INGENIERÍA ELECTRÓNICA

Diseño de un carné de identificación universitario mediante tarjetas inteligentes

Edwin Vargas-García*, Vladimir Trujillo-Olaya*, Jaime Velasco-Medina*§

***** *Escuela de Ingeniería Eléctrica y Electrónica, Universidad del Valle, Cali, Colombia*
§ *e-mail: jvelasco@univalle.edu.co*

(Recibido: Abril 10 de 2007 - Aceptado: Noviembre 9 de 2007)

Resumen

Este artículo presenta el diseño de un carné de identificación universitario mediante tarjetas inteligentes. Este diseño se concibe para una aplicación multipropósito y la seguridad se implementa en el micro-circuito integrado de la tarjeta usando curvas elípticas sobre GF(2^{163}). El carné se diseña usando tarjetas *BasicCards*, las cuales permiten que el diseñador de la aplicación determine los parámetros relacionados con la seguridad y con la generación de claves, para lo cual se tienen en cuenta los recursos de hardware disponibles en la tarjeta inteligente, el nivel de seguridad y los procedimientos de verificación. Con el propósito de verificar la funcionalidad y la seguridad del carné diseñado, varias pruebas se llevaron a cabo sobre las tres aplicaciones desarrolladas: administrador, servicio médico y centro deportivo universitario. Teniendo en cuenta la alta flexibilidad en la implementación y el alto nivel de seguridad para estas tres aplicaciones, las tarjetas inteligentes pueden considerarse como la solución más eficiente para controlar todas las actividades y procedimientos realizados en un campus universitario; es decir, un carné inteligente es la mejor solución para realizar la identificación, el control de acceso y la prestación de servicios cuando existe una variedad de servicios y usuarios.

Palabras clave: Criptografía, Carné universitario, Curvas elípticas, Tarjetas inteligentes.

ELECTRONICS ENGINEERING

Design of a university identification card by means of smart cards

Abstract

This article presents the design of a university identification card by means of smart cards. This design is based on a multipurpose application and the security is implemented into the card's microchip by means of elliptic curves over GF (2^{163}). The card is designed using *BasicCards*, which allow the designer of the application to determine the parameters related to the security and the generation of keys, for which the resources of hardware available in the smart card, the level of security and the procedures of verification must be considered. To check the functionality and the security of the designed card, several tests were carried out on the three developed applications: administrator, medical service and university sport center. From the consideration of the wide flexibility in the implementation and the high level of security for these three applications, it follows that the smart cards may be regarded as the most efficient solution to control all activities and procedures carried out in the university campus; that is, an intelligent card is the best solution to carry out the identification and the control of access and for the benefit of services when it exists a variety of services and users.

Keywords: Cryptography, University identification card, Elliptic curves, Smart cards.

1. Introducción

La identificación de usuarios y el control de acceso se puede realizar de diversas maneras. Actualmente, en muchos casos, la identificación de usuarios se realiza con un carné que contiene datos estáticos, es decir, el carné tiene impresos los datos de la persona con su respectiva fotografía, y contiene un dato único que lo identifica ante un sistema de control o un sistema central de información.

Los sistemas de identificación con las características anteriores más usados son: códigos de barras, tarjetas de banda magnética y tarjetas de radiofrecuencia. En estos casos, una aplicación de software se encarga de leer los datos que identifican al usuario para posteriormente enviarlos y verificarlos ante el sistema central de información. Este tipo de aplicación presenta algunas limitaciones para la seguridad del sistema, por ejemplo, las tarjetas de banda magnética usadas en entidades financieras, pueden ser leídas y copiadas muy fácilmente, causando fraudes en el sistema financiero. Una solución es usar la tecnología de tarjetas inteligentes (*smart cards*), las cuales suministran un muy alto nivel de seguridad debido al uso de algoritmos criptográficos y adicionalmente pueden incorporar diversas aplicaciones, proporcionando una mayor eficiencia y flexibilidad.

Teniendo en cuenta las consideraciones anteriores, este artículo presenta el diseño de un carné universitario usando tarjetas inteligentes, que son la mejor alternativa tecnológica para implementar las diversas actividades y procedimientos que se llevan a cabo en un ambiente universitario.

Este trabajo está organizado de la siguiente forma: inicialmente, la Sección 2 describe algunas consideraciones tecnológicas sobre tarjetas inteligentes. Posteriormente, la Sección 3 presenta el diseño de un carné universitario usando tarjetas inteligentes, y finalmente la Sección 4 presenta las conclusiones de este trabajo.

2. Consideraciones tecnológicas de las tarjetas inteligentes

Una tarjeta inteligente es una tarjeta que usa un circuito integrado que es capaz de almacenar y procesar información. En el caso de tarjetas inteligentes, el circuito integrado es un microcomputador (Hansmann et al., 2002; Chen, 2000).

