CAMPUS
DE EXCELENCIA
INTERNACIONAL

Graduado en Ingeniería Informática

Universidad Politécnica de Madrid

Escuela Técnica Superior de
Ingenieros Informáticos

TRABAJO FIN DE GRADO

Control de asistencia mediante técnicas NFC

Autor: Sergio Conde Gómez

Director: Jorge Dávila Muro

MADRID, ENERO DE 2017

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

Resumen

El control de asistencia a clases y exámenes es una tarea tediosa pero necesaria de cara a evitar el fraude académico. Con la implantación de la asistencia obligatoria a clases se ha incrementado el número de fraudes cuando se usan listas de firmas como control. Por tanto se presenta la necesidad de un nuevo sistema que sea sencillo y seguro.

Mediante el uso de técnicas NFC se propone una solución a este problema válida para clases, exámenes o eventos. Esta solución permite validar la identidad de los asistentes mediante el uso medidas de seguridad, y por tanto evitar el fraude.

Palabras clave: control de asistencia, tarjeta sin contacto, seguridad, NFC.

Abstract

Control of students' attendance is a tedious but necessary task in order to avoid academic fraud. With the introduction of compulsory class attendance, the number of frauds has increased when lists of signatures are used to monitor this attendance. Therefore, the necessity for a new system, simpler and more secure, has arisen.

Through the use of NFC techniques, a solution to this problem is proposed, valid for classes, exams or events. This solution allows to validate the identity of the attendees by implementing security measures and consequently, to avoid fraud.

Keywords: control of attendance, contactless card, security, NFC.

1. INTRODUCCIÓN

El control de asistencia a clases se realiza tradicionalmente mediante el uso de una lista de firmas que los asistentes van rotando por la clase o el profesor pasando lista en voz alta. En el caso de la hoja de firmas se encuentra el problema de la falsificación de las mismas por parte de los asistentes desvirtuando así el sistema, mientras que el segundo método implica la pérdida de tiempo de clase por parte del docente.

En otros casos como es el de los exámenes se utiliza como asistencia el propio examen que dada la índole de esta situación la identidad del examinado es importante para evitar el fraude. Solo algunos pocos docentes realizan una verificación de la identidad del alumno examinado mirando su DNI[1] ya que en convocatorias con 200 alumnos o con hasta 5 aulas de examen se vuelve una tarea tediosa.

Para solucionar estos problemas se propone la creación de un sistema seguro y que no repercuta un alto coste a la universidad mediante el uso de técnicas de comunicación inalámbrica de corto alcance, también denominadas sin contacto o *contactless*. Para este fin se va a utilizar la tecnología NFC[2].

1.1. ¿Qué es la tecnología NFC?

Le tecnología NFC posibilita una forma sencilla de comunicación bidireccional entre dos dispositivos electrónicos permitiendo compartir información sin necesidad de una conexión física pero limitando a una distancia máxima de 4 centímetros entre los dispositivos a una velocidad de hasta 424 kbps.[1]

Entre las especificaciones publicadas por el NFC Forum[3] se define el uso de tarjetas de proximidad pasivas que se clasifican como tarjetas tipo 1, 2, 3 y 4[3]. Estas tarjetas se basan en el estándar ISO 14443 el cual está dividido en 4 partes:

ISO 14443-1 Describe las características físicas de las tarjetas sin contacto tales como el tamaño máximo de la antena (84 mm x 54 mm x 3 mm) y tolerancia al campo electromagnético[4].

ISO 14443-2 Describe las características del nivel físico tales como la potencia de la emisión, las frecuencia, el tasa de bits y la modulación[5].

ISO 14443-3 Describe las características del nivel de enlace tales como la forma de los paquetes de datos y el sistema anticolisión que es usado en el descubrimiento de tarjetas pasivas por parte del sistema activo[6].

[1] Documento Nacional de Identidad

[2] Near Field Communication

[3] El NFC Forum es una organización sin animo de lucro de la industria cuyos miembros son los distintos componentes del ecosistema NFC. Las organizaciones que lo componen comparten su experiencia en de desarrollo, aplicaciones y marketing para mejorar y avanzar en la creación de productos NFC mejorando la vida de los consumidores y promoviendo los objetivos empresariales de los miembros.[2]

ISO 14443-4 Describe un protocolo opcional para el nivel de transporte[7]. En la práctica las tarjetas pasivas comerciales suelen desarrollar su propio protocolo, aunque este estándar se encuentra implementado en múltiples aplicaciones como el pasaporte electrónico o en el DNIe español desde su versión 3.0 introducida en 2015[8].

Figura 1: Representación del estándar ISO 14443 según el modelo OSI

2. ESTADO DEL ARTE

El control de acceso mediante tecnologías inalámbricas es un campo de sobra investigado y con soluciones comerciales disponibles, sin embargo dichas soluciones se basan principalmente en el uso de RFID[4], tecnología en la que se basa NFC.

La tecnología RFID se diseñó para la identificación automática de objetos permitiendo obtener un identificador del mismo al atravesar un campo electromagnético. A los objetos se les añade pequeños chips o etiquetas (tags) las cuales tienen un identificador único que transmiten pero no pueden almacenar más datos o actuar como *smart card*[5] a diferencia de las etiquetas o tarjetas NFC.

Existen proyectos comerciales que pueden asemejarse al ámbito de este trabajo tales como el control de entrada y salida de paquetes en un almacén de forma que cada paquete tiene una etiqueta RFID que al pasar por la entrada o salida se lee y comprueba o apunta en la base de datos. Esto permite llevar un control automatizado del inventariado del almacén lo cual consigue de cierta forma uno de los requisitos de este trabajo. Otros proyectos que llevan años funcionando son los chips de identificación animal que trabajan con esta tecnología.

[4]Radio-Frequency Identification

[5]Una tarjeta inteligente (smart card), o tarjeta con circuito integrado, es cualquier tarjeta del tamaño del bolsillo con circuitos integrados, que permite la ejecución de cierta lógica programada.

Una de estas soluciones comerciales es *ClearStream RFID*[9] donde ofrecen desde opciones como la anterior hasta otras aplicaciones que permiten seguir en conferencias por que puertas pasa cada asistente permitiendo controlar el aforo.

