Sistema de control de acceso basado en Java Cards y Hardware libre

Access control system based on Javacards and Hardware Free

Carlos Henríquez[1]

Mg Ingeniería de Sistemas y Computación. Profesor Tiempo completo de Ingeniería de Sistemas. Grupo Ingeniería de software y nuevas tecnologías Universidad Autónoma del Caribe. chenriquez@uac.edu.co

Recibido 6/10/2010, Aceptado 3/12/2010

RESUMEN

El presente artículo presenta los resultados de la investigación "S*istema de Control de Acceso y Registro de Asistencia Utilizando Smart Cards con Tecnología JavaCard y Plataforma de Hardware Libre Arduino*", que presenta la creación de un sistema parametrizable que permite el control de acceso a las puertas y el registro del ingreso del personal en la empresa donde se labora a través de conexión remota a servidores de autenticación y dispositivos electrónicos de hardware libre. Para la implementación de la solución, se partió del conocimiento que se tenía sobre las tarjetas inteligentes (*SmartCard*), se integraron tecnologías como *JavaCard* y *Jsp* y por último se hizo uso de tarjetas como *Arduino* y *Ethernet shield*.

El proceso que se implementó se describe a continuación: se abordó inicialmente las teorías, los componentes y las arquitecturas de los sistemas de control de acceso; luego se adaptó la plataforma *Arduino* a las necesidades de los sistemas, posteriormente se analizó y diseñó el sistema web y el desarrollo de la aplicación fue embebida en *Arduino*. Por otro lado, se construyeron servicios para lectura de las tarjetas *SmartCard* y su respectiva autenticación, seguidamente se realizó el acople y ensamble de los componentes del sistema a un panel de paso y a la red. Al final se construyó una aplicación de alta funcionalidad que enmarca un conjunto de tecnologías emergentes, cuyo producto es una herramienta que puede ser adquirida por cualquier organización a un costo muy bajo.

Palabras clave: Arduino, Control de acceso, Hardware Libre, Smart Card

ABSTRACT

This article presents the results of the investigation "Access Control System and Attendance Record Using Smart Cards with JavaCard Technology Hardware Platform Free Arduino ," featuring the creation of a configurable system that allows access control doors and registration of personal income in the company where one works through remote connection to authentication servers and hardware electronics devices free. To implement the solution, started from the knowledge that was available about the smart card (SmartCard), were integrated and Jsp technologies such as JavaCard and finally made use of cards as Arduino Ethernet shield.

The process was implemented as described below, was first addressed the theory, components and architectures of access control systems, then the Arduino platform adapted to the needs of the systems, then analyzed and designed the web system and development of the application was embedded in Arduino. On the other hand, were built reading services and their respective SmartCard authentication, then the coupling was carried out and assembling the components to a panel of way and network. Eventually built a highly functional application that frames a set of emerging technologies, whose product is a tool that can be acquired by any organization to a very low cost.

Key words: Arduino, Acces control, free hardware, Smart Card

1. Introducción

Conociendo la existencia de los sistemas de control de acceso y de registro de asistencia, la mayoría de las organizaciones siguen implementando controles manuales o ineficientes para su administración ya que resulta costoso y/o 'innecesario'. Inclusive empresas con grandes sistemas de seguridad costosos siguen teniendo problemas puesto que los empleados llegan a prestar sus credenciales, o bien a falsificarlas, y por ende 'adulteran' al sistema. Por lo anterior se buscó con la investigación mejorar los procesos a nivel de seguridad en la empresa y reducir la falsificación de credenciales, todo a un costo razonable.

El siguiente artículo muestra como resultado la construcción de un sistema de control de acceso basado en la integración de múltiples tecnologías a un bajo costo. En la primera parte se aborda la metodología, seguida del estado del arte. Luego se muestran en los resultados la construcción del sistema y por último las conclusiones.

