



Sistemas de Administración de Identidad, Tarjetas Inteligentes y Privacidad

No importa donde usted vaya, hoy en día, es muy probable que en algún momento alguien le solicite ver su identidad (ID). Hoy, la verificación de identidad se solicita a diario en una variedad de situaciones familiares – cuando una persona desea obtener servicios de salud, cuando entra a un edificio público o a una oficina corporativa, o para subirse a un avión.

Las organizaciones que necesitan verificar identificaciones encuentran problemas sobre privacidad y la protección de información personal, que rápidamente emergen como temas centrales cuando se consideran nuevos sistemas de administración de identidad. Los requerimientos específicos de seguridad que tiene una organización deben ser balanceados con el deseo genuino de proteger la privacidad de los individuos cuyas identidades deben ser verificadas. Tal requerimiento – cómo identificar a las personas inequívocamente mientras se protege también su privacidad – moldea cualquier discusión de cómo diseñar, construir o implementar un nuevo sistema seguro de administración de identidad.

Diseñar un nuevo sistema de administración de identidad es complejo, y la necesidad de obtener un balance entre la seguridad y la privacidad afecta todo lo referente al diseño de sistema, desde las políticas y los procesos establecidos para apoyar y mantener el sistema, hasta la arquitectura del sistema y la tecnología en particular que se escoge para autenticar los individuos. Por ejemplo:

- La organización debe tener políticas de seguridad y privacidad que claramente definan que información personal se va a recolectar, como será usada la información, quien podrá tener acceso a la información, como será protegida la información, y como el individuo puede controlar su uso y brindar actualizaciones a la información a través del tiempo.
- La inscripción y el proceso de validación de identidad debe verificar que la información presentada es veraz y protege la integridad de la información.
- El sistema debe proteger la información de cada individuo en todo momento, incluyendo el periodo en el cual la información está siendo grabada y mientras está siendo usada.
- El documento de identificación que un individuo lleva consigo debe estar protegido en su contenido para evitar ser copiados, alterados o robados, para prevenir su uso no autorizado, el mal uso o divulgación de la información personal que contiene.
- El intercambio de datos entre el documento de identificación y cualquiera que sea el dispositivo que lee la identidad debe ser protegido para prevenir la captura no autorizada y el uso de datos para personificar a un individuo.
- El acceso a la información personal debe ser garantizado solamente después de un proceso definido por el usuario de autenticación. Solo la información necesaria debe ser liberada y solo al sistema o al individuo autorizado.

- Todo personal involucrado en el uso del sistema debe ser cuidadosamente capacitado y monitoreado para asegurar la conformidad estricta con las políticas y prácticas del sistema. Si tales políticas y prácticas quedan comprometidas; esto significa que el sistema de administración de identidad como un todo ha quedado comprometido.

El diseño de un sistema de administración de identidad para guardar la privacidad individual envuelve, por lo tanto, más que simplemente seleccionar un tipo particular de tecnología de identidad. La organización que emite un documento de identidad, debe diseñar la seguridad y la privacidad de la información en el sistema como un todo y tener las adecuadas políticas y procesos establecidos para apoyar los requerimientos de privacidad y seguridad e implementar las tecnologías que brindan estas características. Las organizaciones que emiten documentos de identidad, también deben tener prácticas operacionales establecidas para monitorear y asegurar que las políticas de identidad y seguridad son seguidas de manera estricta.

Selección de Tecnología de Identidad

La selección de la tecnología de identidad es también crítica. La tecnología de identidad debe ser una que, tanto facilite como refuerce el diseño y las metas de seguridad del sistema. Muchos sistemas de identidad y de distintivos para su personal utilizan tecnologías como cintas magnéticas y códigos de barras. Tales tecnologías ya no son adecuadas, debido a que no pueden lograr los requerimientos de alcanzar una alta seguridad, mientras guardan la privacidad. Los documentos de identidad basados en dichas tecnologías son muy propensos a manipulación, pueden ser fácilmente falsificados, y brindan poca o ninguna protección para la información que está contenida en dichos documentos.

