ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DISEÑO E IMPLEMENTACIÓN DE UN PROTOTIPO PARA CONTROL DE ACCESO DE PERSONAS APLICANDO LA TECNOLOGÍA NFC POR MEDIO DEL USO DE TELÉFONOS CELULARES COMPATIBLES CON ESTA TECNOLOGÍA

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

DIEGO FERNANDO VELOZ CHÉRREZ
diegochoveloz@yahoo.com

DIRECTOR: ING. FABIÁN CORRAL
fvcorral@gmail.com

Quito, Junio 2010

DECLARACIÓN

Yo, Diego Fernando Veloz Chérrez, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____

Diego Fernando Veloz Chérrez

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Diego Fernando Veloz Chérrez, bajo mi supervisión.

_____

Ing. Fabián Corral C.
DIRECTOR DEL PROYECTO

AGRADECIMIENTO

Agradezco a Dios por darme la vida y así permitirme terminar mis estudios para mejorar como ser humano y desarrollarme como una persona preparada para los retos de la sociedad.

A mis padres por darme la oportunidad de estudiar una carrera y abrirme las puertas hacia un futuro prometedor que me ayude a valerme por mí mismo, a tomar mis propias decisiones y pueda realizarme profesionalmente.

A mi abuelita Lidita que con sus oraciones me alentaba para seguir adelante y no desmayar, sabiendo que con esfuerzo se puede lograr lo que se desea.

Gracias a toda mi familia por su apoyo y cariño, por su comprensión en mis momentos difíciles y porque siempre han querido mi felicidad; ustedes también forman parte de este logro.

A mis amigos a lo largo de mi carrera que a pesar de las dificultades con las que nos chocamos, pudimos arrimarnos al hombro el uno del otro y así superarlos; creo que ese fue un gran apoyo y más que en lo estudiantil, el apoyo moral fue el que me ha permitido superar esos obstáculos que enturbiaron mi carrera, gracias amigos a todos y a cada uno con los que compartí en algún momento de mi vida universitaria.

Y a mis amigos de fuera, los que no son parte de mi carrera universitaria pero son parte de mi vida, les agradezco a quienes me alentaron y me apoyaron en su momento, cuando yo los necesité, muchas gracias.

DEDICATORIA

Este trabajo dedico a Dios porque es Él quien ha permitido que sea posible y sin Él no soy nada. Por su bendición y amor.

A mi querida abuelita Lidita, mi segunda madre, a quién por todo su amor y entrega le debo todo y quien tiene derecho a formar parte de todos mis éxitos y mis logros. Al igual que ella lo hizo conmigo desde mi nacimiento, darme amor, con amor le dedico este trabajo que me permite terminar una etapa de mi vida y que me permite conquistar la culminación de mis estudios de Ingeniería.

A mi amado hijo, que a pesar de todas las dificultades, las penas y lágrimas, lo amo con todo mi ser y es por él que ahora tengo una razón para luchar y ser mejor. Le dedico este trabajo en el que a lo largo de toda su realización siempre estuvo presente en mis pensamientos y con el cual le demuestro mi esfuerzo y mis ganas de superación y que quede constancia de que mis éxitos y logros serán suyos también por darme la mayor felicidad del mundo, ser su padre, y hacerme feliz con solo verlo. Te amo mucho Dieguito Alejandro eso jamás lo dudes. Recuerda siempre que mientras tenga vida yo seré tu apoyo y si necesitas de algo, papi estará ahí para ti.

CONTENIDO

RESUMEN

El proyecto desarrollado a continuación tiene la finalidad de dar a conocer la tecnología NFC explicando en un principio sus definiciones y sus características de operación, así como sus principales funcionalidades técnicas y la situación de desarrollo y de implementación en el momento en que este proyecto se desarrolló.

Más adelante se trata de dar una visión de sus características al compararla con otras tecnologías similares a ella, para diferenciar las ventajas y desventajas de NFC respecto a estas otras tecnologías. De esta manera se podrá comprender el por qué de su creación y si realmente era necesaria.

Para dar un enfoque más amplio aún se tomó en cuenta que una implementación haría que se perciba todas las características inclusive las dificultades que ocasionarían su uso y decisión para aplicarla en proyectos presentes y futuros, además que nos permitiría comprobar si realmente las especificaciones teóricas realmente funcionan como se espera.

Es por esta razón de este proyecto que implementa un prototipo que usa la tecnología NFC por medio del manejo de teléfonos celulares compatibles y a través de una aplicación tan útil como un control de acceso orientado más hacia la domótica.

La parte de la implementación no solo se lo hizo directamente después de su diseño sino que se utilizó herramientas de simulación para que sea más eficaz la corrección de errores y tener una idea anterior a su realización del comportamiento que se esperaba.

También se muestran los resultados después de hecha la implementación dando fin al proyecto y cumpliendo con los requisitos y objetivos iniciales del proyecto. Además en las conclusiones se trata de las dificultades y de la experiencia en general de la realización y se proporcionan recomendaciones para su correcto uso y posibles mejoras que puedan hacerse posteriormente.

PRESENTACIÓN

Este documento ha sido realizado con el objetivo de dar un enfoque acerca de la tecnología NFC y mediante una aplicación real poder tener criterio acerca de las ventajas que nos ofrece su uso, además de comparar si las especificaciones teóricas se acercan a la realidad.

Dentro de este documento se muestra información de NFC así como sus protocolos y su modo de funcionamiento, la situación actual de la tecnología y una comparación entre otras tecnologías similares. Sin duda esta parte es importante ya que permite que el lector tenga información y un conocimiento básico de NFC y sus componentes.

La parte de la implementación, complementa el enfoque acerca de la tecnología NFC ya que mediante simulaciones y presentación de resultados, el lector puede hacer elección de ésta si se ajusta a sus necesidades, así como puede darse cuenta de su desenvolvimiento real.

De esta forma, a continuación presento mi proyecto esperando que satisfaga las dudas acerca de NFC y que contribuya para que se tenga un mayor conocimiento e interés de tecnologías inalámbricas futuras

CAPÍTULO 1. DESCRIPCIÓN DE LA TECNOLOGÍA NFC, SUS PRINCIPIOS BÁSICOS Y SUS CARACTERÍSTICAS DE FUNCIONAMIENTO

1.1 INTRODUCCIÓN (1)

La tecnología con su gigantesco crecimiento diario, siempre ha buscado el bienestar humano, automatizando procesos para que no haya la necesidad de un manejo manual que pueda ocasionar errores, de tal manera que brinda comodidad al simplificar la vida de las personas. Entre estos avances aparece el teléfono celular, que en un principio se creó como un dispositivo netamente de comunicación para dar movilidad[1] a las personas. Pero su crecimiento acelerado ha hecho que se convierta en una herramienta diaria e indispensable capaz de converger un sinnúmero de aplicaciones y tecnologías dentro del mismo.

