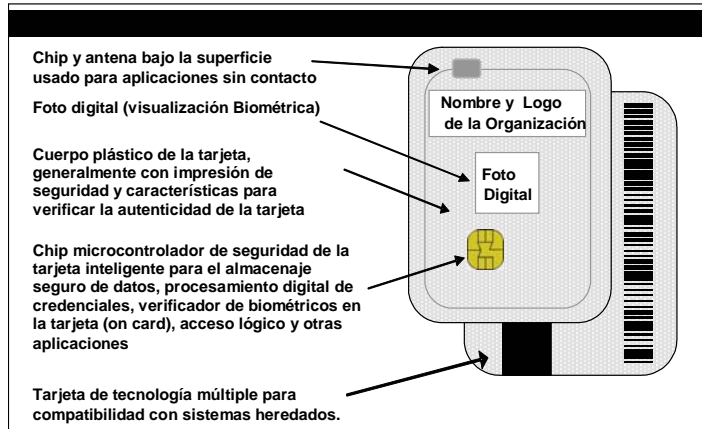
Un gran número de organizaciones gubernamentales y de grupos de la industria han desarrollado recomendaciones para llevar a cabo prácticas o procedimientos justos en el manejo de la información y pautas para proteger la privacidad individual. Los diseñadores de sistemas necesitan considerar las prácticas del negocio, las políticas de seguridad y las arquitecturas del sistema; así como, las tecnologías en el desarrollo de un sistema que garantice la privacidad.

Tarjetas Inteligentes y Sistemas de Identificación Seguros

Las Tarjetas Inteligentes son ampliamente reconocidas como una de las formas más seguras y confiables de identificación electrónica. Una Tarjeta Inteligente incluye un chip de computador agregado a la tarjeta, que puede ser un micro controlador con una memoria interna o una memoria externa solamente. La tarjeta puede ser conectada al lector, ya sea directamente por contacto físico o de forma remota, a través de una interfase electromagnética. Al tener un micro controlador agregado, las tarjetas inteligentes tienen la habilidad única de almacenar enormes cantidades de datos, realizar sus propias funciones en la misma tarjeta (por ejemplo,

encriptar y hacer firmas digitales) e interaccionar inteligentemente con el lector de la tarjeta inteligente.

La tarjeta de identificación inteligente puede combinar varias tecnologías de identificación; incluyendo el chip, marcas de seguridad visual, tiras magnéticas, códigos de barra y/o tiras ópticas.



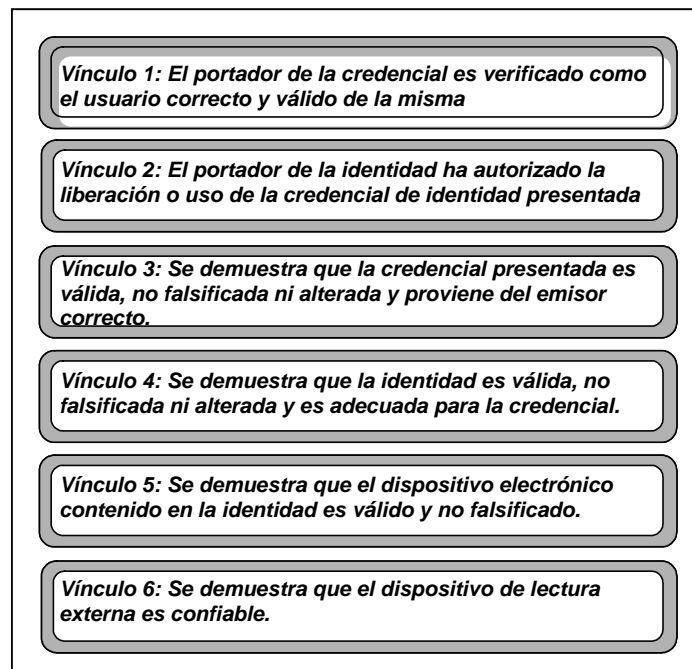
Muchas organizaciones de gobierno y empresas están implementado sistemas de identificación segura, basado en tarjetas inteligentes, para acceso físico y lógico, agregando otras aplicaciones que tradicionalmente han requerido procesos y tarjetas de identificación separadas.

Uso de la Identificación, la Cadena de Confianza y el Rol de las Tarjetas Inteligentes

La cadena de confianza para un sistema de Identificación seguro abarca todos los componentes y procesos, asegurando que el sistema como tal es merecedor de confianza.