2. Metodología

2.1 Enfoque metodológico

La investigación realizada en este trabajo fue "Investigación aplicada tecnológica" [1] la cual buscó mejorar los procesos de control de asistencia y los sistemas de seguridad en cuanto a la integridad de recursos en las organizaciones, tomando como base el desarrollo las nuevas tecnologías en materia de sistemas de identificación como las tarjetas inteligentes. El entendimiento de los sistemas de control de acceso, en cuanto su teoría, componentes y arquitecturas fue la primera tarea de la investigación. Paralelamente se estudió el soporte que brinda la plataforma de hardware libre *Arduino* como panel de control del sistema de control de acceso. La tecnología de las tarjetas inteligentes (*Smartcard*) fue manejada por los investigadores en [2] por lo que se hizo énfasis en el diseño de las aplicaciones que irían en la tarjeta. Luego de seleccionar el *Arduino* como panel de control, se da comienzo al análisis y diseño del software orientado a la Web y al desarrollo de la aplicación embebida en la plataforma de hardware. En la siguiente etapa se elaboraron los servicios para lectura de las tarjetas inteligentes y de autenticación para luego dar paso al acople y ensamble de los componentes del sistema al panel y la red. Por último se realizaron las pruebas que confirman y avalan la funcionalidad de todo el sistema.

Por el lado de la tecnología involucrada en las tarjetas inteligentes y la plataforma de hardware *Arduino* en la investigación, se utilizó observación documental [3] y la búsqueda de recursos en la Web de los sitios del fabricante respectivamente.

2.2 Estado del Arte

Los *sistemas de control* de acceso son sistemas que permiten manejar una autoridad para controlar el acceso a recursos o áreas en una instalación física dada o en un sistema de información basado en computadoras. El control de acceso en términos reales es un tema de gran envergadura pues puede llegar a ampliarse de tal forma que se implementen todas las técnicas de seguridad electrónica al integrarse con diferentes tecnologías, particularmente Sistemas de intrusión y *CCTV* [4]. Con base en lo anterior se integran en el proyecto un sin numero de tecnologías a destacar: *Arduino* plataforma de electrónica abierta para la creación de prototipos basada en software y hardware flexibles y fáciles de usar. Se creó para artistas, diseñadores, aficionados y cualquiera interesado en crear entornos u objetos interactivos [5]. Hay multitud de diferentes versiones de placas *Arduino*. La actual placa básica, el *Duemilanove,* usa *Atmel ATmega328*. Esta es la última revisión de la placa *Arduino USB* básica. Se conecta al computador con un cable *USB* estándar y contiene todo lo necesario para programar la placa. Se puede ampliar con gran variedad de *shields*: placas de extensión con funcionalidades específicas [6]. La *SmartCard* es un dispositivo que incluye un chip de circuito integrado incrustado que puede ser un micro controlador de seguridad o de inteligencia equivalente con memoria interna o un solo chip de memoria. La *SmartCard* se ajusta a las normas internacionales (*ISO 7816 e ISO / IEC 14443*) y está disponible en una variedad de factores de forma, incluidas las tarjetas de plástico, dijes, módulos de identificación del abonado (*SIM*) utilizados en teléfonos móviles *GSM*, y *USB* basados en chips [7]. *La tecnología Java Card* permite que tarjetas y otros dispositivos con capacidades de memoria muy limitadas ejecutar pequeñas aplicaciones que utilizan la tecnología *Java* [8]. Esta tecnología permite a los desarrolladores diseñar, construir, evaluar e implementar aplicaciones y servicios de forma rápida y segura, reduciendo costos, incrementar la productividad y generar un valor agregado al cliente [9].

3. Resultados: Sistema de Control "Java Card Access Control & Attendance System"

3.1 Características del sistema

Java Card Access Control & Attendance System "*JACAS*" (Sistema de Control de Acceso y Asistencia Java Card), es el nombre que recibe la solución orientada a la Web para el control de acceso a recintos cerrados implementando las tarjetas inteligentes usando tecnología *Java Card*. Como tal *JACAS* hace parte del componente de control y administrativo en donde se registran lógicamente los elementos del sistema, los cuales son: puertas, paneles, lectoras,

relés,[1] carnés, usuarios y los permisos. Una vez puesto en marcha el sistema, el mismo permite abrir una puerta sin necesidad de la credencial; además posee un modulo de reportes el cual brinda la funcionalidad de obtener información detallada de los ingresos y los egresos por fechas, por puerta, por usuario, por carné, entre otros.

Para el diseño de las políticas de control de acceso, se implemento un sistema basado en roles [10], los cuales son asignados a los usuarios, de manera que podrían existir usuarios con mayores privilegios que otros. Un rol está compuesto por un conjunto de puertas a las que el usuario tiene acceso y por solo un intervalo de tiempo (zona de tiempo, ver figura 1), lo cual facilita la gestión de entradas o salidas del usuario al grupo de puertas.