La tecnología inalámbrica NFC, por sus siglas en inglés Near Field Communication, aparece como un progreso en la convergencia de aplicaciones dentro del teléfono móvil al ofrecer los servicios de las tarjetas inteligentes y las ventajas de las tecnologías inalámbricas de corto alcance mediante su uso.

Una de las características más significativas de NFC es su compatibilidad con las tecnologías inalámbricas ya existentes como Bluetooth[2] y RFID[3], lo que hace aún más interesante su uso e incrementa el interés de más y más empresas en su inversión y desarrollo, por eso se han puesto en marcha proyectos pilotos,

[1] Movilidad: Capacidad que tiene un dispositivo para iniciar o recibir servicios en diferentes sistemas y mantener la sesión mientras se viaja entre sistemas.
[2] Bluetooth: especificación industrial para Redes Inalámbricas de Área Personal (WPAN) que permite la transmisión de voz y datos entre diferentes dispositivos por medio de radiofrecuencia en la banda ISM de los 2,5 GHz.
[3] RFID: es un sistema de almacenamiento y recuperación de datos remotos que usa dispositivos denominados etiquetas, tarjetas, transpondedores o tags RFID.

principalmente en Europa, para probar su desenvolvimiento con los llamados servicios de proximidad, aquellos servicios a los que se puede tener acceso con sólo acercar el teléfono móvil a un lector o terminal que ofrezca este servicio.

A pesar de que ya existen una variedad de tecnologías de corto alcance como Bluetooth, RFID, ZigBee[4], el interés que NFC está generando tiene que ver con la potencialidad que promete para el desarrollo e implementación de novedosas e interesantes aplicaciones, como el pago a través del celular, con un nivel de seguridad mejorado y también permitiendo que la experiencia de los usuarios en servicios ya existentes sea atractiva, es decir que su interacción guste a los usuarios para que a la hora de elección se inclinen hacia esta.

Es por tal motivo que con la realización de este proyecto de titulación, intento dar a conocer el entorno que conforma la tecnología NFC, brindando, más allá de un estudio, una experiencia real al implementar un prototipo que permita sacar provecho de sus características y ventajas para la satisfacción del usuario y que así se juzgue de manera objetiva si la creación de NFC estará justificada.

1.2 DEFINICIÓN DE LA TECNOLOGÍA (2)

Near Field Communication o Comunicación de Campo Cercano, por sus siglas NFC, es una tecnología de comunicación inalámbrica de corto alcance que permite el intercambio bidireccional de datos entre dispositivos a una distancia corta aproximadamente de 10 cm.

La idea de desarrollar esta tecnología fue crear un nuevo protocolo que preste compatibilidad con las tecnologías sin contacto de corto alcance ya existentes, razón

[4] ZigBee: especificación de un conjunto de protocolos de alto nivel de comunicación inalámbrica para su utilización con radios digitales de bajo consumo, basada en el estándar IEEE 802.15.4 de redes inalámbricas de área personal WPAN. Orientado más a su uso como sensores.

por la que NFC es una extensión simple del estándar ISO/IEC 14443[5] de tarjetas de proximidad (tarjetas RFID sin contacto) que combina la interface de una tarjeta inteligente y de un lector dentro de un mismo dispositivo.

Su desarrollo empieza en el año 2002 y sus promotores fueron Philips y Sony principalmente para conseguir compatibilidad con sus tecnologías, Mifare y FeliCa respectivamente, pero no sino hasta finales del año 2003 que se la aprueba como el estándar ISO 18092[6].

Un dispositivo NFC puede comunicarse con cualquier tarjeta inteligente y lector, existentes dentro del estándar ISO/IEC 14443, tan bien como con otros dispositivos NFC, y es por lo tanto compatible con la infraestructura sin contacto ya en uso para la transportación pública y de pago, por ejemplo en el caso de Málaga en donde hay un proyecto piloto para la utilización de NFC en su transportación pública. NFC está destinado principalmente para el uso en teléfonos celulares ya que no está orientada para la transmisión masiva de datos como Wi-Fi por ejemplo.

1.3 ESPECIFICACIONES TÉCNICAS (2)

NFC fue aprobado como un estándar ISO/IEC el 08 de diciembre del 2003 y posteriormente como un estándar ECMA. Al igual que la ISO/IEC 14443 se comunica vía inducción de campo magnético, donde dos lazos de antena son localizados dentro de cada campo cercano del otro, formando efectivamente un transformador núcleo de aire.

[5] **ISO/IEC 14443:** Es un estándar que define el uso de tarjetas electrónicas de identificación en especial las tarjetas inteligentes. Se anexa el estándar en la parte de Anexos del presente proyecto.
[6] **Este estándar se detalla como anexo del presente proyecto.**

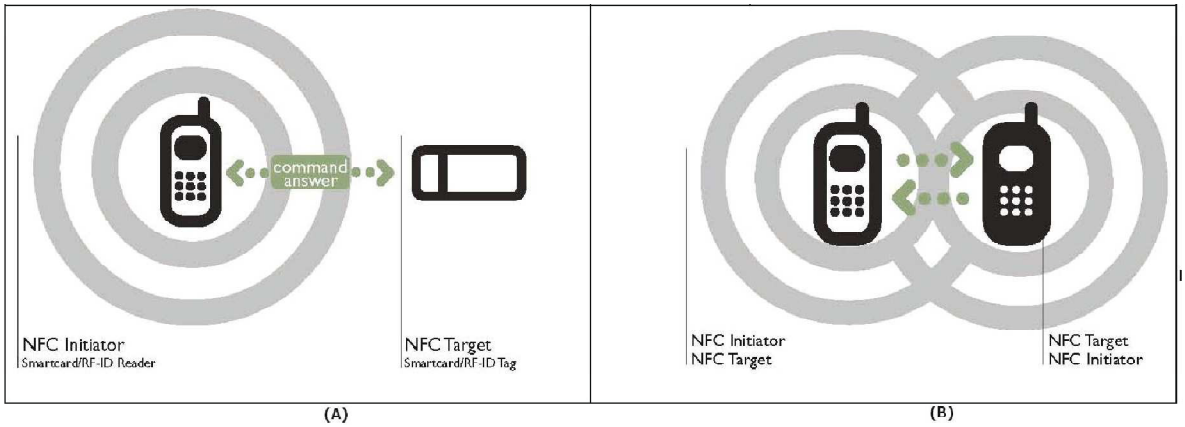


Fig 1. Inducción del campo magnético de NFC[7]

Opera dentro de la banda ISM (Industrial, Scientific and Medical) de radio frecuencia de 13,56 MHz disponible globalmente sin restricción y sin necesidad de licencia para su uso, con un ancho de banda de casi 2 MHz.