Otro proyecto similar al que se presenta es el llevado a cabo por la Universidad Pontificia de Salamanca en colaboración con Samsung Electronics. En Enero de 2012[10] presentaron conjuntamente un proyecto piloto con dispositivos Samsung para el registro de asistencia a clase mediante tecnología NFC, esto permitiría a la universidad prescindir de que los docentes tengan que pasar lista permitiendo generar partes de asistencia durante el semestre de forma automática.

En Septiembre de 2013 se muestran los resultados de este proyecto en la publicación *Expert Systems with Applications*[11] donde se manifiesta una satisfacción general por parte de los docentes y el alumnado, sin embargo se manifiesta el problema de la falta de dispositivos con NFC.

En el artículo se hace una valoración indicando que al rededor del año 2016 la mayoría de alumnos tendrán un smartphone con NFC, sin embargo, a día de hoy, la tecnología NFC en los dispositivos móviles no se encuentra tan extendida como se esperaba en un principio y en el caso de algunos dispositivos que lo incorporan su uso esta reservado para el propio fabricante no pudiendo aprovecharlo desde aplicaciones de terceros. Este es el caso del iPhone de Apple[12].

La opción de proveer un dispositivo móvil con NFC a cada alumno sería muy costosa ya que además sería necesario realizar un mantenimiento y control sobre los propios dispositivos por lo que es necesario buscar una alternativa.

3. SOLUCIÓN PROPUESTA

3.1. Estudio de las soluciones disponibles

Realizando el estudio de las distintas tarjetas o etiquetas NFC se ha valorado distintas alternativas con las que trabajar. A continuación se detalla cada una de ellas explicando sus ventajas y desventajas.

3.1.1. DNIe 3.0

El DNIe 3.0 se presenta como una tarjeta de identificación con grandes ventajas. En esencia se trata de un dispositivo doble que funciona como una *smart card* con comunicación NFC o mediante un lector de chip que permite realizar operaciones criptográficas con una identidad digital *X.509*[6] la cual hace uso de criptografía asimétrica (par de cla-

[6]X.509 es un estándar para infraestructuras de claves públicas. X.509 especifica, entre otras cosas, formatos estándar para certificados de claves públicas[13].

ves publica y privada) o como pasaporte electrónico para la identificación electrónica de personas.

Figura 2: DNIe 3.0 de ejemplo

Existirían múltiples ventajas si se implementase el sistema haciendo uso del DNIe 3.0:

- Ahorro por parte de la universidad al no tener que expedir tarjetas a cada alumno.
- La tarjeta al usarse como una *smart card* que cumple con los estándares existentes al respecto de algoritmos y comunicación por lo que requiere poco esfuerzo a la hora de implementar una aplicación con ella. Si se usa como pasaporte electrónico las ventajas son las mismas al tratarse de un estándar ampliamente extendido.
- La identidad digital está expedida por el Estado español por lo que asegura su validez e identidad y proveen medios para comprobar el estado de la misma en tiempo real, por ejemplo OCSP[7].

Por otro lado las desventajas de usar el DNIe 3.0 para el sistema son las siguientes:

- El DNIe 3.0 se empezó a expedir a finales de 2015, sin embargo no existe la obligatoriedad de cambiar un DNI o DNIe antiguo por el nuevo modelo hasta que el documento no se encuentre en los 90 días previos a la fecha de caducidad. Los DNI antes de los 30 años (y después de los 5 años) tiene un periodo de validez de 5 años pudiendo hacer que, actualmente, existan alumnos que durante su vida académica no posean un DNIe 3.0.
- El control de la tarjeta lo tiene el Estado español y la universidad simplemente podría hacer uso de la misma.
- Requiere la introducción de un número de acceso (CAN[8]) para poder acceder a su información, sin embargo esto podría automatizarse leyendo los caracteres que se encuentran en el reverso mediante reconocimiento de imagen, si se quiere utilizar como pasaporte electrónico. Dichos caracteres cumplen con la normativa OACI[9] para documentos de viaje[14]. Si se desea utilizar como *smart card* con acceso a firma electrónica el CAN se encuentra en la esquina inferior derecha del frontal.

[7]Online Certificate Status Protocol - `https://en.wikipedia.org/wiki/Online_Certificate_Status_Protocol`

[8]Card Access Number

[9]Organización de Aviación Civil Internacional

Figura 3: CAN y zona MRZ (Machine Redable Zone) de un DNIe 3.0

- Para la realización de una firma de asistencia usando la identidad digital del DNIe se requiere introducir el PIN del DNIe lo cual requiere de un teclado completo, sin embargo podría realizarse simplemente la lectura de la información publica que provee el DNIe (nombre, apellidos, fecha de nacimiento, sexo y fotografía).
- Los alumnos Erasmus no disponen de esta tarjeta aunque si se implementa el sistema cumpliendo con la normativa de pasaporte electrónico estos alumnos podrían utilizar el pasaporte.

En un principio podría ser el dispositivo ideal de identificación usando su característica de pasaporte electrónico debido a su madurez y extensión, como se puede observar en la figura 4 siendo los países en verde oscuro los que actualmente lo utilizan y los verde claro los que están en proceso de inclusión. Sin embargo algunas características como la necesidad de introducir el CAN o la actual extensión del mismo hacen que no.

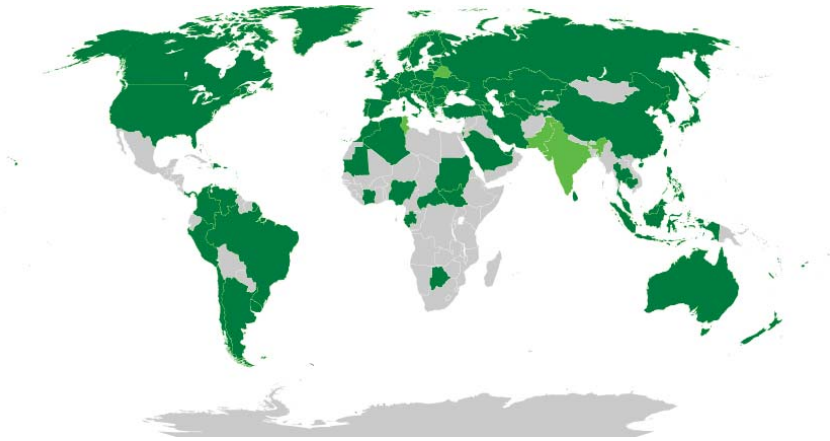

Figura 4: Expedición del pasaporte electrónico por países

3.1.2. MIFARE Classic

MIFARE es la marca de NXP Semiconductors, el principal fabricantes de chips NFC, bajo la cual se comercializan diferentes soluciones.