2.1 Aplicaciones comunes

Una tarjeta inteligente es un computador portátil, que puede ser usado para almacenar información confidencial con alta seguridad usando una clave secreta. En el caso de dinero electrónico, la tarjeta puede almacenar el saldo actual de la cuenta bancaria sin necesidad de estar en línea con el banco, debido a su capacidad para procesar y almacenar datos.

Una de las características más importantes de las tarjetas inteligentes es la seguridad para la información, debido a que computacionalmente es casi imposible copiar o alterar la información almacenada. Por lo tanto, las tarjetas inteligentes son la mejor alternativa tecnológica para llevar a cabo las transacciones financieras (Hansmann et al., 2002). Sin embargo, las tarjetas inteligentes pueden ser usadas en muchas aplicaciones (Hansmann et al., 2002; Chen, 2000; Hendry, 2001; Jurgensen & Guthery, 2002), tales como:

Sistema de acceso y control. La tarjeta inteligente puede ser usada para almacenar los datos requeridos para abrir una puerta, autenticar el uso de un computador, o puede ser usada para pagar en la cafetería de una institución.

Sector bancario. La tarjeta inteligente puede ser usada en una red pública para la autenticación entre el usuario y la entidad bancaria, lo cual es más seguro que las contraseñas usadas hoy en día en las tarjetas de banda magnética.

Sistema de transporte masivo. La tarjeta inteligente puede reemplazar los tiquetes, y la tarifa correspondiente puede ser calculada de acuerdo a la distancia. Esto puede realizarse

cuando el usuario abandone el sistema de transporte masivo y la tarifa puede ser deducida de la tarjeta en ese instante. Usando una tarjeta sin contactos, el viajero puede incluso dejar la tarjeta en su bolsillo.

Industria de las telecomunicaciones. Las tarjetas telefónicas prepago no requieren mantenimiento y ofrecen un mecanismo antifraude para acceder a teléfonos públicos sin necesidad de usar monedas. Actualmente, las compañías de telecomunicaciones inalámbricas usan tarjetas inteligentes para la seguridad. Un teléfono inalámbrico GSM tiene un módulo para la identificación del subscriptor (conocido como SIM, que significa *Subscriber Identity Module*), el cual es una tarjeta inteligente. La tarjeta SIM identifica al usuario y suministra claves de encriptación para la transmisión digital de voz. Estas claves generadas por la tarjeta SIM son temporales y se cambian cada vez que se usan, lo cual hace que sea muy difícil interceptar números telefónicos en los teléfonos celulares.

Sector de la salud. La tarjeta inteligente facilita el manejo de la información o de la historia clínica de los pacientes. La tarjeta puede almacenar datos para administrar la asignación de los beneficios y procedimientos para los pacientes; además, la tarjeta puede almacenar información de clínicas, hospitales y farmacias.

Internet. Una tarjeta inteligente puede ser usada para la autenticación de usuarios mediante firmas digitales, lo cual permite controlar el acceso a páginas web y realizar transacciones de forma segura.

2.2 Clasificación de las tarjetas con circuito integrado

En la Figura 1 se muestra la clasificación de las tarjetas con circuito integrado teniendo en cuenta la función que realizan (Chen, 2000).

2.2.1. Tarjetas con solo memoria (*memory cards*)

En este tipo de tarjetas, el circuito integrado es una simple memoria con interfaces I/O. Estas tarjetas son usadas principalmente para sistemas de pago, tales como teléfonos públicos y servicios. Las tarjetas pueden ser programadas, en su mayoría, usando cualquier lector de tarjetas inteligentes y se pueden clasificar de la siguiente manera:

Tarjetas sin protección. Estas tarjetas contienen una memoria que puede ser leída directamente a través de los contactos usando un protocolo asíncrono. De hecho, esa memoria se usa en algunas tarjetas telefónicas que no requieren de mayor seguridad.

Tarjetas protegidas. Las tarjetas protegidas tienen, como mínimo, un área protegida. La memoria de estas tarjetas generalmente es EEPROM, la cual se divide en dos áreas de acceso restringido.

Tarjetas de lógica segura (*secure-logic*). Estas tarjetas controlan el acceso a la memoria y pueden restringir la lectura o escritura por parte de aplicaciones externas**.** Son usadas para aplicaciones que requieren un alto grado de seguridad, como por ejemplo, tarjetas telefónicas modernas, tarjetas de transporte público y tarjetas prepago (Hendry, 2001).

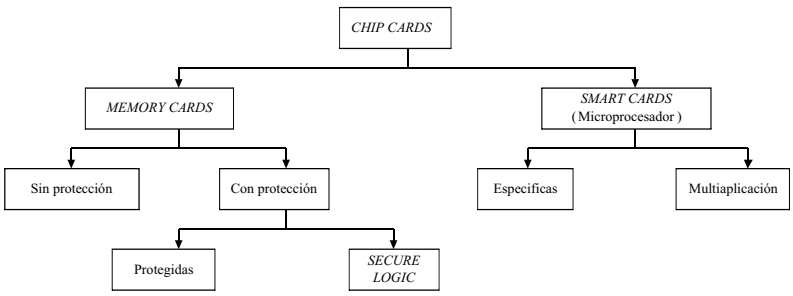

Figura 1. Clasificación de las tarjetas con circuito integrado.