Esta sección describe la cadena de confianza que se requiere para autenticar la identidad individual y asegurar la validez de la identificación y credencial una vez que la identificación ha sido emitida y se encuentra en uso. Con el fin de ilustrar una cadena de confianza que sea la más fuerte posible, está discusión asume que la identificación incluya un dispositivo electrónico (o chip) agregado en un documento personal portátil (por ejemplo, un pasaporte electrónico) o en una tarjeta.

La figura inferior presenta un resumen de los vínculos claves de la cadena de confianza del sistema de identificación seguro, durante el proceso de autenticación, cuando el documento de identidad es usado.



Verificación Física de la Identidad

La autenticación de la identidad comienza con la verificación de la identidad física misma. Las identidades pueden ser verificadas de diferentes formas. El método seleccionado debe ser apropiado para el nivel de confiabilidad requerido. Tales métodos incluyen:

- Examen de una identidad que es portada por el usuario, pero que no requiere ser entregada al que la examina (tal como los pases interinos "Flash Pass").
- Examen de una identidad que es entregada por el usuario.
- Inspección por una máquina de datos característicos únicos almacenados sobre o dentro del dispositivo de identidad (tal como un código de barras) o la comparación de una identidad con un patrón de referencia establecido.

En todos los casos, la Identidad presentada es revisada visual o electrónicamente con detalles específicos que indican su autenticidad. Los detalles pueden tomar la forma de una o más características de seguridad, tales como:

- Información topográfica correcta.
- Validación visual de la fecha de expiración
- Impresión de seguridad (por ejemplo micro-impresión)
- Dispositivos de seguridad óptica incluidos en la tarjeta, tales como hologramas y dispositivos de variabilidad óptica o tintas con variabilidad óptica o tintas ultravioleta
- Laminado de seguridad sobre la información impresa
- Construcción correcta
- Fotografía del portador del documento
- Medios pasivos que pueden ser leídos por una máquina (por ejemplo, códigos de barra o características ópticas)

Autenticación del Dispositivo de Identificación

Para asegurar que el dispositivo electrónico usado en la identificación presentada es el autorizado y no fraudulento, el dispositivo es autenticado electrónicamente usando claves secretas simétricas compartidas, claves públicas/privadas asimétricas o una clave de autenticación de un solo uso (OTP). La verificación electrónica se logra usando un dispositivo que pueda "leer" la identificación. El proceso de autenticación puede lograrse entre la identificación y el lector o puede requerir que el lector se comuniquen con un sistema de base o un servidor de autenticación.

Autenticación de Dispositivo usando una Clave Secreta Simétrica Compartida. Para autenticar una identificación usando una clave secreta simétrica compartida, tanto el dispositivo del documento de identificación como el lector deben conocer una clave secreta en común (compartida). El lector presenta una señal que solicita una contraseña al dispositivo que debe ser encriptada de alguna manera con la clave secreta compartida. El resultado es enviado del dispositivo que está en el documento de identificación al lector y es verificado contra un cálculo independiente hecho por el lector que recibió la señal. Si, los resultados coinciden, se asume que la identificación es auténtica. Una variación de este proceso es agregar códigos de autenticación de mensajes (MACs) a todos los mensajes; estos códigos proveen la más alta autenticación posible cuando el MAC es computarizado en tiempo real basado en una señal que requiere contraseña por el lector.

Autenticación del dispositivo usando claves asimétricas públicas/privadas. Este mecanismo se fundamenta en dispositivos de identificación que generan una clave par pública/privada asimétrica, con la porción pública disponible a todos los interesados que necesiten verificar la autenticidad del dispositivo. Cuando el lector desea validar la identidad, puede presentar una señal que requiere contraseña para que el dispositivo digitalice su firma usando su clave privada. Cuando el dispositivo regresa la firma corroborada, el lector puede verificar la firma digital del dispositivo usando la clave pública del dispositivo. Una variación de esta técnica requiere que la Identificación firme un bloque de datos o un mensaje, el cual es transmitido al equipo externo en tiempo real.