Este tipo de tarjetas se diseño para aplicaciones como tarjetas de socio, tickets de transporte o de acceso a eventos. Tienen una memoria de 1kB o 4kB dividida en diferentes sectores que pueden protegerse con diferentes claves.

El protocolo de comunicación es propietario aunque a día de hoy está ampliamente

documentado y tiene soporte en la mayoría de los lectores incluyendo en teléfonos con NFC.

Las ventajas de este tipo de tarjeta son:

- El coste de la tarjeta se encuentra entre 0.45€ y 0.55€ según el número que se compren.
- Los carnets universitarios de la Universidad Politécnica de Madrid que se solicitan sin cuenta bancaria cuentan con un chip NFC de este tipo[10].

Las desventajas de este tipo de tarjeta son:

- Existen ataques que permiten recuperar en horas las claves de los sectores de memoria lo cual permite leer, modificar y clonar su contenido.
- Mediante la interceptación de una comunicación entre tarjeta y lector se puede obtener la clave del sector de memoria leído, con la clave de ese sector puede realizarse otro tipo de ataque que permite recuperar rápidamente el resto de claves.
- Si se cambia el contenido de la tarjeta entre transacciones no se valida que el estado que la tarjeta da no es un antiguo.

A pesar de las desventajas pueden seguirse usando para ciertas aplicaciones si se es consciente de las limitaciones que presentan. NXP ha creado un documento donde se trata de la seguridad de estos chips NFC y una guía de buenas prácticas para proteger las implementaciones de estos ataques[15].

Del análisis del documento citado las cosas a tener en cuenta usando en estas tarjetas serían:

1. La información almacenada debe estar protegida criptográficamente de manera que dependa del identificador único tarjeta. Esta recomendación es necesaria aplicarla si se decide usar este tipo de tarjeta y es la única manera de asegurar el contenido de la tarjeta. Al depender del identificador de la misma un clon no serviría salvo que se clone a una tarjeta MIFARE Classic falsificada o con un emulador que permita cambiar dicho identificador. Sin embargo se puede vigilar que la tarjeta sea oficial.
2. Diversificar las claves de los sectores entre las diferentes tarjetas. Se puede implementar un método para que las claves de los sectores se generen en base a el identificador único de la tarjeta.
3. Usar un contador decremental de transacciones. Para este sistema no es necesario ya que, como se verá más adelante, no se va a modificar el contenido de la tarjeta.

[10] Al menos las que se han podido comprobar expedidas entre los años 2007 y 2011. No se han conseguido muestras de años siguientes.

3.1.3. MIFARE DESFire

Al igual que las tarjetas MIFARE Classic estas tarjetas están diseñadas por NXP.

Estas tarjetas utilizan un protocolo que cumple con el estándar ISO 14443-4 por lo que hacie que sean compatibles con cualquier dispositivo NFC que implemente el estandar.

Las ventajas de este tipo de tarjeta son:

- Su procesador está basado en el 8051 (Intel MCS-51[11]) el cual se encuentra acompañado de un acelerador criptográfico 3DES/AES permitiendo realizar operaciones utilizando 3DES[12] o AES[13] de manera rápida lo cual provee una robusta capa de seguridad en la transmisión y almacenamiento de los datos.
- Posee un sistema operativo que ofrece una estructura basada en directorios y ficheros haciendo que sea sencillo su uso. Esto supone una ventaja frente a las MIFARE Classic al no tener que gestionar la memoria por sectores.

Las desventaja principal de este tipo de tarjeta es que a pesar de poseer fuertes medidas de protección, tales como AES 128-bits, existen fallos en su diseño hardware que permiten clonar las tarjetas en un tiempo de unos 100ms[16].

3.2. Elección de la plataforma

Para el desarrollo del sistema se ha optado por el uso de tarjetas MIFARE Classic cuyas características principales se han visto en la sección 3.1.2.

Los motivos para la elección de esta tarjeta son la existencia de carnets universitarios con MIFARE Classic y la posibilidad de detectar modificaciones y clones. A pesar de que las tarjetas MIFARE DESFire pudieran parecer en un principio más seguros el hecho de que puedan clonarse de forma sencilla hace que pierdan su atractivo principal equiparándolas, para las características del sistema planteado, a las MIFARE Classic.

Para el desarrollo del sistema se va a trabajar sobre el modelo MIFARE Classic 1K el cual posee una memoria de 1KB de los cuales pueden usarse 768 bytes para el almacenamiento de datos.

La memoria de estas tarjetas de divide en 16 sectores de 64 bytes, cada sector posee 4 bloques de memoria de 16 bytes. Uno de estos bloques, denominado *sector trailer* se encuentra reservado para almacenar dos claves (Key A y Key B) de 6 bytes (48 bits) y 4 bytes para indicar el uso de las claves denominados *access bits*. En la figura 5 pode observarse el esquema de la memoria de este tipo de tarjetas.

[11] `https://en.wikipedia.org/wiki/Intel_MCS-51`

[12] Triple Data Encryption Algorithm - `https://en.wikipedia.org/wiki/Triple_DES`

[13] Advanced Encryption Standard - `https://en.wikipedia.org/wiki/Advanced_Encryption_Standard`