NFC es una tecnología de plataforma abierta estandarizada en la ISO/IEC 18092 y la ECMA-340. Estos estándares especifican los esquemas de modulación, codificación, velocidades de transferencia y formato de la trama de la interfaz RF de dispositivos NFC, así como los esquemas de inicialización y condiciones requeridas para el control de colisión de datos durante la inicialización para ambos modos de comunicación, activo y pasivo. También definen el protocolo de transporte, incluyendo los métodos de activación de protocolo y de intercambio de datos.

La interface de aire para NFC está estandarizado en: ISO/IEC 18092 / ECMA – 340: Near Field Communication Interface and Protocol-1 (NFCIP-1) ISO/IEC 21481 / ECMA – 352: Near Field Communication and Protocol-2 (NFCIP-2).

NFC incorpora una variedad de estándares pre-existentes incluyendo ISO/IEC 14443 de ambos tipos, tipo A (normal) y tipo B (banking/short range), y FeliCa. Por lo tanto

[7] **http://mami.uclm.es/nuevomami/publicaciones/UCAmI-chavira.pdf**

los teléfonos habilitados para NFC muestran interoperabilidad básica con módulos que ya existen como RFID.

La distancia de trabajo con antenas compactas estándar es aproximadamente 20 cm, aunque generalmente efectivo es cercano a los 10 cm. Las velocidades de transmisión que soporta esta tecnología son de 106, 212, 424 u 848 kbits/s.

La comunicación NFC es bidireccional, por lo tanto los dispositivos NFC son capaces de transmitir y recibir datos al mismo tiempo. De esta manera, ellos pueden verificar el campo de Radio Frecuencia y detectar una colisión si la señal recibida no coincide con la señal transmitida.

1.3.1 ESTÁNDARES DE COMUNICACIÓN (3)

Dentro de los estándares de NFC se ha establecido un formato común de datos para que los dispositivos NFC puedan compartir información entre sí. Estos estándares señalan las especificaciones que permiten la comunicación y son propiedad del NFC Forum, una asociación industrial sin fines de lucro encargada de regular la interacción inalámbrica y la interoperabilidad entre dispositivos NFC.

1.3.1.1 NDEF, Formato de intercambio de Datos NFC

NFC Forum ha definido un formato de datos común llamado NDEF, por sus siglas en inglés NFC Data Exchange Format, el cual puede ser usado para guardar y transportar diferentes tipos de elementos, que van desde cualquier objeto escrito MIME[8] hasta documentos RTD[9] ultra pequeños, tales como URLs[10].

[8] Por sus siglas Multipurpose Internet Mail Extensions (Extensiones de Correo de Internet de Propósitos Múltiples)

La Especificación NDEF define un formato de encapsulación de mensaje para el intercambio de datos entre dispositivos NFC o de un dispositivo NFC a una etiqueta NFC y las reglas para construcción de un mensaje NDEF válido y también de una cadena ordenada de registros NDEF. La diferencia entre una etiqueta y un dispositivo NFC es que la primera no permite una interacción con el usuario y por si sola no podría mostrar ninguna información al usuario, además es pasiva es decir que no genera su propia energía de funcionamiento y necesita de un dispositivo activo para que funcione. En cambio un dispositivo NFC permite una interacción del usuario así como es el propio generador de su energía y a través de su campo de inducción puede estimular y generar la energía para el funcionamiento de los elementos pasivos.

NDEF es un formato binario ligero que puede encapsular una o más payloads[11] de diferente tipo y tamaño dentro de la estructura de un solo mensaje. El payload está identificado por un tipo, una longitud y un identificador opcional.

- **Longitud de la carga (payload):** Indica el número de octetos de payload, es decir, indica la longitud de payload encapsulada en un registro. Se encuentra dentro de los primeros 8 octetos de un registro. El Campo PAYLOAD_LENGTH es un octeto para registros pequeños y cuatro octetos para registros normales. Los registros pequeños están indicados estableciendo el bit de la bandera SR[12] en 1.
- **Tipo de Payload:** Indica la clase de datos que está siendo transportado en el payload de ese registro. El tipo del primer registro, por convención, debería proveer el contexto de procesamiento no solo para el primer registro sino para todo el mensaje NDEF. Los tipos de identificadores podrían ser URIs[13], MIME

---

[9] Por sus siglas en inglés Record Type Definition (Definición del Tipo de Registro)
[10] Por sus siglas Uniform Resource Locator (Localizador de Recursos Uniforme)
[11] Payload: Es la carga útil, es decir la información útil para el usuario del flujo de información transferido.
[12] SR (Short Record): Esta bandera se usa cuando un registro no es grande, se detalla más adelante en el formato del Registro NDEF en este capítulo.
[13] Por sus siglas en inglés Uniform Resource Identifier (Identificador de Recurso Uniforme)

o tipos específicos NFC (NFC-specific). Al identificar el tipo de carga útil, es posible despachar la carga para la aplicación del usuario apropiada.

- **Identificador de Payload:** La payload puede dar un identificador opcional en la forma de una URI absoluta o relativa; esto permite a las cargas que soportan URI vincular tecnologías de referencia con otras cargas.

NDEF es simplemente un formato de mensaje, es decir que solo especifica la estructura del formato por lo que no se debe pensar que declara algún tipo de circuito o algún concepto de conexión o que pueda especificar el intercambio de información. El formato de datos de NDEF es el mismo tanto para un dispositivo NFC como para una etiqueta NFC, por lo que la información de NDEF es independiente del tipo de dispositivos que se estén comunicando.

Dentro del formato de un mensaje NDEF se puede enviar un variado tipo de información como:

- Puede encapsular documentos XML[14], fragmentos XML, datos encriptados, e imágenes como archivos JPEG, GIF, etc.
- Encapsular cadenas de información.
- Agregar documentos múltiples y entidades que están asociados lógicamente de alguna manera. Por ejemplo, se puede encapsular un mensaje NFC-specific y un conjunto de archivos adjuntos de tipos estandarizados que tienen referencia desde ese mensaje NFC-specific.
- Encapsulado compacto de pequeños payloads.