Claves de un solo uso (One Time Password - OTP). Las claves de un solo uso sirven como credenciales de autenticación dinámica que tienen un tiempo de vida muy limitado para prevenir ataques estáticos comunes basados en claves. Autenticaciones basadas en OTP (claves de un solo

uso) viene en dos formatos—o sincronizados, en el cual tanto el dispositivo que esta siendo autenticado como el servidor de autenticación, deben actuar en total sincronía, o desincronizados, o en respuesta a las señales que requieren contraseñas, donde los datos son intercambiados de forma segura entre el dispositivo y el servidor de autenticación.

Autenticación del Lector

Las claves secretas simétricas compartidas también pueden ser usadas para que el dispositivo del documento de identidad autentique el lector de la Identificación. En este caso, la Identificación emitiría una señal que pediría una contraseña al lector. Luego el lector verificara el resultado con un valor interno calculado. Si la respuesta no es satisfactoria, el dispositivo de identificación no liberaría ningún contenido de sus credenciales. Esta técnica es usada, para prevenir que lectores falsos sean capaces de robar información de credenciales que podrían luego ser utilizadas para hacer documentos de identidad falsificados.

Autenticación de la Credencial de Identificación

Las credenciales digitalizadas almacenadas en la tarjeta de identificación pueden ser autenticadas usando una firma digital del emisor o un código de autenticación de mensajes. En este caso, la autenticación de la credencial se basa típicamente en datos estáticos. Otras técnicas pueden ser usadas para asegurar que la información no ha sido clonada o de alguna otra forma comprometida o que no esta siendo presentada en forma de un contra ataque. Una complicación adicional es que el lector tiene que ser capaz de determinar cuando la credencial expira.

Autenticación del Portador del Documento de Identidad

La persona portadora de un Documento de Identidad puede ser autenticada de dos maneras, por revisión de:

- Lo que el usuario conoce (por ejemplo, un PIN o clave), y/o
- Lo que el usuario es (por ejemplo, un factor biométrico).

Al ingresar un PIN o clave esto le indica al dispositivo electrónico que está en el documento de Identidad, que el usuario está presente. Esto permite al dispositivo liberar la credencial del documento de Identidad del portador o permitir su uso.

Para verificar la autenticidad del usuario, se compara la foto en la tarjeta de identificación con el rostro del portador que presenta el documento de identidad, o se realiza una equiparación biométrica automática. Los sistemas de identificación basados en biométricos capturan una imagen biométrica “en vivo” (por ejemplo, una huella digital o escaneo geométrico de la mano) y lo compara con la imagen biométrica almacenada que fue capturada al momento en que el individuo se registró en el sistema. Esta equiparación biométrica de pareo uno-a-uno, verifica que el portador de la identidad es la misma persona que se registró en el sistema de Identificación y que es la persona correcta para usar dicho documento. Las características biométricas pueden proteger también el acceso a las credenciales que se encuentran en la Identificación.

Papel de las Tarjetas Inteligentes en la Cadena de Confianza

La tecnología de las tarjetas Inteligentes puede reforzar muchos vínculos de la cadena de confianza en un Sistema de Identificación seguro. Las tarjetas

inteligentes pueden actuar como la tarjeta de Identificación individual y permitir el acceso seguro a información y servicios, tanto en diseños de sistemas en línea como fuera de línea. Dada la habilidad de almacenar, proteger y modificar la información escrita en el dispositivo electrónico (por ejemplo, chip) presente en la tarjeta (On Card), las tarjetas inteligentes ofrecen una incomparable flexibilidad y opciones para compartir y transferir información, mientras se brinda una habilidad única de incorporar características sensitivas de privacidad.

Apoyo para la Identificación Física y Digital. Las tarjetas inteligentes tienen la capacidad única de fácilmente combinar identificación y autenticación, tanto en el mundo físico como digital. Esto puede generar un ahorro significativo, dado que la tarjeta de identificación basada en tarjetas inteligentes podrá ser usada para permitir acceso físico a los servicios, así como también permite someter declaraciones de impuestos, solicitar documentos oficiales (por ejemplo, un certificado de nacimiento) en línea, o obtener acceso a redes seguras.

Acceso a Información Autenticada y Autorizada. La información requerida para identificar a un individuo, generalmente depende del rol del individuo en una situación dada. Por ejemplo, cuando se compran cigarrillos, la única información de identificación requerida será la edad del individuo. Si el individuo puede manejar y dónde vive es irrelevante en este caso.