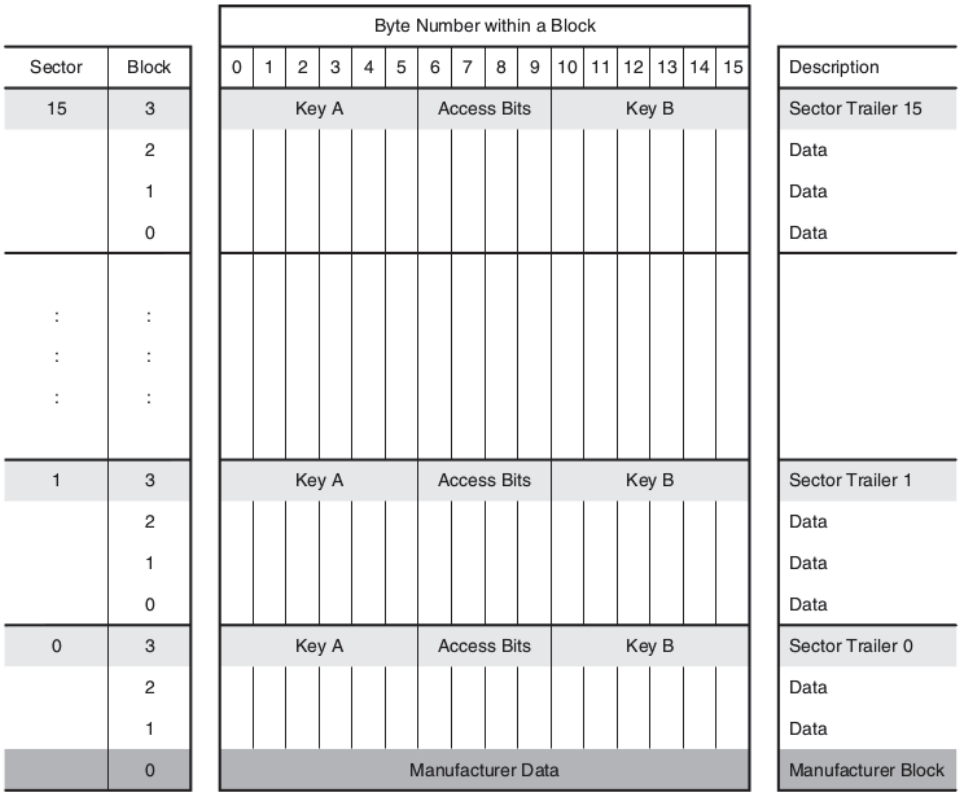

Figura 5: Estructura de memoria de una tarjeta MIFARE Classic 1K

Mediante los *access bits* se puede definir, para cada sector, que clave es necesaria para la escritura y lectura, además de otras operaciones que no vamos a utilizar tales como el incremento o decremento del contenido de un bloque. Como se puede observar en la figura 6 se trata de 3 bits que dada la secuencia de negación o no correcta de bit terminan formando 3 bytes.

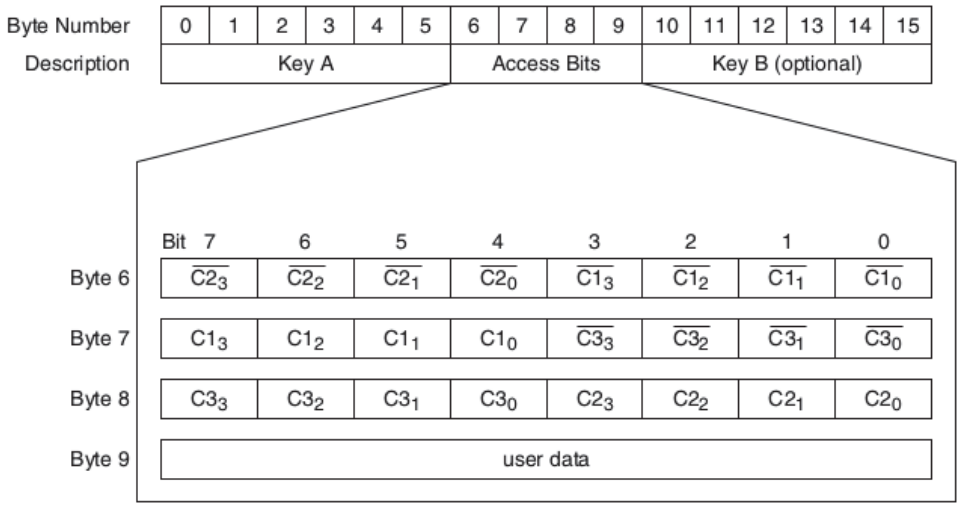

Figura 6: Formato de los access bits

El valor de dichos bytes termina las condiciones de acceso para cada sector, como se puede observar en la figura 7.

Access bits			**Access condition for**			
C1	C2	C3	read	write	increment	decrement, transfer, restore
0	0	0	key A|B	key A|B	key A|B1	key A|B
0	1	0	key A|B	never	never	never
1	0	0	key A|B	key B	never	never
1	1	0	key A|B	key B	key B[1]	key A|B
0	0	1	key A|B	never	never	key A|B
0	1	1	key B	key B	never	never
1	0	1	key B	never	never	never
1	1	1	never	never	never	never

Figura 7: Valores posibles para los access bits

Una característica especial del primer sector es que solo tiene disponibles dos bloques de memoria para almacenar datos, a diferencia del resto, ya que el primero de ellos se encuentra destinado a la información de la propia tarjeta donde podemos encontrar el identificador único y el fabricante de la misma.

4. DISEÑO DE LA APLICACIÓN

Para el desarrollo de la aplicación se ha elegido como lenguaje de programación C y el uso de la biblioteca *libnfc*[14] la cual se encarga la comunicación con los dispositivos hardware soportados e implementa, entre otros, la modulación y protocolo definidos por el estándar ISO 14443. Durante el desarrollo del sistema se ha utilizado la versión 1.7.1[15].

La biblioteca es compatible con el hardware nfc que haga uso de chips NFC NXP PN53x y ACR122, sin embargo estudiando la compatibilidad de los dispositivos publicada por los desarrolladores de la misma[17] se ha optado por el uso de un lector/escritor basado en el chip NXP PN533[16].

El dispositivo elegido con el cual se ha desarrollado y probado el sistema es el *NFC USB reader DL533N OEM*[17]. Sin embargo la biblioteca *libnfc* provee una API[18] que permite el uso de cualquier dispositivo soportado por la misma en la actualidad o que en un futuro soporte sin necesidad de cambiar el código.

Para las operaciones criptográficas se ha optado por el uso de la biblioteca *openssl*[19] ya que por su trayectoria es una de las usadas. La versión utilizada durante el desarrollo del sistema ha sido la 1.0.2i[20].

4.1. Generación de tarjeta (aplicación de escritura y lectura)

Tal como se explica en la sección 3.2 la tarjeta elegida se divide en 16 sectores (cuya numeración empieza por 0) con 48 bytes disponibles, cada uno a excepción del primer sector que dispone de 32 bytes, para almacenamiento de datos.

Como se observa en la tabla 1, en la tarjeta se guardará el nombre y apellidos del alumno así como su número de matrícula ya que estos datos son los relevantes desde el punto de vista de este sistema. Sin embargo quedará memoria libre suficiente por si en un futuro desea añadirse mas información.