3.2 Applets Usuario y Carné

Para que un usuario pueda acceder a ciertas áreas dentro de una organización, todo lo que debe hacer es ingresar su carné por el dispositivo lector. Previamente el carné es dotado de dos *applets* [11]; el *applet* "Carné" está destinado para el almacenamiento de un número identificador o código único y del *applet* "Usuario". Cuando un usuario *administrador* registra un carné en el sistema, en realidad *JACAS* está recuperando ese código y lo almacena en su base de datos.

Posteriormente, *JACAS* permite asignar el carné al usuario; mediante este proceso se almacena en el *applet* "Usuario" la información personal del usuario además de su identificación en el sistema. De esta forma se amplían los controles sobre el ingreso de manera que un carné que no haya sido asignado a un usuario no tendrá ningún uso sobre alguna puerta. Además sugiere la reutilización de los carnés porque se podrían des-asignar para una nueva asignación a otro usuario, independientemente de los permisos de los mismos.

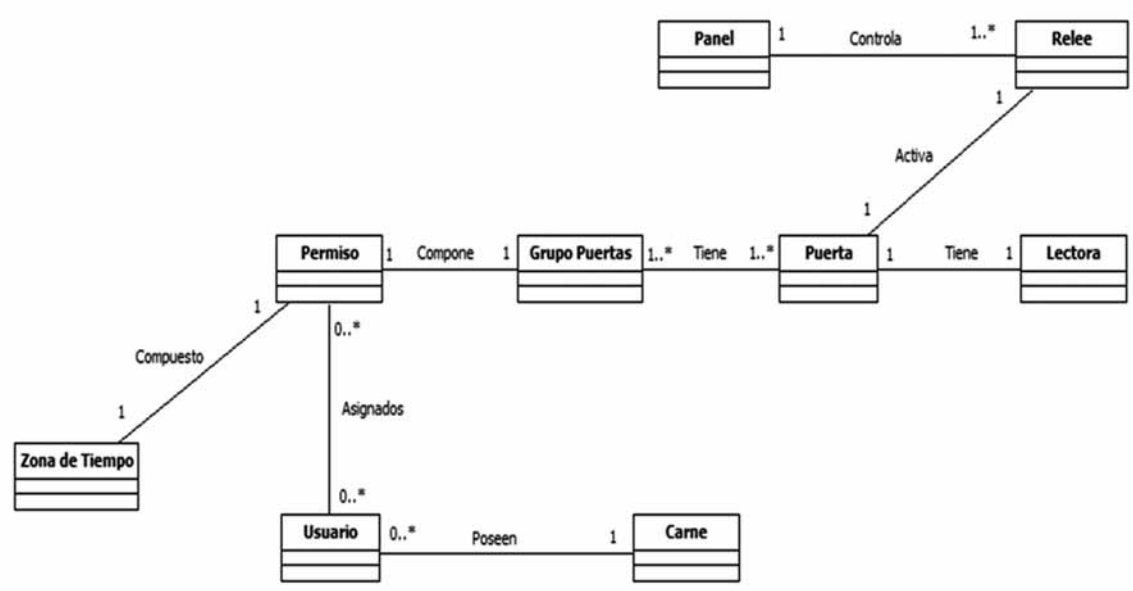
3.3 Panel de Control: Arduino, Ethernet Shield e Interfaz de Potencia.

Para la fabricación del panel de control se implementó tecnología *Arduino* articulada con una *Ethernet Shield* [12], del mismo fabricante. El panel suple las necesidades de control al estar conectado con el servidor de control de acceso y además de conectar las cerraduras de las puertas de acceso para permitir el ingreso o egreso de una determinada área.

La programación del 'panel' fue llevada a cabo a través del software *Arduino*. Inicialmente, fue programado para abrir puertas sin el uso de las tarjetas inteligentes (usando *JACAS*); de este modo se comprobó su funcionalidad

[1] El **relé** es un dispositivo electromecánico que funciona como un interruptor controlado por un circuito eléctrico en el que, por medio de una bobina y un electroimán, se acciona un juego de uno o varios contactos que permiten abrir o cerrar otros circuitos eléctricos independientes

Figura 1. Modelo del Dominio del Sistema. (System Domain Model)



además del *Ethernet Shield*. Básicamente, el panel recibe las peticiones del servidor de control de acceso y/o de *JACAS* para enviar un pulso por cuatro (4) segundos a la "salida" ó relé correspondiente y devuelve sí la tarea fue realizada con éxito o no.