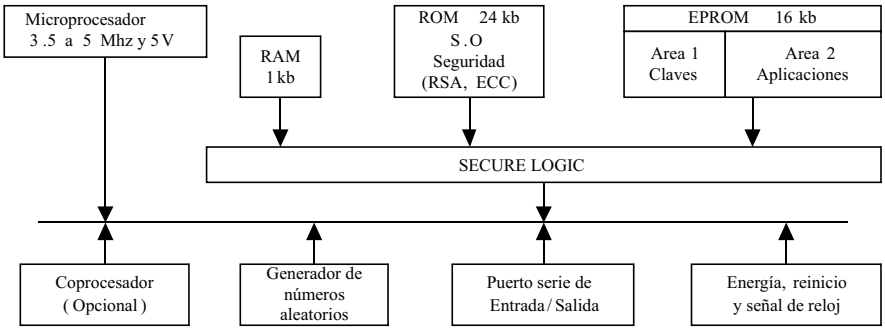

Figura 2. Componentes de una tarjeta inteligente.

2.2.2. Tarjetas inteligentes

En este tipo de tarjetas el circuito integrado contiene los siguientes elementos: procesador, memorias, interfaces I/O y circuitos de seguridad. En una tarjeta con microprocesador, los datos nunca están disponibles para aplicaciones externas porque tienen que pasar a través del microprocesador.

La mayoría de los fabricantes de tarjetas inteligentes adoptaron la arquitectura convencional de von Neumann (Hansmann et al., 2002; Hendry, 2001), como se muestra en la Figura 2.

En esta tarjeta, los datos pasan a través de un bus, bajo el control del bloque *Secure-Logic*, el cual controla el acceso a las memorias. En la memoria se almacenan las claves secretas propias de la tarjeta.

Las tarjetas inteligentes son muy adecuadas para aplicaciones que requieren realizar funciones criptográficas especializadas. En este caso, muchas de estas funciones requieren aritmética que usa operandos muy grandes ocasionando que el procesador se torne demasiado lento. Por esta razón, algunas tarjetas inteligentes tienen un coprocesador aritmético, el cual ayuda a procesar las funciones criptográficas. Por ejemplo, Trujillo-Olaya et. al. (2005) presentan el diseño de un criptoprocesador para tarjetas inteligentes.

Algunas tarjetas tienen un circuito generador de números aleatorios, el cual se usa cuando se requiere autenticación bidireccional.

Estas tarjetas también tienen un simple puerto de entrada / salida, un puerto serial bidireccional o una interface inalámbrica.

2.3 Software-hardware de seguridad para tarjetas inteligentes

Las tarjetas inteligentes usan módulos de encriptación como medio de autenticación. La criptografía es usada principalmente para autenticar entidades, como usuarios, tarjetas, y terminales (lector de tarjetas inteligentes conectado a un PC).

Los sistemas y programas pueden beneficiarse del uso de la criptografía, suministrando las siguientes características de alta seguridad, las cuales son mutuamente independientes:

- **confidencialidad**: garantiza privacidad, evitando que personas no autorizadas puedan ver los datos.

- **integridad**: garantiza exactitud, pues los datos originales no pueden ser cambiados sin previa autorización.

- **autenticidad**: garantiza la verdadera identidad, es decir, la persona que se está comunicando electrónicamente es realmente quien afirma ser.

En los sistemas de encriptación existen tres tipos de datos, los cuales son procesados por un algoritmo de encriptación. El primero es el texto plano (*plaintext*), el cual es un dato sin encriptar. El segundo es el dato encriptado, el cual es

conocido como texto cifrado (*ciphertext*); y el tercero es la clave (*key*), una o más de las cuales son requeridas para la encriptación y la desencriptación.

Generalmente, los algoritmos criptográficos usados en tarjetas inteligentes son orientados a bloques, de modo que el texto plano y el texto cifrado solamente pueden ser procesados en paquetes con longitud fija. La desencriptación es el proceso inverso de la encriptación, es decir, se toma el texto cifrado para recuperar el texto original. Conceptualmente, se puede pensar que una clave es un valor secreto, una contraseña o un PIN, pero en realidad una clave es una secuencia de números, y se usa en la formulación matemática del algoritmo criptográfico.

Por lo tanto, si se encripta el mismo texto plano con diferentes claves, se obtienen diferentes textos cifrados. Recíprocamente, el texto plano se puede recuperar partiendo del texto cifrado, usando la clave apropiada. Usar claves secretas en los algoritmos de transformación, permite que éstos puedan ser de dominio público sin perder seguridad (Jácome-Calderón, 2003).