1.3.1.1.1 Formato del Registro NDEF

Los registros NDEF son de longitud variable pero todos tienen un formato común que se representa a continuación con la siguiente figura:

[14] siglas en inglés *Extensible Markup Language* (Lenguaje de Marcas Extensible), un metalenguaje extensible de etiquetas que permite definir la gramática de lenguajes específicos para varias necesidades.

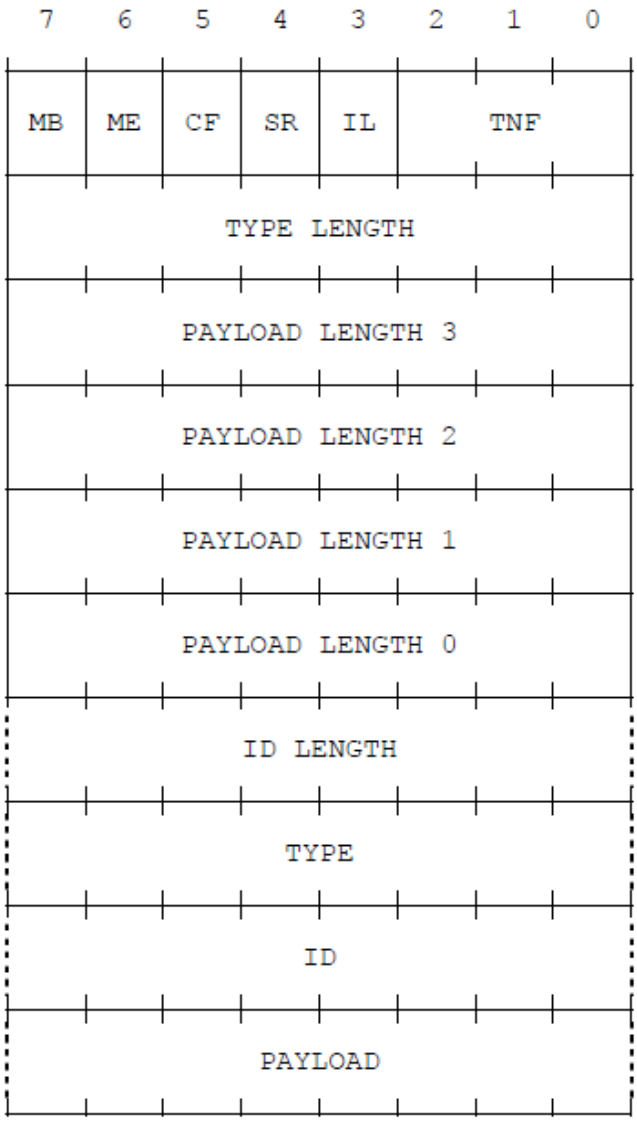


Fig. 2 Formato de un Registro NDEF[15]

La información de los registros NDEF se presenta en nivel de octetos. El orden de transmisión es de izquierda a derecha y de arriba hacia abajo; de esta manera el bit más significativo del octeto es el bit del extremo izquierdo y para una cadena de octetos es igual, el bit más significativo es el de la extrema izquierda de todo el campo de octetos y es el que se transmite primero.

[15] **www.nfc-forum.org/specs/spec_list/**

A continuación se detallan los campos que conforman el formato del registro NDEF:

- **MB (Message Begin):** Es una bandera de 1 bit que cuando se constituye indica el inicio de un mensaje NDEF.

- **ME (Message End):** Esta bandera es un campo de 1 bit que si se establece, ya que en el caso de una payload fragmentada esta bandera solo se establece en el segmento de terminación de esta payload fragmentada, indica el final de un mensaje NDEF.

- **CF (Chunk Flag):** Es una bandera de 1 bit que de establecerse indica que es el primer segmento de registro o que es un segmento de registro del medio de una payload fragmentada.

- **SR (Short Record):** Se conforma por 1 bit y al establecerse indica que el campo PAYLOAD_LENGTH es un solo octeto y no cuatro octetos como lo es para un registro NDEF normal. Este registro pequeño está destinado para una encapsulación compacta la cual permite que pequeños payloads sean parte de campos de payloads con un tamaño de entre 0 a 255 octetos. Un mismo mensaje NDEF podría tener tanto registros NDEF normales como registros cortos.

- **IL (ID_LENGTH):** La bandera IL es de 1 bit que si se establece indica que el campo ID_LENGTH está presente en la cabecera del registro como un octeto pero si el campo IL es cero entonces éste es omitido de la cabecera y el campo ID también es omitido del registro.

- **TNF (TYPE NAME FORMAT):** Es un campo de 3 bits que indica la estructura del valor del campo TYPE. Estos valores se detallan a continuación:

Type Name Format	Valor
Vacío	0x00
Tipo NFC Forum (NFC RTD)	0x01
Tipo de Medios	0x02
URI Absoluto	0x03
Tipo NFC Forum externo	0x04
Tipo Desconocido	0x05
Sin Cambio (Unchanged)	0x06
Reservado	0x07

Tabla 1. Valores de TNF

EL valor 0x00 (vacío) significa que no hay ningún tipo o payload asociada al registro. De esta manera los campos TYPE_LENGTH, ID_LENGTH y PAYLOAD_LENGTH deben ser cero y por lo tanto los campos TYPE, ID y PAYLOAD respectivamente serían omitidos del registro.

El valor 0x05 (Unknown) debería ser usado para indicar que el campo de payload es desconocido. Este valor de TNF ocasiona que el campo TYPE sea omitido del registro NDEF ya que el valor del campo TYPE_LENGTH debe ser cero. Se recomienda que cuando un analizador NDEF esté recibiendo un registro NDEF de este tipo, provea un mecanismo para guardar pero no para procesar la payload.

EL valor 0x06 (Unchanged) no debe usarse en otro registro que no sean los fragmentos de registro del medio y el fragmento del registro terminal que forman payloads segmentadas. Si se establece este valor TNF, el campo TYPE_LENGTH debe ser cero y el campo TYPE será omitido del registro NDEF.

El valor 0x07 (Reservado) es para usos futuros y no debe ser usado.

- **TYPE_LENGTH:** Este campo es un entero no asignado de 8 bits que representa la longitud en octetos del campo TYPE. Al referirse a un entero no asignado, quiere decir que no es una constante sino que su valor depende de la longitud del campo TYPE.

- **ID_LENGTH:** Este campo también es un entero no asignado de 8 bits que especifica la longitud del campo ID en octetos y está presente sólo si la bandera IL en la cabecera del registro se establece en 1.