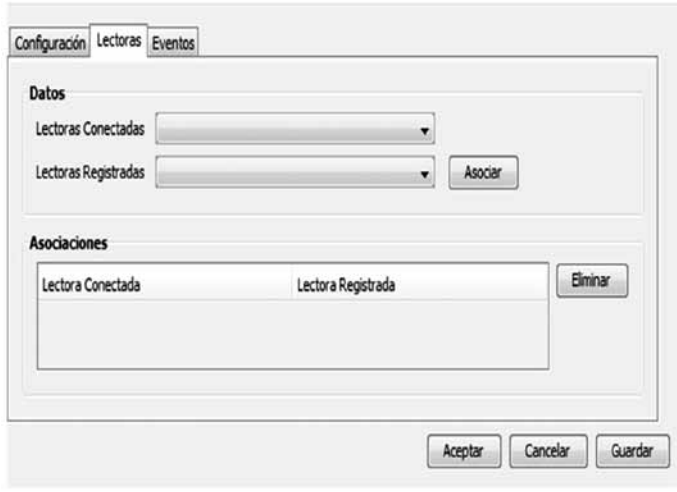
La interfaz de potencia no es más que un circuito que amplifica y convierte la salida del *Arduino* de 5 *VDC*[2] a 110 *VAC*[3] para la activación temporal de las cerraduras. En el momento en que el *Arduino* termina la emisión del pulso, las cerraduras vuelven a su estado normalmente cerrado. Esta interfaz es donde se realizan las conexiones hacia las cerraduras y recibe los pulsos del *Arduino* a través de una correa o bus.

3.4 Servicio de Lectura de Carnés

En el contexto de la solución, los dispositivos lectores [13] están conectados a una computadora. Esta máquina debe alojar el servicio de lectura, el cual valida la información de la tarjeta para su posterior envío al servidor de control de acceso, aunque previamente, se deben relacionar las lectoras conectadas a esta máquina con las lectoras registradas en la base de datos de *JACAS;* de este modo cuando los usuarios inserten su carné en el dispositivo lector, se abrirá la puerta que corresponde a ese punto de acceso (ver figura 2 y 3).

Figura 2. Pestaña de Configuración del Servicio De autenticación (Settings tab Authentication Service)

Figura 3. Pestaña de Configuración del Servicio de Lectoras (Configuration tab Readers Service)



3.5 Servicio AAA (Authentication, Authorization and Accounting): servicio de control de acceso

Este servicio está desarrollado con el fin de autenticar el usuario y carné que viene de la petición del servicio de lectura; decide bajo ciertos parámetros, además de sus permisos, si permite o no el ingreso y además registra el resultado en la base datos. Una vez que el usuario es autorizado, el servicio establece la comunicación con el panel para la transmisión del pulso que activa las cerraduras. Este proceso se da gracias a que el servicio de lectura envía información del dispositivo lector y mediante ciertas asociaciones el servicio *AAA* halla el relé que se debe activar. La figura 4 muestra la interfaz del servicio *AAA*.

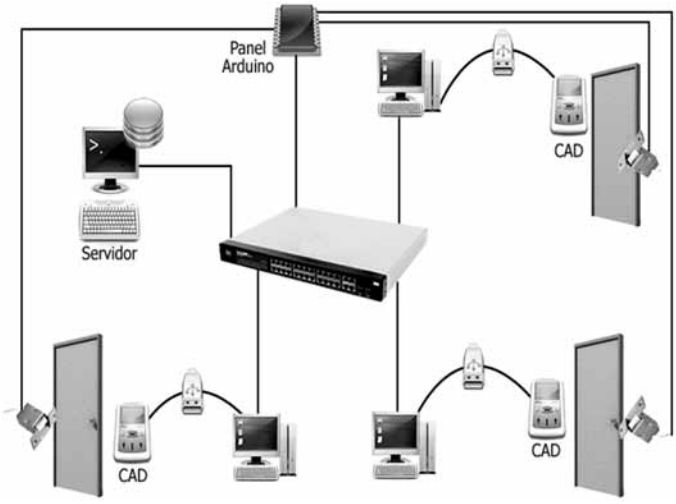
Figura 4. Servicio AAA. (AAA Service)

[2] Volts of continuous current
[3] Volts Alternating Current

3.6 Prototipo de la Solución

Una vez los componentes listos para el despliegue de la solución, se realizan las conexiones físicas al panel y a una *LAN*, se agregan los componentes a *JACAS*, se conectan los dispositivos lectores y se suben los servicios correspondientes. La figura 5 muestra la arquitectura del prototipo.