2.4 Criptosistemas basados en curvas elípticas

El criterio para seleccionar un algoritmo criptográfico y la longitud de la clave es el costo y el esfuerzo requeridos para encontrar la clave o romper la seguridad, que deberían ser mayores que la máxima recompensa posible. Este criterio es importante para los sistemas basados en tarjetas, debido a que éstas tienen un limitado rango de algoritmos y longitudes de clave disponibles.

En este contexto, las criptosistemas basados en curvas elípticas son la solución más eficiente y económica. Los algoritmos de encriptación basados en curvas elípticas son más rápidos que un algoritmo RSA y requieren claves de tamaño menor para el mismo nivel de seguridad. Por ejemplo, se requiere la misma complejidad computacional para romper un ECC (*Elliptic Curve Cryptosystem*) con una clave de 160 bits que para romper un algoritmo RSA con una clave de 1024 bits. Un ECC con una clave de 320 bits, con referencia al criterio computacional, corresponde a un sistema RSA con clave de 5120 bits.

Las ventajas de las curvas elípticas las convierten en excelentes candidatas para ser usadas en tarjetas inteligentes. La computación puede ser realizada incluso sin coprocesador criptográfico y la clave puede ser almacenada en la memoria de la tarjeta inteligente debido a su pequeño tamaño. Sin embargo, las tarjetas inteligentes pueden usar un criptoprocesador de alto desempeño como el presentado por Trujillo-Olaya et al. (2005).

Además de los procedimientos de encriptación, los algoritmos criptográficos permiten realizar los procedimientos de autenticación para verificar la identidad y autenticidad en la comunicación entre entidades. En este caso, los procesos de autenticación pueden ser estáticos o dinámicos. En un procedimiento estático, los mismos datos son siempre usados para la autenticación, mientras que en un procedimiento dinámico, cada autenticación está basada en datos diferentes. También existe una diferencia fundamental entre procedimientos de autenticación unilateral y mutua.

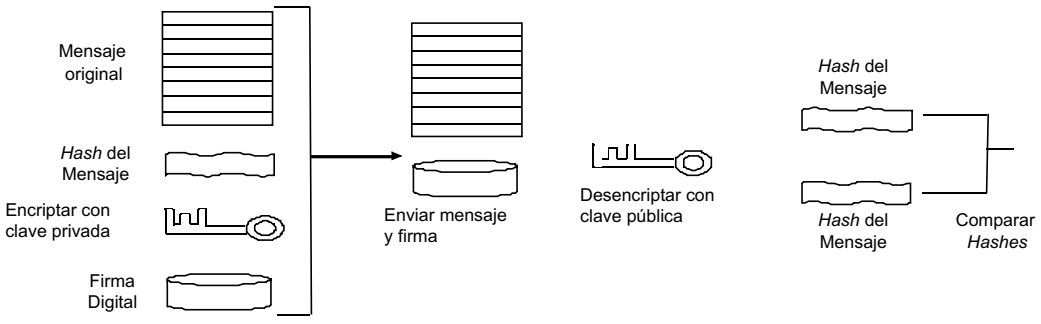

Figura 3. Procedimiento para verificar una firma digital.

La autenticación unilateral establece la autenticidad de una de las dos partes de la comunicación, y la autenticación mutua establece la autenticidad de ambas partes de la comunicación.

Para establecer la autenticidad de mensajes o documentos transmitidos electrónicamente se realizan firmas digitales (U.S. Department of Commerce / NIST, 2000). Es posible determinar si el mensaje o documento ha sido alterado mediante la verificación de la firma digital, como se muestra en la Figura 3.

Una firma digital es generada por una persona, pero puede ser verificada por cualquiera que reciba el mensaje, o quien tenga disponible una copia para la comparación. Una de las características especiales de las firmas digitales es que sólo una persona o una tarjeta inteligente pueden firmar un documento.

Generalmente, el mensaje o documento para ser firmado tiene el tamaño de varios kb. Entonces, es necesario hacer una compresión de los datos por medio de una función *hash*. Esta compresión no es reversible, es decir, los datos originales no pueden ser reconstruidos a partir del valor *hash*.

3. Carné universitario mediante tarjetas inteligentes

En el diseño de aplicaciones basadas en el uso de tarjetas inteligentes se deben tener en cuenta varias consideraciones, las cuales dependen en gran parte del tipo de aplicación. Desde el punto de vista técnico, estas consideraciones se encuentran muy relacionadas con el nivel de seguridad, la funcionalidad y los recursos de hardware disponibles en la tarjeta inteligente. Teniendo en cuenta estas consideraciones, se diseñó e implementó un carné universitario usando tarjetas inteligentes, el cual permite identificar usuarios con alto nivel de seguridad, registrar actividades o procedimientos y almacenar datos con autorización.

En este caso, el carné universitario es desarrollado para implementar aplicaciones propias de la Universidad del Valle.