Solamente los documentos de identidad que utilizan tecnología de tarjetas inteligentes tienen las características de alta seguridad, que pueden aumentar la protección de la privacidad en un sistema bien diseñado y adecuadamente implementado. Los documentos de identidad que utilizan tecnología de tarjetas inteligentes, incluyen un micro controlador seguro o inteligencia equivalente y una memoria interna que está disponible en una variedad de formatos (por ejemplo, tarjetas plásticas, documentos u otros dispositivos manuales portátiles). Contar con tecnología de tarjetas inteligentes brinda un sistema de administración de identidad que cuenta con las siguientes ventajas:

- **Alta protección de la información.** La tecnología de tarjetas inteligentes protege los datos de identidad guardados en la identidad completamente y en forma constante. Los documentos de identidad basados en tarjetas inteligentes pueden cifrar la información de identidad guardada en ellos y cifrar las comunicaciones entre la identidad y el dispositivo que lee la identidad, previniendo de esta forma ser víctima de acecho. La tecnología de tarjetas inteligentes, también puede bloquear la información personal en la identidad, liberarlo solamente después de que el dueño de dicha tarjeta autoriza su liberación al proveer o brindar una información única tal como un número de identificación personal (PIN), una clave, o un factor biométrico, como una huella dactilar o impresión digital.
- **Alta Seguridad de la identidad.** Los documentos de identidad que incorporan tecnología de tarjetas inteligentes son extremadamente difíciles de duplicar o falsificar. En adición a las obvias características contra falsificación visual y de resistencia a la manipulación, tales como hologramas, micro impresiones y dispositivos de variabilidad ópticas, los chips de tarjetas inteligentes tienen un sistema de resistencia a la manipulación incluido

dentro del mismo chip. El chip de una tarjeta inteligente o de un documento de identidad basado en tarjetas inteligentes, incluye una variedad de hardware, es decir unidades físicas o componentes y software o sea, programas que tienen la capacidad de detectar inmediatamente y de reaccionar a cualquier tentativa de manipulación y de contrarrestar posibles ataques.

- **Procesamiento sofisticado en la tarjeta “on card”.** Las tarjetas inteligentes tienen muchas funciones de administración de identidad dentro de un ambiente de procesamiento seguro en la misma tarjeta. Las tarjetas inteligentes almacenan datos que, pueden ser luego manejados o administrados con toda seguridad, protegiendo la información mientras está siendo almacenada o usada. El procesamiento que realiza la tarjeta inteligente permite que los documentos a base de tarjetas inteligentes puedan realizar funciones en la misma tarjeta (por ejemplo, cifrar, descifrar y otros procesamientos de datos) y de interactuar de una manera segura e inteligente con el lector de la tarjeta. Dichas capacidades tienen importancia particular cuando un sistema de administración de identidad está basado en información biométrica para verificar la identidad de un individuo. Las tarjetas de identificación inteligentes pueden almacenar de forma segura la información biométrica y realizar la comparación de los datos biométricos dentro del chip de la tarjeta inteligente y verificar la identidad del individuo que utiliza la tarjeta. Esto ofrece una mayor privacidad, una vez que la información biométrica del individuo está guardada y nunca dejará la identidad (que se mantiene en posesión del mismo individuo) luego se equipara la información que está almacenada en el chip, con la que se captura en el momento que el individuo utiliza la tarjeta y esto sucede dentro del chip de la tarjeta inteligente en un ambiente de procesamiento totalmente seguro.
- **Acceso a la información autenticada y autorizada.** La habilidad de la tarjeta inteligente de procesar información y de reaccionar a su ambiente es única. Cuando el acceso seguro a la tarjeta es un requerimiento; solo los documentos de identidad basados en tarjetas inteligentes pueden verificar la autenticidad del lector de la identidad y brindar su propia autenticidad al lector. Las tarjetas inteligentes también pueden verificar la autoridad de quien solicita la información y luego restringir el acceso únicamente a solamente la información solicitada en particular. La información personal guardada puede ser luego protegida por una información única, como por ejemplo, un PIN o un factor biométrico, brindado por el que utiliza la tarjeta antes de que cualquier acceso a la tarjeta sea ofrecido.