Figura 5. Arquitectura del Sistema de Control de Acceso y Registro de Asistencia. (System Architecture Access Control and Attendance Record)



El sistema inicia su trabajo cuando un usuario junto con su tarjeta trata de entrar a un recinto (puerta) e introduce su S*martcard* asignada en el lector (*cad*). Si el usuario tiene todos los permisos de ingreso a esa puerta, el servidor envía una orden de apertura al panel (*Arduino*) y este por intermedio de una señal de voltaje se conecta a un relé y este a su vez abre la puerta. Si el usuario no esta habilitado, el sistema no permite la apertura de la puerta y genera los mensajes correspondientes.

La funcionalidad del prototipo se examinó llevando a cabo escenarios de prueba, en donde se establecieron ciertas configuraciones de permisos, carnés, usuarios y puertas. Los casos de prueba estuvieron basados en las características que brindan los sistemas actuales del mercado y bajo las consideraciones que implica la credencial inteligente. Se demostró que el diseño del servicio *AAA* maneja de manera eficiente todas las peticiones que recibe del servicio de lectura cuando los usuarios insertan su respectiva tarjeta en los dispositivos lectores, en los distintos puntos de acceso.

Para la implementación en un sistema real solo basta con mantener la maquina servidora y el número de maquinas cliente se verá afectada por la cantidad de puertas que se desee con un máximo de ocho (8) puertas por panel (*Arduino* y placa base). Si las condiciones físicas de la infraestructura donde se implemente son favorables (si hay dos puertas a 1.80 m de una maquina) se podría reducir el número de maquinas cliente al conectar más de una lectora en una sola maquina. Para asegurar y mantener la integridad del panel se instalaron en una caja de paso[4].

3.7 Solución dé bajo costo

Es un reto cuantificar los beneficios que trae un sistema de control de acceso en la seguridad de una organización. En general, los proyectos de seguridad hacen parte de una estrategia de una organización para administrar el riesgo que existe sobre la seguridad de los activos.

En el mercado colombiano es común encontrar soluciones de sistemas de control de acceso con tarjetas de proximidad de marca *HID* [14] en conjunto con paneles electrónicos de marcas como *General Electrics* [15], *IdentiCard* [16], etc. Este tipo de tarjetas de proximidad de 125KHz, al igual que las de banda magnética, simplemente almacenan un código que es enviado al lector y posteriormente al panel para la identificación y autorización. Su uso extendido hace que sea una alternativa de solución. En la tabla 1, se presenta un comparativo de los costos aproximados de implementación de otras alternativas de solución con respecto a la propuesta, mirando los precios de los componentes del sistema de control de acceso.

Tabla 1. Análisis costo - beneficio. (Cost-benefit Analysis)

No.	Componente	Otras Soluciones	Nuestra Solución
1	Panel de Control (c/u)	(GE) $1859.00 USD (IdentiCard) $1555.00 USD	$350.000
2	Tarjetas de Identificación (por paquete)	$2.60 USD	$15 USD
3	Lector de tarjetas (c/u)	(GE) $200.00 USD (HID) $59.00 USD	$19 USD
4	Relee/Cantonera/Electroimán (c/u)	$118.00 USD	$90.000
5	Botón de Salida (c/u)	$40.50 USD	$40.50 USD
6	Software de Administración (c/u)	(Secure Perfect) $2300.00 USD (IDentiPass) $550.00 USD	$1'500.000
	TOTALES	(GE) $4520 USD (IdentiPass) $2325 USD	$1044 USD

Como se puede apreciar en la tabla los costos de implementar un sistema de control de acceso en el mercado local son bastante elevados. Hoy en día estas soluciones son acogidas por grandes organizaciones que lo necesitan por el gran flujo de personal entrante y saliente; por reducir riesgos de seguridad además de automatizar y optimizar sus procesos. El hecho de que la solución que se planteó

[4] Una caja de paso es un contenedor para las conexiones eléctricas, generalmente con la intención de ocultarlas de la vista y evitar la manipulación indebida.

sea más económica brinda a organizaciones más pequeñas la oportunidad de satisfacer sus necesidades en cuanto a seguridad de acceso se refiere.