Figura 4. Interfaz de la aplicación ***Administrador****.*

Inicialmente, el carné se debe personalizar usando la aplicación *Administrador* y luego el usuario debe registrar el PIN o clave secreta mediante la aplicación *Usuario*. Una vez se haya realizado este proceso, el usuario está habilitado para llevar a cabo una actividad o procedimiento en particular usando el carné; es decir, el usuario puede usar el centro deportivo, el servicio médico, la cafetería, la biblioteca, los parqueaderos, los laboratorios, las salas de cómputo, etc.

En este contexto, se desarrollan varias aplicaciones con el propósito de implementar funcionalmente un carné universitario. Las principales aplicaciones se describen a continuación.

3.1. Aplicación *Administrador*

La aplicación *Administrador* despliega la ventana que se muestra en la Figura 4, y permite llevar a cabo la personalización del carné y los procedimientos referentes a la seguridad. En este caso, los procedimientos son los siguientes:

1) Autenticación de la tarjeta. Este procedimiento verifica la autenticidad de la tarjeta inteligente. En este caso, el programa *Terminal* (la aplicación *Administrador*) busca en la tarjeta el programa *OnCard*, el cual tiene el ID de la tarjeta y la aplicación solamente leerá las tarjetas válidas, es decir, las que tienen el programa *OnCard* adecuado.

2) Generación de la curva elíptica. Inicialmente, se digitan los datos del formato de la aplicación y se presiona el botón *Personalizar* para enviar la información a la tarjeta. Sin embargo, antes de transferir la información, la aplicación primero verifica que los datos estén completos y después permite buscar los parámetros para la generación de la curva elíptica, la cual es usada para implementar los procedimientos criptográficos.

3) Generación de las claves para el programa terminal y la tarjeta. Una vez los programas *Terminal* y *OnCard* tienen la misma curva elíptica, se generan la clave privada para el programa *Terminal* y las claves pública y privada para la tarjeta, las cuales son generadas por la misma tarjeta. En este procedimiento, primero se genera la clave privada de la tarjeta de forma aleatoria, y con el propósito de alcanzar mayor seguridad, la generación aleatoria se hace a partir de un banco de datos, los cuales cambian para cada tarjeta. El banco de datos se compone de algunos valores aleatorios y algunos datos del usuario, por ejemplo los nombres, el número de la cédula, etc.

Usando este procedimiento, la generación de la clave privada de la tarjeta permite entonces garantizar que las claves para otras tarjetas son completamente distintas.

Es importante destacar que para la generación de las claves, el programa *Terminal* solamente envía el banco de datos a la tarjeta y no envía su clave privada. Similarmente, la tarjeta no envía su clave privada al programa *Terminal*; es decir, la clave privada nunca sale de la tarjeta, por lo tanto, no existe la posibilidad de ser interceptada en la comunicación con un programa *Terminal*. En este caso, la tarjeta solo envía al programa *Terminal* la clave pública.

4) Generación de la firma digital. Después de generar las claves de encriptación se pueden llevar a cabo los otros procedimientos referentes a la seguridad. Por ejemplo, la tarjeta puede generar una firma digital. En este caso, el programa *Terminal* produce un número aleatorio y lo envía a la tarjeta, con este número la tarjeta genera la firma digital y la envía al programa *Terminal*.

El programa *Terminal* (que en este caso es la aplicación *Administrador*) usa el número aleatorio, la firma digital y la clave pública de la tarjeta para verificar la autenticidad de la firma digital. Entonces, con el propósito de llevar a cabo esta verificación, el programa *Terminal* genera un valor *hash* a partir del número aleatorio que generó previamente; con este valor y la clave pública de la tarjeta, entonces verifica la autenticidad de la firma digital.

El procedimiento descrito anteriormente tiene como objetivo verificar la seguridad en el canal de comunicación y la integridad de los datos que se envían.

5) Generación del secreto compartido. Una vez el programa *Terminal* ha comprobado la firma digital, este programa genera y envía su clave pública a la tarjeta, la cual genera y almacena en su memoria EEPROM un dato que se conoce como secreto compartido (*shared secret*). Entonces, para generar el secreto compartido se requiere usar un algoritmo asimétrico, en este caso, el EC-167, ECC para GF(2^{167}), el cual proporciona un alto nivel de seguridad y tarda cerca de 2 s en generar este dato. Lo importante es que este procedimiento se realiza una sola vez en el ciclo de vida de la tarjeta. El secreto compartido es muy importante en la seguridad del criptosistema. Es por esta razón que primero se realizó una verificación por medio de la firma digital.