[14] http://nfc-tools.org/index.php?title=Main_Page

[15] https://github.com/nfc-tools/libnfc/archive/libnfc-1.7.1.zip

[16] http://www.nxp.com/products/identification-and-security/nfc-and-reader-ics/nfc-controller-solutions/usb-nfc-integrated-solution:PN5331B3HN

[17] http://www.d-logic.net/nfc-rfid-reader-sdk/products/nfc-usb-card-size-reader-dl533n-oem

[18] Application Programming Interface (interfaz de programación de aplicaciones)

[19] https://www.openssl.org/

[20] https://github.com/openssl/openssl/archive/OpenSSL_1_0_2i.zip

Sector	Contenido
0	Vacío
1	Apellidos
2	Nombre
3	Número de matrícula
4	HMAC_SHA384(Sector 1)
5	HMAC_SHA384(Sector 2)
6	HMAC_SHA384(Sector 3)
7-15	Vacío

Tabla 1: Memoria de la tarjeta del alumno

4.1.1. Calculo del HMAC de la información almacenada

Tal como indica la tabla 1, los sectores 1, 2 y 3 contienen la información que se desea validar y en los sectores 4, 5 y 6 se almacena un HMAC[21] o código de autenticación de mensajes en clave-hash. El uso de un HMAC de los sectores permite que mediante el uso de una función hash y una clave secreta se pueda comprobar la integridad de los datos a la vez que se autentican para protegerse de una posible manipulación de los datos.

La función hash elegida para usar en el HMAC es SHA-384, la cual pertenece al conjunto de funciones hash SHA-2[22] y produce una salida de 384 bits lo que significa que obtenemos 48 bytes de salida pudiendo ser almacenado en el sector sin problemas.

El uso de un HMAC requiere de una clave conocida por el sistema de generación y de autorización. Esta clave se ha generado mediante el sorteo de 64 bytes (512 bits) de forma aleatoria haciendo un XOR con el identificador de la tarjeta (UID) para que sea dependiente de de cada tarjeta.

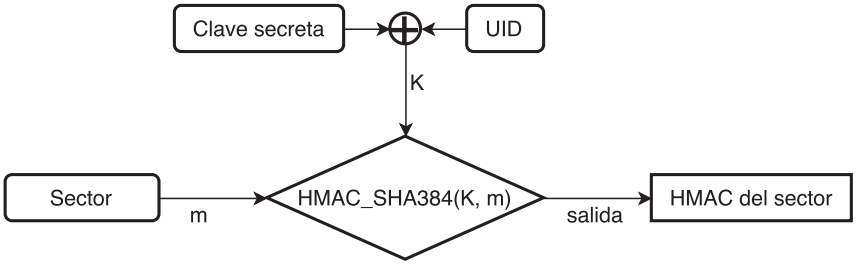

Figura 8: Diagrama del calculo del HMAC

[21] Keyed-Hash Message Authentication Code - https://en.wikipedia.org/wiki/Hash-based_message_authentication_code

[22] Secure Hash Algorithm 2 - https://en.wikipedia.org/wiki/SHA-2

4.1.2. Calculo de las claves de los sectores

Por último en la generación se necesita generar las claves de cada sector. Como se ha visto el la seción 3.2, cada sector, utiliza 2 claves de 48 bits (6 bytes) y que a pesar de solo utilizar 6 sectores de los 16 disponibles se deben cambiar las claves de todos los sectores y que sean diferentes entre si, tal como indica NXP en su guía de buenas practicas[15]. Teniendo en cuenta que la tarjeta tiene 16 sectores se requieren 1536 bits (192 bytes) para las claves.

Para la genración de claves diferentes para cada tarjeta y sector se ha optado por el uso de la función de derivación de claves PBKDF2[23] usando como función hash SHA-512. En este tipo de funciones puede especificarse el tamaño de la salida por lo que podemos obtener los 192 bytes necesarios para cubrir todas las claves. El valor de entrada de la función será el UID de la tarjeta y se usara una salt secreta que han sido sorteada de forma aleatoria.

Además este tipo de funciones requiere un número de iteraciones para hacer que un ataque por fuerza bruta sea complejo. A la hora de determinar un número de iteraciones se encuentra con que no se ha llegado a ningún consenso y distintas recomendaciones van de 10000 iteraciones hasta 200000. Uno de los factores importantes para el tiempo de calculo que supone el número de iteraciones es el tipo de hash utilizado ya que dependiendo de su construcción este podría ser fácilmente acelerado mediante hardware, por ejemplo usando computación distribuida o tarjetas gráficas mediante OpenCL o CUDA.

Finalmente se ha optado por el uso de 10000 iteraciones ya que, como se ha mencionado en la sección 3.1.2, existen ataques de fuerza bruta que permiten recuperar estas claves en horas y la validez de los datos que contiene la tarjeta se comprueba mediante un HMAC como se ha mencionado anteriormente.

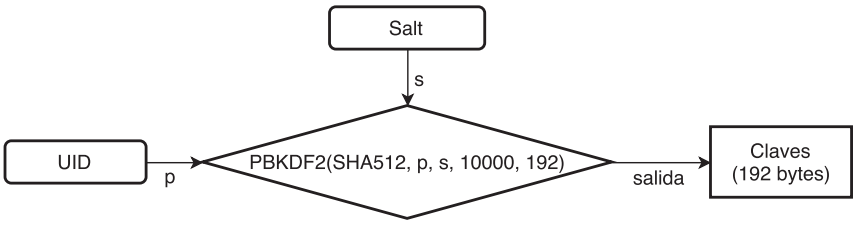

Figura 9: Diagrama del calculo del PBKDF2

El resultado del PBKDF2 se divide en bloques de 6 bytes (48 bits) y se va asignando en orden como clave A del sector 0, clave B del sector 0, clave A del sector 1, clave B del sector 2, ...

4.1.3. Funcionamiento del programa

El programa consta de dos partes, `generar_tarjeta` y `escribir_tarjeta`.