- **PAYLOAD_LENGTH:** Es un entero no asignado que representa la logitud en octetos del campo PAYLOAD y a su vez el tamaño del campo PAYLOAD_LENGTH depende del valor de la bandera SR. Si la bandera SR está establecida, el campo PAYLOAD_LENGTH representa un solo octeto; pero si esta bandera está vacía, el campo PAYLOAD_LENGTH es de 4 octetos representando un entero no asignado de 32 bits.

- **TYPE:** Este campo es un identificador que especifica el tipo de payload de la información transmitida. El valor de este campo debe seguir la codificación, la estructura y el formato implícito por el valor del campo TNF. El tamaño máximo de este campo es 255 octetos.

- **ID:** El valor de este campo es un identificador que tiene la forma de una referencia URI (Identificador de Recursos Uniformes). Para NDEF, una URI es simplemente una cadena de texto que identifica un nombre, una localización o alguna característica de un determinado recurso. La singularidad requerida del identificador del mensaje es garantizada por el generador. Los fragmentos finales y del la mitad de una payload segmentada no debe tener el campo ID ya que se trata del mismo campo de datos pero en diferentes fragmentos por lo que solamente basta con definir una vez la información completa acerca de todo el payload. Todos los demás tipos de registros podrían tener este campo ID. El tamaño máximo de este campo es 255 octetos.

- **PAYLOAD:** Dentro de este campo se lleva la carga o información útil para las aplicaciones del usuario y la estructura interna de los datos llevados en este campo es oculta para NDEF. El tamaño máximo del campo PAYLOAD es 2^{32}-1 octetos para un diseño de registro NDEF normal y 255 octetos para un registro pequeño. Pero para tamaños de payload mayores a 2^{32}-1 se segmenta dicha payload para poder ser transmitida en fragmentos (Payloads fragmentadas).

1.3.1.1.2 Mensaje NDEF

Un mensaje NDEF está compuesto por uno o varios Registros NDEF. El primer registro de un mensaje está marcado con la bandera MB (Message Begin) y el último registro lleva la bandera ME (Message End). Si un mensaje está compuesto por un solo registro, éste mismo lleva tanto la bandera MB como la bandera ME. El número de registros que un mensaje NDEF puede llevar es ilimitado.

Los mensajes NDEF no deben superponerse, es decir, que las banderas MB y ME no deben ser utilizadas para anidar mensajes NDEF. Los mensajes NDEF pueden ser anidados llevando un mensaje completo como una payload en un registro NDEF.

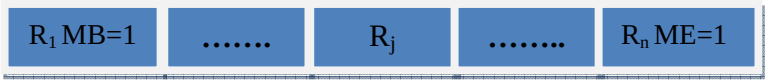


Fig.3 Mensaje NDEF con varios registros

1.3.1.1.3 Fragmentos de Registros

En realidad los mensajes NDEF no llevan números índices para indicar su orden, sino que está implícito en el orden en que los registros son serializados. Por ejemplo si los registros son empaquetados por una aplicación intermedia, ésta es la responsable de asegurar que el orden de los registros sea el mismo.

Un registro es la unidad para llevar un payload en un mensaje NDEF y cada payload es descrita por sus propios parámetros.

Un pedazo de registro (record chunk) lleva solo un pedazo de payload. Estas cargas en pedazos son utilizadas para particionar un contenido generado dinámicamente o mensajes demasiados largos en múltiples pedazos de registro ordenados en un mismo mensaje NDEF. Este agrupamiento sirve para reducir la necesidad de almacenamiento en el búfer de salida en el lado generador.

Un mensaje NDEF puede contener cero o más payloads fragmentados. Cada payload fragmentada es codificada con las siguientes reglas:

- El pedazo de registro *inicial* tiene la bandera CF (Chunk Flag). El tipo de toda la payload fragmentada debe estar indicado en el campo de tipo. El campo ID podría ser usado para llevar un identificador de toda la payload fragmentada. El campo de la longitud de payload indica solo el tamaño de los datos que lleva el registro actual y no el tamaño de toda la payload.
- El fragmento de registro *medio* tiene la bandera CF indicando que este registro contiene el próximo pedazo de datos del mismo tipo y con el mismo identificador como el fragmento de registro inicial. El valor del campo TYPE_LENGTH y del campo ID_LENGTH debe ser cero y el campo TNF (Type Name Format) debe ser 0x06.
- El pedazo de registro *final* es un registro NDEF con la bandera CF limpia indicando que este fragmento de registro es el que contiene el último fragmento de datos del mismo tipo y con el mismo identificador que el fragmento del registro *inicial.* El valor del campo TYPE_LENGTH y del campo ID_LENGTH debe ser cero y el campo TNF (Type Name Format) debe ser 0x06.

Una payload fragmentada debe ser enteramente encapsulada en un simple mensaje NDEF, o sea que no debe abarcar múltiples mensajes NDEF. Por lo tanto, ni un fragmento de registro inicial o medio puede tener una bandera ME establecida.

1.3.1.2 RTD, Definición de Tipo de Registro

La especificación RTD, por sus siglas en inglés Record Type Definition, provee las pautas para la especificación de los tipos de registros NFC bien conocidos (well-

known record types) que puedan ser incluidos en mensajes NDEF transmitidos entre dispositivos NFC o entre un dispositivo NFC y una etiqueta NFC. Es decir que esta especificación permite soportar aplicaciones específicas NFC.

En el campo de formato de los tipos de registros de un registro NDEF están contenidos los nombres del tipo de registro llamado “record type name”. Cada definición de tipo de registro es identificado por su Record Type Name. Los Record Type Name pueden ser especificados en distintos formatos llamados Type Name Format (TNF) como ya se vio anteriormente. Estos podrían ser URIs absolutos, tipos NFC bien conocidos, tipos de medios MIME, tipos externos NFC.

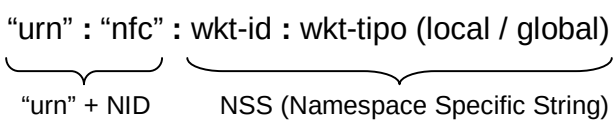
1.3.1.2.1 Tipo NFC well-known

El tipo bien conocido NFC (NFC well-known) es un formato diseñado para las etiquetas NFC y también para crear formatos primitivos, es decir un formato primitivo, es decir un formato común, por ejemplo, se puede usar este tipo cuando no hay un equivalente URI o no hay disponible un tipo MIME o también cuando las limitaciones de un mensaje requieren un nombre muy pequeño.

Cuando un mensaje NDEF lleva un tipo NFC well-known en sí, el campo TNF tiene el valor 0x01.

Estos tipos de formatos en la especificación RTD son definidos como URN[16] (Nombre de Recurso Uniforme) y tienen un identificador de nombre, “nfc”, llamado Namespace IDentifier (NID).