6) Generación de claves de sesión. Usando el dato del secreto compartido y los valores de los parámetros de derivación de claves (KPD), se generan las claves de sesión para el programa terminal y la tarjeta, las cuales son claves criptográficas simétricas, es decir, estas claves sirven para encriptar y desencriptar datos usando algoritmos simétricos. Los valores KPD se generan en el programa *Terminal* y son enviados a la tarjeta para que ésta genere la clave de sesión. En este caso, ambas partes de la comunicación tienen la misma clave de sesión, sin importar que el canal de comunicación sea inseguro, porque la clave de sesión que se utilizará se genera en ambas partes y se borra después de cada transferencia.

7) Encriptación de datos. La clave de sesión se utiliza para encriptar los datos personales del usuario (nombres, apellidos, cédula, etc.) con el algoritmo *Triple-DES*. Estos datos encriptados se envian a la tarjeta, se desencriptan y se almacenan en la memoria, para ser usados en otras aplicaciones.

8) Generación del PIN del usuario. La aplicación *Administrador* crea un PIN inicial para la tarjeta. En este caso, son los últimos cuatro dígitos de la cédula del usuario. Sin embargo, por seguridad, el usuario debe cambiar el PIN una vez reciba la tarjeta. Si la tarjeta es bloqueada por el usuario en cualquiera de las aplicaciones que requieren PIN, la aplicación *Administrador* permite generar un nuevo PIN.

Con el propósito de alcanzar un control más riguroso, cada vez que se personaliza el carné se registra la fecha, la hora y los datos principales del usuario en archivos clasificados por la categoría del usuario (estudiantes, profesores, empleados, trabajadores y médicos), y se calcula la fecha de expiración, la cual dependerá del semestre en que se personalizó la tarjeta.

Figura 5. Interfaz de la aplicación ***Usuario****.*

3. 2. Aplicación *Usuario*

En la Figura 5 se muestra la interfaz de la aplicación *Usuario*, la cual realiza o permite llevar a cabo los siguientes procedimientos:

1) Autenticación de la tarjeta. Inicialmente, esta aplicación verifica la autenticidad de la tarjeta inteligente de manera similar a la llevada a cabo en la aplicación *Administrador*.

2) Verificación de la vigencia del carné. La aplicación *Usuario* verifica la vigencia del carné mediante el envío a la tarjeta de la fecha actual, la cual se compara internamente con la fecha de vencimiento y determina si la tarjeta puede ser usada por la aplicación.

3) Verificación del PIN del usuario. Este procedimiento verifica que la tarjeta no tenga el PIN bloqueado o vencido.

4) Cambiar el PIN. Con este procedimiento, los usuarios pueden cambiar el PIN, para lo cual se utiliza el botón *CambiarPIN*. En este caso, primero se digita el PIN actual, y después el nuevo PIN y la confirmación de este último. La aplicación verifica que los datos ingresados sean correctos, y envía el PIN actual a la tarjeta, el cual se compara con el PIN que tiene en su memoria. Entonces, si el PIN actual es correcto, la aplicación envía el nuevo PIN para reemplazar el existente. Pero, si el PIN no es correcto, el programa de la tarjeta registra internamente este evento iniciando un conteo de errores. En este caso, el PIN será bloqueado cuando el usuario ingrese más de tres veces un PIN incorrecto.

5) Consultar datos. Con este procedimiento**,** los usuarios puedan consultar los datos registrados en la tarjeta. En el caso de los préstamos, se utiliza el botón *VerPréstamos* y la aplicación muestra un mensaje con el nombre del elemento, la cantidad y la fecha en la que se realizó tal préstamo. También, se pueden consultar los medicamentos recetados, las multas, etc., adicionando un nuevo botón, por ejemplo *VerDatos*.

3.3. Aplicación *CDU*

La aplicación *CDU* es para acceder al centro deportivo universitario, la cual tiene las características típicas de un sistema para controlar el préstamo de elementos deportivos y el acceso a servicios como piscina, gimnasio de pesas, cancha de tenis, etc.

Inicialmente, la aplicación *CDU* realiza los mismos procedimientos de seguridad realizados en la aplicación *Usuario* tales como: autenticación de la tarjeta, verificación de la vigencia del carné y la verificación del PIN del usuario.

Una vez cumplidos estos procedimientos, se realiza una autenticación dinámica y asimétrica, por medio de una firma digital, y si la autenticación es exitosa, la aplicación lee los datos desde la tarjeta, los cuales se pueden observar usando la ventana que se muestra en la Figura 6.

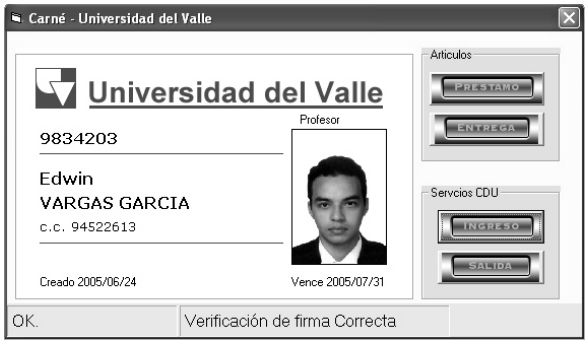

Figura 6. Interfaz de la aplicación ***CDU****.*

En este caso, en la ventana se habilitan los botones *préstamo y entrega de artículos*, e *ingreso a servicios del CDU*.