4. Conclusiones

- El sistema construido permite gran escalabilidad porque en cualquier momento permite el crecimiento de la infraestructura y permite añadir cuantos *Arduino* sean necesarios para mantener el control de acceso en las instalaciones. Por otra parte fue construido para brindar soluciones parametrizables a cualquier organización independientemente de su entorno tecnológico.

- Las tecnologías empleadas en la solución como el uso de *Smartcard* implican un alto grado de confidencialidad e integridad en las credenciales del sistema de control y ofrece un alto desempeño a nivel de seguridad y de funcionalidad.

- La tecnología *Java Car*d ofrece una gran compatibilidad de plataformas con soluciones basadas en la plataforma *Java*, ampliando las posibilidades de el uso de la misma tarjeta para distintas aplicaciones.

- La plataforma de hardware libre *Arduino* junto a un *Ethernet Shield*, se convierten en una potente herramienta en cuanto a diseño de sistemas distribuidos y paneles de control que bien pueden incluir desde distintos tipos de alarmas hasta domótica.

- Este sistema es un paso importante en la construcción de sistemas de control de acceso utilizando como base tecnológica software y hardware libre de punta lo que la hacen una herramienta potente de bajo costo.

5. Referencias

[1] Castro M. Caracterización de la investigación y de la tecnología. Disponible en : http://hosting.udlap.mx/profesores/miguela.mendez/alephzero/archivo/historico/az27/clasificacion.html

[2] Henríquez C y Ramos F, "Diseño e implementación de tecnología basada en dispositivos inteligentes para apoyo a diferentes servicios educativos de la Universidad Autónoma del Caribe", Prospectiva 6 (2). 2008

[3] De la Mora, M., Metodología de la investigación: Desarrollo de la Inteligencia, Thomson, México, 2006.Pag 217-218

[4] Honey, G., Electronic Access Control, Newnes, Inglaterra, 2000.

[5] Banzi, M., Cuartielles, D., Igoe, T., Martino, G. y Mellis, D. (2010) Arduino HomePage [Internet], Disponible desde < http://www.arduino.cc/es/ > [Acceso 14 de Junio 2010]

[6] Banzi, M., Cuartielles, D., Igoe, T., Martino, G. y Mellis, D. (2010) Arduino Hardware [Internet], Disponible desde < http://arduino.cc/es/Main/Hardware > [Acceso 14 de Junio 2010]

[7] Smart Card Alliance (2010) About Smart Cards: Introduction: Primer – Smart Card Alliance [Internet] Disponible desde < http://www.smartcardalliance.org/pages/smartcards-intro-primer> [Acceso 15 de Junio 2010]

[8] Sun Microsystems (2009) Java Card Technology [Internet] Disponible desde <http://java.sun.com/javacard> [Acceso 10 de Octubre 2009]

[9] Sun Microsystems (2008). Java Card Technology Overview. Disponible desde] <http://java.sun.com/javacard/overview.jsp.>

[10] Ferraiolo D.F, Kuhn D.R., Chandramouli R.. Role-Based Access Control. Artech House . 2003

[11] Chen Z. "Java Card Technology for Smart Cards" Addison Wesley.2004

[12] Arduino. Arduino Ethernet Shield. Disponible en: http://www.arduino.cc/en/Main/ArduinoEthernetShield

[13] Kimaldi Electronics. Lectores Tarjeta chip y DNI. Disponible en: http://www.kimaldi.com/productos/lectores_de_tarjetas/lectores_tarjeta_chip_y_dni

[14] Hid Global. The Trusted Source for Secure Identity Solutions. Disponible en : http://www.hidglobal.com/main/espanol/

[15] General Electric Company. A-Series Lighting Control Panel. Disponible en: http://www.geindustrial.com/cwc/dispatcher?request=products&id=remote_ope

[16] Identicard Systems. Id Card Guide. Disponible en : http://www.identicard.com/id-card-guide.htm