La estructura de un tipo de registro well-known viene de la siguiente manera:



[16] URN: por sus siglas en inglés Uniform Resource Name (Nombre de Recurso Uniforme), son identificadores de recursos en la web.

Un ejemplo de cómo sería un URN de tipo NFC well-known es “urn:nfc:wkt:a” en el cual:

- **urn** identifica a este tipo como un Nombre de Recurso Uniforme.
- **nfc** es el identificador de nombre NID.
- **wkt** es el wkt-id, un prefijo necesario antes del formato de tipo que lo identifica como un tipo well-known.

Pero cuando se codifica dentro de un mensaje NDEF, tanto el NID ”nfc” como el prefijo “wkt” son omitidos.

Dos ejemplos de tipos well.known son considerados iguales si y solo si sus representaciones binarias son equivalentes, es decir que se compara de una manera sensitiva[17] de carácter en carácter.

Existen dos clases de este tipo NFC well-known:

a. **Tipo NFC Forum Global:** Un tipo NFC Global iniciará con una letra mayúscula, por ejemplo, “A”, “Hello_world”,etc.
b. **Tipo NFC Forum Local:** La finalidad de los tipos NFC Forum Locales es para ser usados en el contexto de otro registro. Se los utiliza cuando no hay la necesidad de definir el significado del formato fuera de un contexto Local.

- **Texto RTD:** La Definición de Tipo de Registro de Texto (Texto RTD) fue diseñado con el objetivo de definir un registro NFC well-known que contenga solamente datos de texto y que sea liviano para ser usados sin que se requiera de mucho espacio. El nombre que se utiliza para representar este tipo de registro es “T”.

- **URI RTD:** La Definición de Tipo de Registro URI no permite acceder a recursos de internet o para transportar los identificadores de Recursos, URI, de un

[17] **Diferenciar entre mayúsculas y minúsculas**

dispositivo a otro. Es básicamente un contenedor compacto de URI's. El nombre de este registro para poder identificarlo es "U".

- **Smart Poster RTD:** La Definición de Tipo de Registro Smart Poster especifica la manera de incorporar datos como SMS[18], URI's o números de teléfono en etiquetas NFC o la manera de transportarlos entre dispositivos. El objetivo de los Smart Poster es proveer una manera simple para acceder a un servicio remoto por un toque. Un Smart Poster también puede contener acciones que desplieguen una aplicación en un dipositivo, por ejemplo iniciar un explorador de internet. El nombre que identifica el registro Smart Poster es "Sp". Dentro de la payload de un Smart Poster hay algunos tipos de registros y pueden haber uno o más de estos registros:

    - **Registro Título:** El Registro Título es un ejemplo de registro Texto RTD. Nos permite dar información del contenido del Smart Poster y puede ser visto por el usuario. No hay un límite para el número de estos registros en un Smart Poster, pero dos o más registros de este tipo no pueden utilizar el mismo identificador de lenguaje. Este es un registro opcional

    - **Registro URI:** Este registro es el núcleo del Smart Poster y los demás registros son datos acerca de éste. Debe haber uno y solamente un Registro URI en un Smart Poster.

    - **Registro Ícono:** Este registro permite colocar una imagen para ser mostrada al usuario. Un Smart Poster puede contener algunos registros de este tipo con sus imágenes, pero solo una de estas debería ser mostrada. Los tipos de imágenes compatibles son PNG o JPEG y también podría haber registros ícono animados o videos de tipo MPEG. Este también es un registro opcional.

[18] Son las siglas de Short Message Service o Servicio de Mensajes Cortos. Están destinados especialmente para teléfonos móviles.

- **Registro Acción:** Es un registro de tipo Local y sugiere el curso de una acción que un dispositivo pueda seguir para realizar un proceso y como ser tratado el contenido. El nombre del tipo Local es “act”. Es registro es opcional. El contenido de este registro es un byte y cada acción tiene un valor:

Valor	Acción
0	Hace la acción que está destinada (iniciar un explorador, enviar un sms)
1	Guardar información (guarda un sms en la bandeja de entrada, un número de teléfono en contactos, etc)
2	Abre la información para ser editada
3…FF	Valores reservados para el futuro

Tabla 2. Valores de las distintas acciones del Registro Acción

- **Registro Tamaño:** Indica el tamaño del objeto al cual hace referencia el registro URI, pero solo debería ser utilizado para propósitos de información y como una guía. Está formado por 4 bytes de enteros no asignados (32 bytes). El nombre que representa este registro de tipo local es “s”. Es un registro opcional.

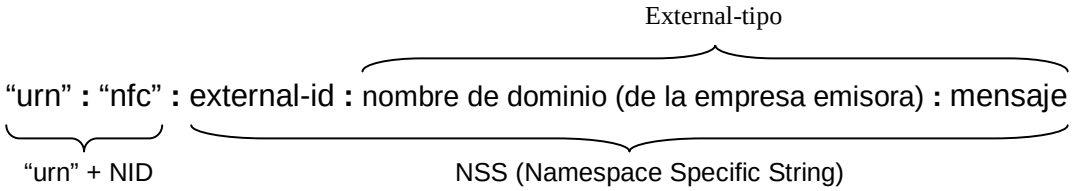
- **Registro Tipo:** Es un registro opcional y puede ser usado para que el dispositivo sepa qué clase de objeto puede esperar antes de abrir una conexión y esto podría ser útil por ejemplo cuando un Smart Poster tenga un archivo media que no sea compatible o no sea reconocido por un dispositivo lector y éste último no tenga la necesidad de reproducir al archivo si sabe de antemano su tipo. El nombre para este registro Local es “t”.

1.3.1.2.2 Tipo NFC Forum Externo

Este tipo de nombre NFC está destinado para las organizaciones que deseen establecer un espacio de nombre particular para ser usado en sus propios propósitos. Al igual que los tipos de registros well-known, el tipo NFC externo también es un URN (Nombre de Recurso Uniforme) con “nfc” como NID (Identificador de nombre) pero con la diferencia de que el prefijo utilizado no es “wkt” sino “ext”.

Para determinar si dos tipos de nombres externos son iguales se debe comparar de manera insensitiva[19] caracter por caracter.

La estructura de un tipo de registro well-known viene de la siguiente manera:



Un ejemplo de este tipo es:

“urn:nfc:ext:example.com:f”

El valor de TNF en un registro NDEF que identifica este tipo es 0x04 y al igual que los tipos well-known, la codificación binaria dentro de los mensajes NDEF debe omitir el NID y el prefijo “ext”.