Préstamo y entrega de artículos. En esta aplicación, el botón *Préstamo* permite seleccionar los artículos deportivos y la cantidad deseada. Inicialmente, la aplicación solicita una autorización para el préstamo, la cual se realiza por medio del PIN del usuario. Después de digitar el PIN, la aplicación verifica si ya se ha registrado en la tarjeta algún préstamo. Si esto es verdad, la tarjeta envía al programa *Terminal* el nombre del artículo, la cantidad y la fecha en la que se realizó el préstamo, y por lo tanto no autoriza un nuevo préstamo. En caso contrario, la tarjeta registra el préstamo con la respectiva fecha y hora.

Para devolver un artículo deportivo, esta aplicación usa el botón *Entrega*. En este caso, el usuario debe ingresar el PIN y la aplicación permite realizar el procedimiento de entrega, es decir, la aplicación primero muestra los préstamos registrados y después registra en la tarjeta la fecha y la hora de la entrega del artículo. Con este procedimiento, el usuario queda a paz y salvo con el centro deportivo universitario.

Uso de las instalaciones del CDU. En esta aplicación, el botón *Ingreso* permite usar una instalación del CDU. En este caso, la aplicación solicita el ingreso del PIN del usuario y verifica que el usuario no está haciendo uso de otra instalación, es decir, la aplicación lee la información registrada en la tarjeta para controlar el acceso a una zona determinada. Por ejemplo, el usuario solamente puede estar en el gimnasio o en la piscina, pero no en ambos sitios simultáneamente.

Cuando el usuario termina su actividad deportiva, el usuario debe registrar su salida de la instalación del CDU. En este caso, el botón *Salida* de la aplicación y el PIN del usuario permiten registrar en la tarjeta la fecha y la hora de la salida de la instalación deportiva y observar la información del último ingreso.

3.4. Aplicación *ServicioMédico*

La aplicación *ServicioMédico* incorpora características básicas de una tarjeta médica (*HealthCard*), la cual es una tarjeta inteligente que contiene información personal y médica. La tarjeta puede ser leída por lectores de tarjetas instalados en PCs o terminales inteligentes, los cuales pueden estar ubicados en diferentes sitios de un servicio médico, como por ejemplo: hospitales, sistemas de emergencia médica móvil, farmacias, clínicas, consultorios particulares, etc.

Las principales ventajas que ofrece el uso de la tarjeta médica (*HealthCard*) es la reducción de gastos asociados a papelería, trámites y fraudes. Además, la tarjeta inteligente brinda un valor agregado como es el servicio *off-line* cuando no es posible acceder a la información centralizada (por ejemplo, sistemas de emergencia móvil y sistemas de salud sin conexión a un sistema central de información).

En la aplicación *ServicioMédico* se debe usar la tarjeta del médico para autorizar el servicio médico para los pacientes. En este caso, se realizan los mismos procedimientos de seguridad para la

tarjeta del médico y del usuario como en las anteriores aplicaciones.

Inicialmente, la aplicación *ServicioMédico* despliega la ventana que se muestra en la Figura 7, para llevar a cabo la autenticación de la tarjeta y del PIN del médico. Si los botones son habilitados, la aplicación registra el código del médico, el cual sirve para autorizar los procedimientos de los pacientes.

Figura 7. Interfaz de la aplicación ***ServicioMédico*** *cuando se usa la tarjeta del médico.*

Una vez la aplicación captura el código del médico, la tarjeta del médico se retira y se inserta la tarjeta del paciente. Si la verificación de la información de la tarjeta del paciente es correcta, se despliega una nueva ventana, tal como se ilustra en la Figura 8. En esta ventana se muestra la información del paciente, como tipo de sangre, sexo, etc. En este caso, se habilitan los botones de la ventana para observar o registrar datos del paciente.

El botón *AddDatos* permite que la aplicación registre en la tarjeta los procedimientos (hospital o clínica), los medicamentos (farmacia o droguería), alergias o enfermedades crónicas, el nombre del médico, la fecha y la hora de la consulta. En este caso, el médico asume la responsabilidad de la información que se registre en la tarjeta. Adicionalmente, para la Universidad del Valle es importante que la aplicación organice esta información de acuerdo al tipo de usuario.

Una consideración muy importante en esta aplicación, es la administración de la memoria disponible en la tarjeta debido a que se deben almacenar datos de tipo estático, como por ejemplo, nombres, apellidos, documento de identidad, etc. y datos de tipo dinámico, como medicamentos, procedimientos, etc. Por consiguiente, se deben usar estrategias eficientes para solucionar el problema del tamaño de la memoria.