[23]Password-Based Key Derivation Function 2 - `https://en.wikipedia.org/wiki/PBKDF2`

La primera parte, `generar_tarjeta`, se encarga de la lectura del UID de la tarjeta presente en el lector y realiza el proceso de generación descrito anteriormente. Puede tomar como parámetros el nombre de un fichero de configuración y el nombre de un fichero de salida. El fichero de configuración sirve para una posible automatización de la generación y debe contener en la primera línea el o los apellidos del alumno, en la segunda su nombre y en la tercera el número de matrícula. De no utilizar el fichero de configuración estos datos se pedirán de forma interactiva. El nombre del fichero de salida por omisión es `tarjeta.mfd` pero puede seleccionarse el que se desee.

La segunda parte, `escribir_tarjeta`, simplemente se encarga de escribir el fichero de salida generado en la tarjeta, comprobando primero que el UID sea el correcto ya que de lo contrario no se escribirá la tarjeta.

4.2. Servicio de autorización

El servicio de autorización se encarga de la lectura y validación de las tarjetas.

Una vez el servicio se inicia queda a la espera de la presencia de una tarjeta en el lector, una vez se detecta la tarjeta se inicia el proceso de verificación el cual consiste en validar las medidas implementadas durante la generación.

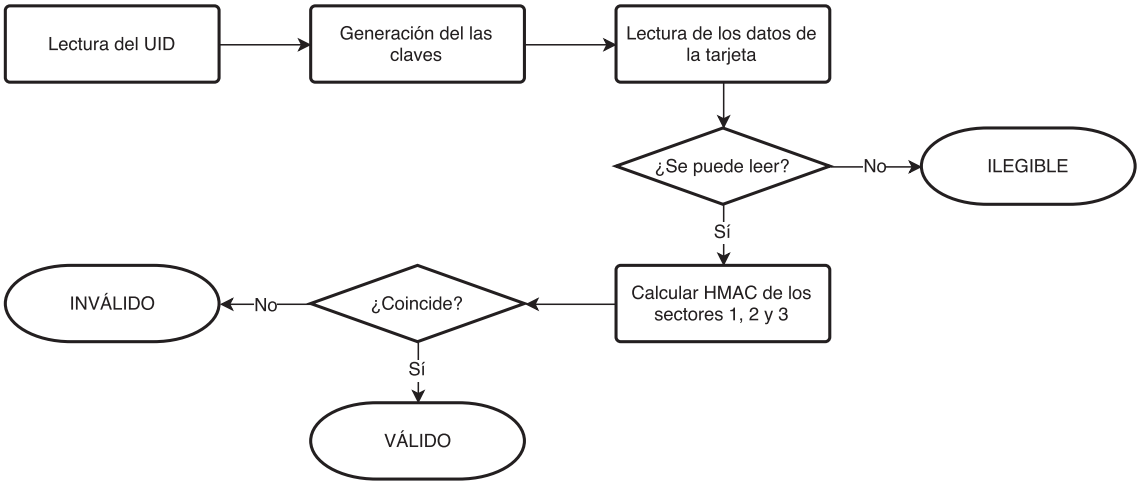

Figura 10: Diagrama de verificación

Lo primero que se realiza es la lectura del UID de la tarjeta y se procede al calculo de las claves, siguiendo el proceso explicado en la sección 4.1.2. Usando las claves calculadas se trata de leer los datos almacenados en la tarjeta.

Si esta lectura fallase significaría que las claves no pertenecen al UID de la tarjeta por lo que se estaría ante un posible intento de clonar otra tarjeta, en este caso saldríamos del proceso anotando el estado *ILEGIBLE*.

Si la lectura ha sido satisfactoria se procede al calculo del HMAC de los sectores 1, 2 y

3 tal como se describe en la sección 4.1.1. Una vez calculados los HMAC se comprueban con los almacenados en los sectores 4, 5 y 6 respectivamente.

Si los HMAC coinciden la verificación será satisfactoria y se anotaría como estado *VÁLIDO*. Si no coinciden, significaría que la información de la tarjeta ha sido manipulada y podría tratarse de un posible intento de falsificación de los datos por lo que se saldría del proceso anotando el estado *INVÁLIDO*.

Este proceso puede observarse en el diagrama de flujo de la figura 10.

4.2.1. Funcionamiento del programa

El programa `autorizacion` es el encargado de llevar el proceso anteriormente descrito y tan solo requiere ejecutarlo con un parámetro indicando el nombre del examen, asignatura o evento.

Opcionalmente se puede indicar un segundo parámetro indicando el fichero de configuración de la base de datos si se desea utilizar esta opción, ver sección 4.3.

El fichero de configuración de la base de datos debe contener los siguientes datos, cada uno en una línea nueva: ip o dominio del servidor, puerto, usuario, contraseña y nombre de la base de datos.

4.3. Generación y transferencia de registros

La generación de registros se encuentra integrada en el servicio de autorización sin embargo puede funcionar de dos maneras diferentes, registro en texto plano o registro en texto plano y escritura en base de datos.

La generación del registro en texto plano se trata de la anotación de la información leída de cada tarjeta junto a su estado de validación, explicado en la sección 4.2.

El formato de este registro es el siguiente:

```
ESTADO UID Nombre Apellidos (Matrícula)
```

La escritura en la base de datos está diseñada para tener un servidor central donde se almacenen los exámenes y su registro de autorización de forma que permita la recolección de los datos de forma simultanea desde diferentes puntos de autorización. Esta opción no es obligatoria, sin embargo es recomendada.

El sistema gestor de bases de datos elegido es MySQL[24] o cualquiera que sea compatible con este, como MariaDB[25] que es el que ha usado durante el desarrollo del sistema.

[24] `https://www.mysql.com/`
[25] `https://mariadb.org/`

El diseño de la base de datos es muy sencillo. Como puede observarse en la figura 11 consta de dos entidades, la primera de ellas, *evento*, se encarga de almacenar el nombre del evento, asignatura o examen que el profesor elija y la fecha y hora en la que se inició el proceso de autorización. La segunda, *registro*, almacena la información de cada tarjeta leída y su estado de validación.