1.3.1.3 Especificaciones Operativas de las etiquetas NFC

Esta especificación describe las características de los diferentes tipos de etiquetas NFC para que los dispositivos sean compatibles y puedan operar con estas en sus diferentes modos lectura o escritura. Dentro de estas especificaciones se trata de parámetros como la velocidad de operación, la radiofrecuencia, el tamaño de

[19] Comparación en la que no se diferencia entre mayúsculas y minúsculas.

memoria, etc. A continuación se presenta una tabla que resume las características de los cuatro tipos de etiquetas:

	Tipo 1	**Tipo 2**	**Tipo 3**	**Tipo 4**
Capacidad de memoria	96 Bytes hasta 2 KBytes	48 Bytes hasta 2 KBytes	Hasta 1 MB	32 KBytes
Interfaz de RF	ISO-14443 A	ISO-14443 A	FeliCa ISO 18092	ISO-14443 A y B
Velocidad	106 kbits/s	106 kbits/s	212 kbits/s	106 – 424 kbits/s
Capacidad Lectura/Escritura	Si	Si	Preconfigurados de fábrica para lectura/escritura o solo lectura	Preconfigurados de fábrica
Usos	Para una sola aplicación		Capacidad para múltiples aplicaciones	

Tabla 3. Características principales de los diferentes tipos de etiquetas

1.3.1.4 Registros de Control Genérico

Esta especificación define un tipo NFC well-know sobre como activar una instrucción específica o establecer una cierta propiedad en un dispositivo receptor NFC. Un registro de Control Genérico permite no solo un simple intercambio de datos entre dispositivos NFC sino que el dispositivo que inicia la comunicación pueda solicitar acciones específicas al dispositivo de destino (dispositivo receptor), por ejemplo un registro de tipo URI puede solicitar que el dispositivo destino abra un navegador.

Pero estas acciones o asociaciones solo ocurren en el dispositivo receptor. Si en este dispositivo existen varias funcionalidades o aplicaciones que compartan el mismo tipo de registro o acción, solo una de estas funcionalidades o aplicaciones es escogida para procesar los datos del registro y esta asociación es evidentemente realizada por el dispositivo que recibe la comunicación.

El nombre de tipo NFC well-know asignado para el registro de Control Genérico es “Gc”.

1.3.1.4.1 Estructura del Registro de Control Genérico

Dentro de la estructura del Registro de Control Genérico existe un Byte de Configuración y algunos sub registros de tipo NFC Locales, es decir que el alcance de estos sub registros está limitado localmente solo en un registro de Control Genérico. Sus funciones se detallan a continuación:

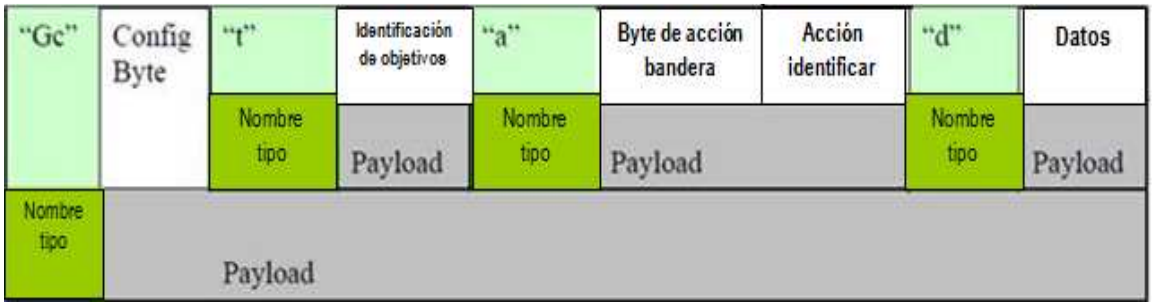


Fig 4. Estructura de un Registro de Control Genérico[20]

- **Byte de Configuración:** Este byte permite especificar opciones sobre cómo manejar el resto de la payload.

Bit	Nombre	Descripción
0	Reservado para el futuro	Debe ser 0
1	SC	Se establece 1 si la condición de salida va a ser verificada
2	EC	Se establece en 1 si los demás registros van a ser ignorados cuando este registro no es procesado satisfactoriamente
3 – 7	Reservado para el futuro	Debe ser 0

Tabla 4. Representación del Byte de Configuración

Los bits de Control de Secuencia (SC y EC) se utiliza para que el dispositivo que está leyendo tenga un criterio para terminar el proceso en la mitad de una secuencia cuando existan múltiples registros de Control Genérico

[20] **http://www.nfc-forum.org/specs/spec_list/**

dependiendo del resultado de cada uno de estos que conforman la secuencia de registros de Control Genérico.

- **Registro Target:** El nombre de tipo Local para este registro es “t”. Este registro contiene un ejemplo de un registro de texto RTD o un registro URI RTD y el dispositivo de destino será el responsable de traducir su contenido. Pero si este dispositivo no entiende el contenido de este registro debería ignorar el registro de Control Genérico.

  Un registro de Control Genérico solo debe contener un registro Target.

- **Registro Acción:** El nombre de tipo Local del registro Acción es “a”. Este registro especifica la acción solicitada por la función de objetivo para manejar los datos. Un registro de Control Genérico solo debe contener un registro Acción.

  La payload de un registro Acción contiene un Byte Bandera de Acción y un registro de datos. Este Byte Bandera debe ser el primer byte en la payload.

Bit	Nombre	Símbolo	Descripción
0	Código Numérico	NC	Se establece un 1 si un código numérico es usado para especificar la acción
1 – 7	Reservados	--	Debe ser 0

Tabla 5. Byte Bandera de Acción

Cuando la bandera NC = 0 (vacía), entonces el resto de la payload contiene un registro de texto RTD o un registro de tipo MIME.

Cuando el bit 0 se establece en 1 (NC = 1), la siguiente secuencia de bits es el código numérico de una acción y su interpretación es:

Valor	Acción
0	La función por defecto de la función Target (por ejemplo abrir una página web por un navegador web, marcar un número para un teléfono)
1	Almacenar para su uso posterior (por ejemplo guardar un número telefónico en un directorio, añadir un URL en los registros de un navegador web, etc.)
2	Abrir para editar (por ejemplo abrir un URI en un editos de URI, abrir un editor de directorio para modificar un teléfono, etc.)
3 – 255	Reservados para posteriores usos

Tabla 6. Códigos Numéricos de Acción

Este Código de Numeración es similar al Registro de Acción del Registro Smart Poster.

- **Registro de Datos:** El nombre de tipo Local de este registro es “d”. Un registro de Datos podría contener cualquier tipo de registros y los datos de estos registros deberían simplemente ser pasados a la función target.