La habilidad de la tarjeta inteligente de procesar información y reaccionar a su entorno, le da una ventaja única en proveer autenticación para acceso a información. La tarjeta inteligente es capaz de liberar únicamente la información requerida y solamente cuando es requerida. A diferencia de otras formas de identificación (tal como una licencia de conducir impresa de forma pasiva), una tarjeta inteligente no expone toda la información personal del individuo (incluyendo información potencialmente irrelevante) cuando es presentada.

Alta Seguridad de la Tarjeta de Identificación. Cuando son comparados con otras tarjetas de identificación resistentes a manipulaciones, las tarjetas inteligentes representan la mejor conciliación entre seguridad y costo. Cuando se utilizan junto con otras tecnologías, tales como criptografías de claves públicas y biométricas, las tarjetas inteligentes son casi imposibles de duplicar o falsificar y los datos almacenados en el chip no pueden ser modificados sin la debida autorización (una clave, una autenticación biométrica o una clave de acceso criptográfico).

Las tarjetas inteligentes también pueden ayudar a detener la falsificación e impedir la manipulación. Las tarjetas inteligentes incluyen una gran variedad de “hardware” y “software” que detectan y reaccionan a cualquier tentativa de manipulación y ayudan a contrarrestar posibles ataques. Cuando se van utilizar también las tarjetas de identidad inteligentes para verificación manual de la identidad, se puede añadir características de seguridad visuales al cuerpo de la tarjeta inteligente.

Seguridad de la Credencial de Identificación. Proteger la privacidad, autenticidad e integridad de los datos codificados en el Documento de Identificación como credenciales, es un requerimiento primario para un sistema de Identificación seguro. Los datos sensitivos son típicamente encriptados, tanto en la tarjeta de Identificación inteligente como durante el proceso de comunicación con el lector externo. Firmas digitales podrán ser utilizadas para asegurar la integridad de los datos, pudiendo requerirse múltiples firmas, si los datos serán creados por diferentes autoridades. Para

asegurar la privacidad, el diseño de las aplicaciones y de los datos en la tarjeta debe evitar que la información pueda ser compartida.

Autenticación de los Componentes del Sistema Para una seguridad y privacidad más robusta, el Sistema de Identificación seguro requerirá que los componentes del sistema autenticuen la legitimidad de los otros componentes durante el proceso de verificación de identidad. La tarjeta de identificación inteligente puede verificar que el lector de tarjeta es auténtico y el lector de tarjeta en turno puede autenticar la tarjeta de Identificación inteligente. La tarjeta de Identificación inteligente también podrá asegurar que el sistema que está solicitando los datos ha establecido el derecho para acceder la información que está siendo solicitada.

Respaldo de la Tarjeta Inteligente para los Requerimientos de Privacidad. El uso de tarjetas inteligentes fortalece la habilidad del sistema para proteger la privacidad individual². A diferencia de otras tecnologías de identificación, las tarjetas inteligentes pueden implementar un “firewall” personal para cada individuo, liberando solamente la información requerida y cuando es exclusivamente solicitada. La habilidad única de la tarjeta de verificar la autoridad del solicitante de la información y su alta seguridad, tanto para la tarjeta como para la información, hace que se convierta en un excelente guardián de la información personal de los portadores de tarjetas. Al permitir acceso autorizado y autenticado solo para la información requerida en la respectiva transacción, el sistema de identificación basado en tarjetas inteligentes puede proteger la privacidad del individuo mientras se asegura que el individuo es correctamente identificado.

Tarjetas Inteligentes y Biométricos. Los Sistemas de Identificación seguro que requieren un alto grado de seguridad y privacidad están crecientemente implementando tecnologías tanto de tarjetas inteligentes como de características biométricas. Las tarjetas inteligentes y las características biométricas se complementan naturalmente para brindar una autenticación en doble vía o hasta multifactorial. La tarjeta inteligente es un medio de almacenaje lógico para información biométrica. Durante el proceso de registro, un patrón biométrico puede ser almacenado en el chip de la tarjeta inteligente para verificación posterior. Solamente el usuario autorizado que corresponda al patrón biométrico que ha sido almacenado en el momento de su registro recibe acceso y los privilegios correspondientes.