Figura 8. Interfaz de la aplicación ***ServicioMédico*** *que muestra la información del paciente.*

En la aplicación *ServicioMédico* se utilizan diez registros para almacenar la información clínica del paciente, sin importar la diversidad de los datos; por ejemplo, el paciente puede usar los diez registros solamente para almacenar medicamentos, o cualquier otra combinación.

Las principales ventajas de esta aplicación son:

• Reducir los trámites en los procedimientos del servicio médico de la Universidad del Valle, debido a la seguridad de la información registrada en la tarjeta con la autorización del médico. Entonces, en un caso normal, el paciente no necesita autorizaciones o trámites adicionales, y por el contrario puede ir directamente a la farmacia para solicitar los medicamentos recetados en la consulta o al hospital (o clínica) en el caso de intervenciones quirúrgicas o tratamientos especializados requeridos por el paciente.

• Usar la información almacenada en la tarjeta en una emergencia o en una situación donde no se pueda acceder fácilmente a la historia clínica del paciente.

Un prototipo del carné universitario se muestra en la Figura 9, el cual fue implementado usando una tarjeta *Basic Card* (Guilfoyle, 2005).

Figura 9. Prototipo del carné universitario.

4. Conclusiones

En este trabajo se presentó el diseño de un carné universitario que permite realizar el control y la identificación de usuarios usando tarjetas inteligentes. En este caso, el diseño tiene en cuenta ciertas consideraciones técnicas, las cuales son diferentes a las requeridas por las aplicaciones desarrolladas para los computadores personales. Las principales consideraciones tenidas en cuenta en el diseño son los recursos de hardware disponibles en la tarjeta inteligente, el nivel de seguridad y los procedimientos de verificación.

Un mérito de la aplicación desarrollada radica en que los parámetros asociados a la seguridad y a la generación de claves son determinados por el diseñador, quién debe tener un excelente conocimiento sobre los criptosistemas basados en curvas elípticas. Entonces, esta capacidad de diseño permite alcanzar un control absoluto para implementar el más alto nivel de seguridad en el carné universitario. Sin embargo, es importante mencionar que existen muchos fabricantes de tarjetas inteligentes que limitan el uso de esta tecnología debido a que usan *cajas negras* para implementar la seguridad; es decir, la seguridad ya está programada y no es posible modificarla.

También es importante mencionar que una tarjeta inteligente puede realizar muchas verificaciones y procedimientos. En este caso, algunas funciones de verificación se diseñaron en el programa *Terminal* y los procedimientos de verificación sobre la autenticidad de la tarjeta, el PIN del usuario y la vigencia del carné se realizan en el procesador de la tarjeta utilizando una pequeña parte de la memoria, lo cual es otro de los méritos del diseño propuesto.

Finalmente, es importante concluir que el carné universitario basado en tarjetas inteligentes puede considerarse como la mejor alternativa tecnológica para implementar el control y la identificación de los usuarios en la Universidad del Valle, lo cual está sustentado por las grandes ventajas competitivas de las tarjetas inteligentes que garantizan el mayor nivel de seguridad para el manejo de la información.

5. Referencias bibliográficas

Chen, Z. (2000). *Java Card™ Technology for Smart Card: Architecture and Programmer's Guide.* Boston: Addison Wesley.

U.S. Department of Commerce / NIST (National Institute of Standards and Technology). (2000). *Digital Signature Standard* (*DSS*). *FIPS PUB 186-2*. http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf

Guilfoyle, T. (2005). *BasicCard developer manual v5.22*. http://www.basicCard.com/index.html?download.htm

Hansmann, U., Nicklous, M.S., Schäck, T., Schneider, A., & Seliger, F. (2002). *Smart card application development using Java.* Berlin: Springer.

Hendry, M. (2001). *Smart card security and applications*. Boston: Artech House Publishers.

Jácome-Calderón, G. (2003). *Implementación en hardware del algoritmo Rijndael*. Trabajo de grado, Escuela de Ingeniería Eléctrica y Electrónica, Universidad del Valle, Cali, Colombia.

Jácome-Calderón, G., Velasco-Medina, J., & López-Hernández, J. (2004). *Implementación en hardware del algoritmo Rijndael.* In Proceedings of X IBERCHIP Workshop, Cartagena, Colombia. http://www.iberchip.org/iberchip2004/articles/109-3-JAIMEVELASCO-VELASCO4-RIJNDAEL.PDF

Jurgensen, T.M., & Guthery, S.B. (2002). *Smart card: the developer's toolkit.* Boston: Prentice Hall.

Trujillo-Olaya, V., Velasco-Medina, J., & López-Hernandez, J.C. (2005). *Design of an elliptic curve cryptoprocessor over GF(2^{163})*. In Proceedings of XI IBERCHIP Workshop, Salvador Bahía, Brazil, p. 138-141. http://www.iberchip.org/iberchip2005/articles/78/78--jvelascoDESIGN%20OF%20AN%20ELLIPTIC%20CURVE%20CRYPTOPROCESSOR.pdf