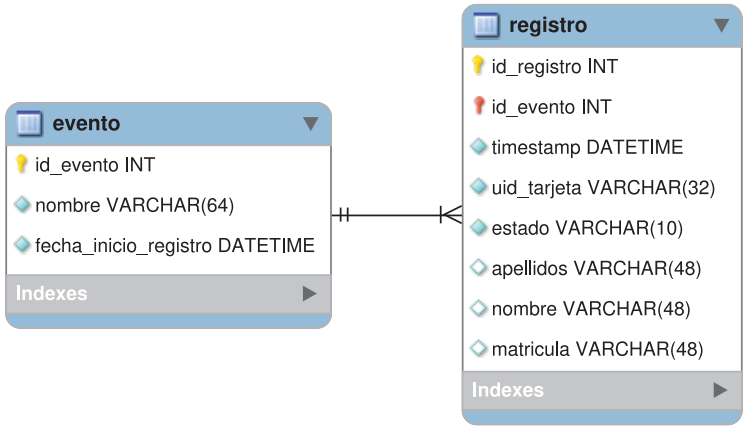

Figura 11: Diseño de la base de datos

5. RESULTADOS Y CONCLUSIONES

5.1. Pruebas del sistema

Para las pruebas del sistema se dispone de un carnet universitario del tipo MIFARE Classic 1K así como 5 tarjetas genéricas del mismo tipo. Como plataforma hardware se ha utilizado una RaspberryPi B, de 512MB de RAM y el lector/escritor NFC indicado en la sección 4.

```
sconde@sycorax ~/Universidad/4/TFG/src $ ./generar_tarjeta -c testcfg -f sergio_
conde_carnet_universitario.mfd
[*] Inicializando libnfc 1.7.1...
    [+] Dispositivo NFC abierto: NXP / PN533
[*] Pase la tarjeta objetivo por el lector...
    [+] Tarjeta detectada UID: 45 48 21 6e
    [+] Memoria detectada: 1024 bytes.
[*] Generando claves A y B para la tarjeta...
[*] Datos del alumno...
    [?] Apellidos: Conde Gómez
    [?] Nombre: Sergio
    [?] Número de matrícula: 080123
[*] Generando tarjeta...
sconde@sycorax ~/Universidad/4/TFG/src $ master* [e375b18] ~ ~ ?
```

Figura 12: Generación del carnet universitario.

El carnet universitario ha sido escrito con mis propios datos, como puede observarse en la figura 12, y 3 de las otras tarjetas se han generado usando datos de prueba. La cuarta tarjeta se ha generado usando más datos de prueba y posteriormente se ha atacado sus claves y se ha modificado el nombre y matrícula del alumno y la quinta tarjeta ha utilizado para realizar un ataque de clonado del carnet universitario.

Todas las tarjetas han sido generadas usando `generar_tarjeta` y escritas usando `escribir_tarjeta`.

En salida del registro del sistema de autorización, que puede ser observada en la figura 13, se aprecia el resultado de la verificación de cada una de las tarjetas que han sido presentadas al lector.

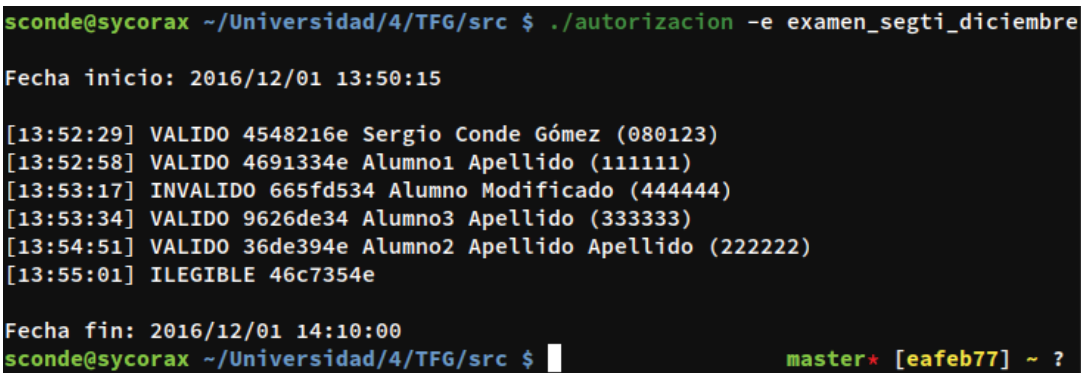

Figura 13: Salida del sistema de autorización.

El resumen de los resultados se puede encontrar en la tabla 2, donde podemos apreciar que se han identificado correctamente la tarjeta modificada y la tarjeta clonada.

Tarjeta	Lectura	Validación
Carnet universitario	Correcta	Válida
Tarjeta 1	Correcta	Válida
Tarjeta 4	Correcta	Inválida
Tarjeta 3	Correcta	Válida
Tarjeta 2	Correcta	Válida
Tarjeta 5	Ilegible	