Sumario de la Cadena de Confianza

Cualquier sistema de Identificación debe definir las metas de seguridad apropiadas y los atributos dentro de una política de seguridad. Esta política debe identificar el nivel de seguridad apropiado y conmensurado con el valor de cada bien a ser protegido. Cuando se desarrolla esta política de seguridad, debemos dar una atención especial a la fortaleza de cada vínculo en la cadena de confianza, durante la utilización de la tarjeta y credencial de Identificación. En la medida que el sistema dependa de verificación visual o manual, una adecuada atención debe ser dada para el entrenamiento a cualquiera que tenga que tomar decisiones sobre la autenticación de las tarjetas y credenciales de Identidad, además debe haber políticas establecidas relativas a fallas en el seguimiento de los procedimientos.

² Para información adicional sobre como las tarjetas inteligentes pueden aumentar la privacidad en un sistema de Identificación, ver el documento de consenso de la Smart Card Alliance “Privacy and Secure Identification Systems: The Role of Smart Cards as a Privacy-Enabling Technology,” disponible en www.smartcardalliance.org.

Una robusta y completa cadena de confianza para una tarjeta de identidad y credencial es obligatoria para un Sistema de Identificación seguro. Con el advenimiento de las tarjetas inteligentes, dispositivos electrónicos que almacenan las credenciales de Identificación y verificación biométrica, el nivel de confianza para una credencial que está siendo presentada podrá ser significativamente incrementado. El dispositivo electrónico (por ejemplo, chip en un pasaporte electrónico o en una tarjeta de Identificación inteligente) es el agente de seguridad portátil del emisor y es un vínculo vital en la cadena de confianza para cualquier sistema serio de Identificación seguro.

Conclusiones

Los sistemas de identificación son necesarios tanto para las organizaciones privadas como públicas. Los sistemas de Identificación pueden operar completamente dentro de una sola organización (una Identificación de empleado), abarcar múltiples organizaciones (a lo largo de varios cuerpos gubernamentales, entre varios negocios y sus clientes), o extendidos a la población en general. Dada la complejidad del problema de verificación de identidad, el número de participantes involucrados y el número de opciones en el diseño de sistemas de identificación, no es de sorprender que muchos de los sistemas de identificación hoy día son vulnerables.

Para afrontar tales vulnerabilidades e implementar un sistema de identificación seguro, las organizaciones deben definir una cadena de confianza que abarque todos los procesos y componentes de un sistema de identificación seguro. La cadena de confianza empieza con la definición del modelo de confianza, la políticas de seguridad, los acuerdos de negocio entre las organizaciones envueltas en los sistemas de Identificación seguro e incluye todos los componentes del sistema de Identificación – desde los procesos y documentos que son utilizados para la verificación inicial de la identidad de un individuo y el registro de este individuo dentro del sistema de identificación hasta el uso el sistema para la gestión general de todo el sistema de identificación.

Las tarjetas inteligentes son un vínculo vital en la cadena de confianza de un sistema de identificación seguro. Ellos actúan como el agente de confianza del emisor y brindan la capacidad única de asegurar y verificar con precisión la identidad de los portadores de tarjetas, autenticar la credencial del documento de identidad y presentar la credencial al sistema de Identificación.

Como se discutió en este informe, los sistemas de identificación basados en tarjetas inteligentes ofrecen beneficios significativos para los individuos, negocios y gobiernos. Los individuos que utilizan tarjetas inteligentes disfrutan de mayor satisfacción, a través de acceso más seguro, conveniente y más rápido a información y servicios. La eficiencia, consolidación de programas y las características de seguridad brindadas a través del uso de tarjetas de identificación inteligentes, permiten a gobiernos y negocios aumentar la seguridad mientras mejoran los servicios y reducen los costos operativos. Las tarjetas inteligentes brindan una plataforma tecnológica óptima para sistemas de identificación seguros que pueden responder a las necesidades de gobiernos y negocios para una verificación segura y exacta de la identificación.

Recursos Adicionales de la Smart Card Alliance

“Logical Access Security: The Role of Smart Cards in Strong Authentication,” Smart Card Alliance report, Octubre 2004

“Privacy and Secure Identification Systems: The Role of Smart Cards as a Privacy-Enabling Technology,” Smart Card Alliance white paper, Febrero 2003

Smart Card Alliance web site, www.smartcardalliance.org

“Smart Card Case Studies and Implementation Profiles,” Smart Card Alliance report, Diciembre 2003

“Smart Cards and Biometrics in a Privacy-Sensitive Secure Personal Identification System,” Smart Card Alliance report, Mayo 2002

“Using Smart Cards for Secure Physical Access,” Smart Card Alliance report, Julio 2003