Al ser implementada correctamente, la tecnología de las tarjetas inteligentes fortalece la habilidad de cualquier organización de proteger la privacidad de los individuos cuya identidad la organización necesita verificar. A diferencia de otros documentos de identidad, los documentos de identidad basados en tarjetas inteligentes pueden implementar un “*firewall*” personal, liberando solamente la información solicitada y solo cuando es genuinamente requerido. Las tarjetas inteligentes son excelentes custodios de la información personal así como de la privacidad individual.

Conclusión

Smart Card Alliance cree que la protección de la privacidad individual es una meta crítica para cualquier sistema de administración de identidad. La Alianza de Tarjetas Inteligentes recomienda que las organizaciones que estén considerando nuevos sistemas de administración de identidad, sigan las siguientes pautas:

- Desarrollar y comunicar una fuerte política de privacidad y seguridad para gobernar todo el sistema de administración de identidad.
- Seguir las pautas y prácticas operativas diseñadas por el sistema para apoyar dichas políticas.
- Implementar el sistema de administración de identidad utilizando tecnologías que fueren dichas políticas.
- Usar credenciales de identidad basadas en tarjetas inteligentes como un componente del sistema.

El uso de la tecnología de tarjetas inteligentes en el diseño de un sistema de administración de identidad, representa el primer paso inteligente para preservar y proteger la privacidad individual, mientras se alcanza un alto grado de seguridad en la verificación de la identidad.

Para mayor información sobre tarjetas inteligentes y el papel que juegan en asegurar identificación y otras aplicaciones, favor visitar el sitio web www.smartcardalliance.org/latinamerica o contacte directamente a Smart Card Alliance al 1-800-556-6828.

Haga “Click” aquí para una versión PDF de “Identity Management Systems, Smart Cards and Privacy”.

Haga “Click” aquí para leer preguntas frecuentemente hechas sobre Sistemas de Manejo de Identidad Tarjetas Inteligentes y Privacidad.

Otros Recursos de la Smart Card Alliance

“Identity Management Systems, Smart Cards and Privacy: Frequently Asked Questions”, March 2005

“Privacy and Secure Identification Systems: The Role of Smart Cards as a Privacy Enabling Technology,” Smart Card Alliance report, February 2003

“Secure Identification Systems: Building a Chain of Trust.” Smart Card Alliance report, March 2004

Sobre Este Documento

Smart Card Alliance desea agradecer a todos los miembros de la Alianza que han participado en el proyecto para desarrollar este documento sobre sistemas de administración de identidad, y tarjetas inteligentes y privacidad. Los que contribuyeron con este documento incluyen a personal de las siguientes organizaciones: AMAG Technology, Atmel Corporation, CardLogix, Fargo Electronics, Gemplus, EDS, Hitachi America, IBM, Lockheed Martin, MaartSoft Corporation, Northrop Grumman Corporation, Philips Semiconductors, SafeNet, Inc., Smart Commerce, Inc., SuperCom, Inc., Verifone.

Acerca de la Smart Card Alliance Latin America (SCALA)

Smart Card Alliance Latin America (SCALA) es una asociación sin fines de lucro, no partidaria, con múltiples miembros de la industria, líder en acelerar la aceptación a gran escala de las múltiples aplicaciones de la tecnología de tarjetas inteligentes. La Alianza incluye entre sus

miembros a compañías líderes en la rama bancaria, servicios financieros, computación, telecomunicaciones, tecnología, servicios de salud, industria de venta al detal, control de acceso, transporte y entretenimiento, así como una gran cantidad de agencias gubernamentales. A través, de proyectos específicos, como programas educativos, investigaciones de mercado, cabildeo, relaciones industriales y foros abiertos; SCALA mantiene a sus miembros conectados con los líderes de la industria y el pensamiento innovador. Smart Card Alliance es la voz unificada de la industria de tarjetas inteligentes, liderando la discusión de la industria sobre el impacto y el valor de las tarjetas inteligentes en los Estados Unidos y América Latina. Para mayor información, visite www.smartcardalliance.org/latinamerica.