Tabla 2: Resultados de la prueba

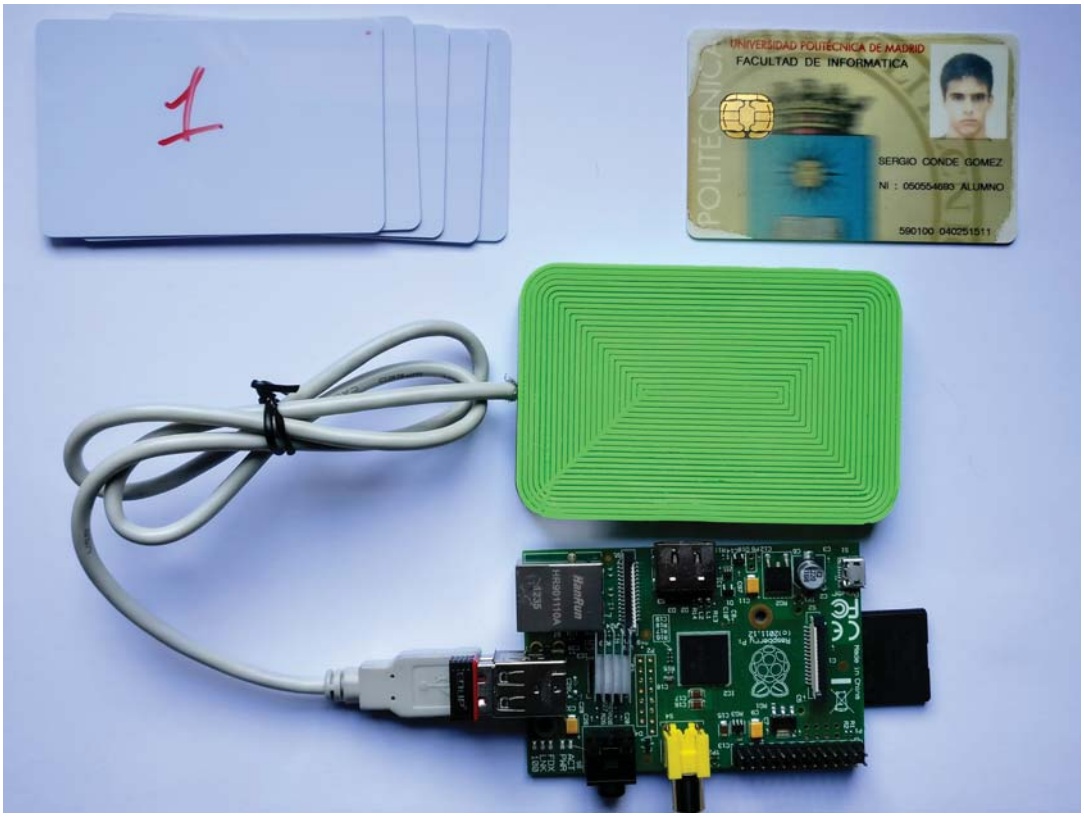

Figura 14: Hardware utilizado durante las pruebas.

5.2. Conclusiones

El sistema planteado cumple con los requisitos, sin embargo debería estudiarse su funcionamiento en un entorno real para probar su eficacia y sencillez de uso por parte del profesorado.

Se requiere el uso de un hardware en el aula aunque este podría ser una plataforma como la RaspberryPi[26] con un lector NFC mediante USB, como el utilizado durante el desarrollo de este trabajo, lo cual permitiría ser portable.

La seguridad de las tarjetas es un punto que podría ser débil en el sistema por lo que una mejora futura que con la expansión del DNIe 3.0 el sistema evolucionase al uso del mismo para la autenticación de alumnos. Aunque se plantearía el problema de los alumnos erasmus siendo necesario que estos utilicen un pasaporte electrónico o sean identificados de forma manual.

No se ha evaluado la posibilidad de uso de tarjetas MIFARE DESFire EV2 las cuales, según el fabricante, proveen una mayor seguridad y podrían solucionar los problemas existentes en versiones anteriores[18]. Si el resultado fuese satisfactorio podría implementarse el sistema usando este tipo de tarjeta incrementando la seguridad del mismo.

[26] `https://www.raspberrypi.org/`

6. REFERENCIAS

[1] N. Forum. (2015). About the technology, dirección: http://nfc-forum.org/what-is-nfc/about-the-technology/ (visitado 18-09-2016).

[2] ——, (2015). About us, dirección: http://nfc-forum.org/about-us/ (visitado 18-09-2016).

[3] ——, (2015). Tag type technical specifications, dirección: http://nfc-forum.org/our-work/specifications-and-application-documents/specifications/tag-type-technical-specifications/ (visitado 18-09-2016).

[4] I. JTC 1/SC 17, "Identification cards – contactless integrated circuit cards – proximity cards – part 1: Physical characteristics", ISO/IEC, inf. téc. ISO 14443-1, 2016.

[5] ——, "Identification cards – contactless integrated circuit cards – proximity cards – part 2: Radio frequency power and signal interface", inf. téc. ISO 14443-2, 2016.

[6] ——, "Identification cards – contactless integrated circuit cards – proximity cards – part 3: Initialization and anticollision", ISO/IEC, inf. téc. ISO 14443-3, 2016.

[7] ——, "Identification cards – contactless integrated circuit cards – proximity cards – part 4: Transmission protocol", ISO/IEC, inf. téc. ISO 14443-4, 2016.

[8] C. N. de Policía. (2016). Diferencias dnie y dnie 3.0, dirección: https://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_038 (visitado 19-12-2016).

[9] P. T. Solutions. (2000). Clearstream rfid solutions - fixed rfid apps, dirección: http://www.clearstreamrfid.com/solutions/ (visitado 15-09-2016).

[10] U. P. d. S. Oficina de Información. (2012). Samsung y la upsam se alían para probar tecnología nfc en las aulas, dirección: http://www.upsam.es/index.php?option=com_content&view=article&id=451:samsung-y-la-upsam-se-alian-para-probar-tecnologia-nfc-en-las-aulas&catid=68:upsam&Itemid=209 (visitado 15-09-2016).

[11] M. J. López Fernández, J. Guzón Fernández, S. Ríos Aguilar, B. Salazar Selvi y R. González Crespo, "Control of attendance applied in higher education through mobile nfc technologies", *Expert Systems with Applications*, vol. 40, n.º 11, págs. 4478-4489, sep. de 2013.

[12] B. Hein y C. of Mac. (2014). Apple confirms iphone 6 nfc chip is only for apple pay at launch, dirección: http://www.cultofmac.com/296093/apple-confirms-iphone-6-nfc-apple-pay/ (visitado 15-09-2016).

[13] Wikipedia. (2016). X.509, dirección: https://es.wikipedia.org/wiki/X.509 (visitado 15-09-2016).

[14] I. C. A. Organization, "Machine redable travel documents", International Civil Aviation Organization, inf. téc. 9303, 2015.

[15] N. Semiconductors, "End to end system security risk considerations for implementing mifare classic", NXP Semiconductors, inf. téc. AN 155122, 2009.

[16] T. Kasper, I. von Maurich, D. Oswald y C. Paar, *Cloning cryptographic rfid cards for 25$*, Horst Görtz Institute for IT Security, Ruhr-University Bochum, Germany, 2010.

[17] N. Tools. (2016). Devices compatibility matrix, dirección: `http://nfc-tools.org/index.php?title=Devices_compatibility_matrix` (visitado 11-10-2016).

[18] N. Semiconductors. (2016). Mifrare desfire ev2, dirección: `https://www.mifare.net/en/products/chip-card-ics/mifare-desfire/mifare-desfire-ev2/` (visitado 12-12-2016).

Este documento esta firmado por

	**Firmante**	CN=tfgm.fi.upm.es, OU=CCFI, O=Facultad de Informatica - UPM, C=ES
	Fecha/Hora	Tue Jan 10 15:32:39 CET 2017
	Emisor del Certificado	EMAILADDRESS=camanager@fi.upm.es, CN=CA Facultad de Informatica, O=Facultad de Informatica - UPM, C=ES
	Numero de Serie	630
	Metodo	urn:adobe.com:Adobe.PPKLite:adbe.pkcs7.sha1 (Adobe Signature)