No hay un orden específico para estos sub-registros sin embargo se recomienda que el registro Target sea especificado primero, el siguiente registro sea un Registro Acción y finalmente se especifique un Registro de Datos fara una fácil lectura y un eficiente proceso.

1.3.1.4.2 Arquitectura de manejo de registro

La figura mostrada a continuación describe el proceso de recepción y manejo de los distintos tipos de registros y así mismo clasificados según su tipo se determina la asociación entre los datos y su correspondiente aplicación o función por medio de los diferentes tipos de iniciadores o launchers de las aplicaciones.

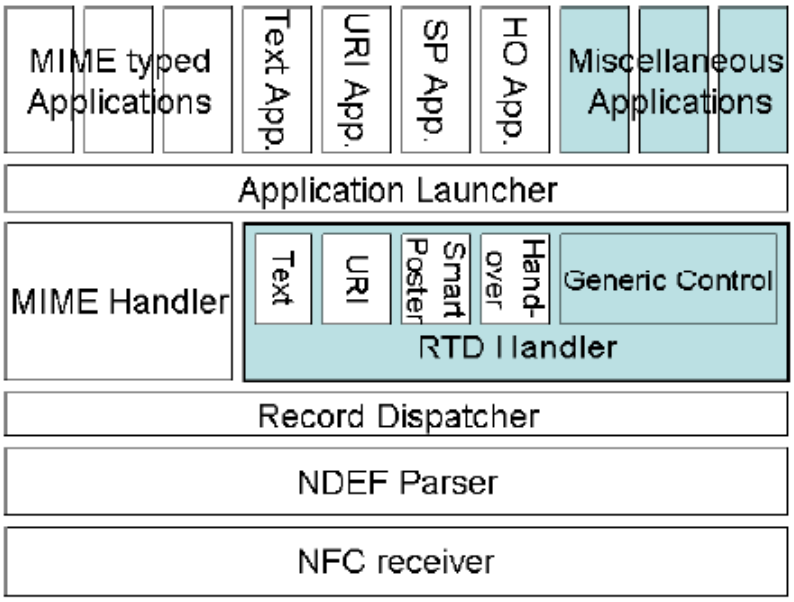


Fig 5. Manejo de registro

La figura explica el proceso para manejar un registro. En primer lugar se recibe el registro y se lo analiza, después se lo envía a un despachador de registro el cual se encargará de enviar a un manejador de acuerdo al tipo de registro. Una vez identificado que tipo de registro, el manejador de registro es el que se comunica con la aplicación que es la encargada de utilizarlo para el propósito que fue creado.

1.3.1.4.3 Seguridad, Privacidad y Autenticación

El dispositivo responsable tanto de la seguridad como de la privacidad en el momento de la ejecución de las acciones descritas en el registro de Control Genérico es el dispositivo de destino.

Por otro lado, el dispositivo emisor es el responsable de los problemas de privacidad que pudieran ser causados por transferir los datos en los registros de Control Genérico. Un registro de Control Genérico simplemente transporta los datos sin ninguna consideración específica sobre asuntos de privacidad.

En cuanto a la autenticación, un registro de Control Genérico no provee ninguna característica específica para la autenticación de un dispositivo o de una aplicación. Sin embargo si la autenticación es requerida, debería ser hecha antes o después de

transferir un registro de Control Genérico ya que la autenticación es un asunto basado en la implementación. Por ejemplo, cuando dos dispositivos se están comunicando en modo Peer-to-Peer, la información de autenticación podría ser intercambiada antes de la transferencia del registro de Control Genérico. Pero si el dispositivo destino está en modo de lectura, la información de autenticación podría estar contenida en un sub-registro del registro de Control Genérico, de esta manera el dispositivo de destino puede verificar esta información de autenticación antes de llevar a cabo cualquier tipo de acción.

Inclusive se puede usar un registro de Control Genérico para transportar la información de autenticación a otro registro de Control Genérico que requiere el estado de autenticación. Esta asociación de múltiples registros de Control Genérico debe ser manejada por los dispositivos que se están comunicando ya que estos registros no proveen ninguna característica para esta asociación.

1.3.1.4.4 Respuesta de un dispositivo de destino a un dispositivo emisor

Básicamente la Definición del tipo de registro de Control Genérico describe un registro de una sola vía de transferencia. Cuando se requiere una respuesta de un dispositivo receptor hacia su emisor es posible hacerla utilizando otro registro de Control Genérico como respuesta al intercambiar de roles entre los dispositivos emisor y receptor.

Si de ser necesaria esa comunicación mutua, las aplicaciones de los dispositivos son las responsables de mantener la consistencia del protocolo entre ambos dispositivos.

1.4 CARACTERÍSTICAS DE FUNCIONAMIENTO (1) (2) (4) (5) (6)

El funcionamiento de NFC se basa en el de las tecnologías sin contacto e Identificación por Radio frecuencia. Su alcance máximo es de aproximadamente 10 cm, por lo que la convierte en una tecnología inherentemente segura.

Dado que el fundamento de su comunicación es la identificación por radio frecuencia, evidentemente se requieren dos tipos de dispositivos para su establecimiento El dispositivo que inicia la conversación es el encargado de monitorizar la misma y este rol es intercambiable entre las dos partes implicadas.

1.4.1 INTERFACES Y PROTOCOLOS NFC

En la estandarización de la comunicación NFC esencialmente se han definido dos protocolos, NFCIP-1 (Near Field Communication Interface and Protocol-1) estandarizado en ISO/IEC 18092 / ECMA – 340 y NFCIP-2 (Near Field Communication and Protocol-2) estandarizado en ISO/IEC 21481 / ECMA – 352.

Dentro del protocolo NFCIP-1 se define el enlace de Radio Frecuencia con la que NFC trabaja que es de 13,56 MHz y los modos de operación activo y pasivo con sus rangos de velocidad desde 106 kbits/s hasta 424 kbits/s. También define las características que tienen estos modos de operación, por ejemplo la iniciación y selección del objetivo en el modo pasivo y el evitar colisiones de radio frecuencia en su modo activo.

A su vez, el protocolo NFCIP-2 especifica mecanismos de selección de los modos de comunicación para que no interfiera otras comunicaciones en curso en la frecuencia de 13,56 MHz. Los modos de comunicación que se especifican en este protocolo son:

- Modo NFC.
- Modo PCD (Proximity Coupling Devices), especificado en la ISO/IEC 14443.
- Modo VCD (Vicinity Coupling Devices), especificado en la ISO/IEC 15693.

La siguiente figura describe el proceso de selección de los diferentes modos de un dispositivo NFCIP-2:

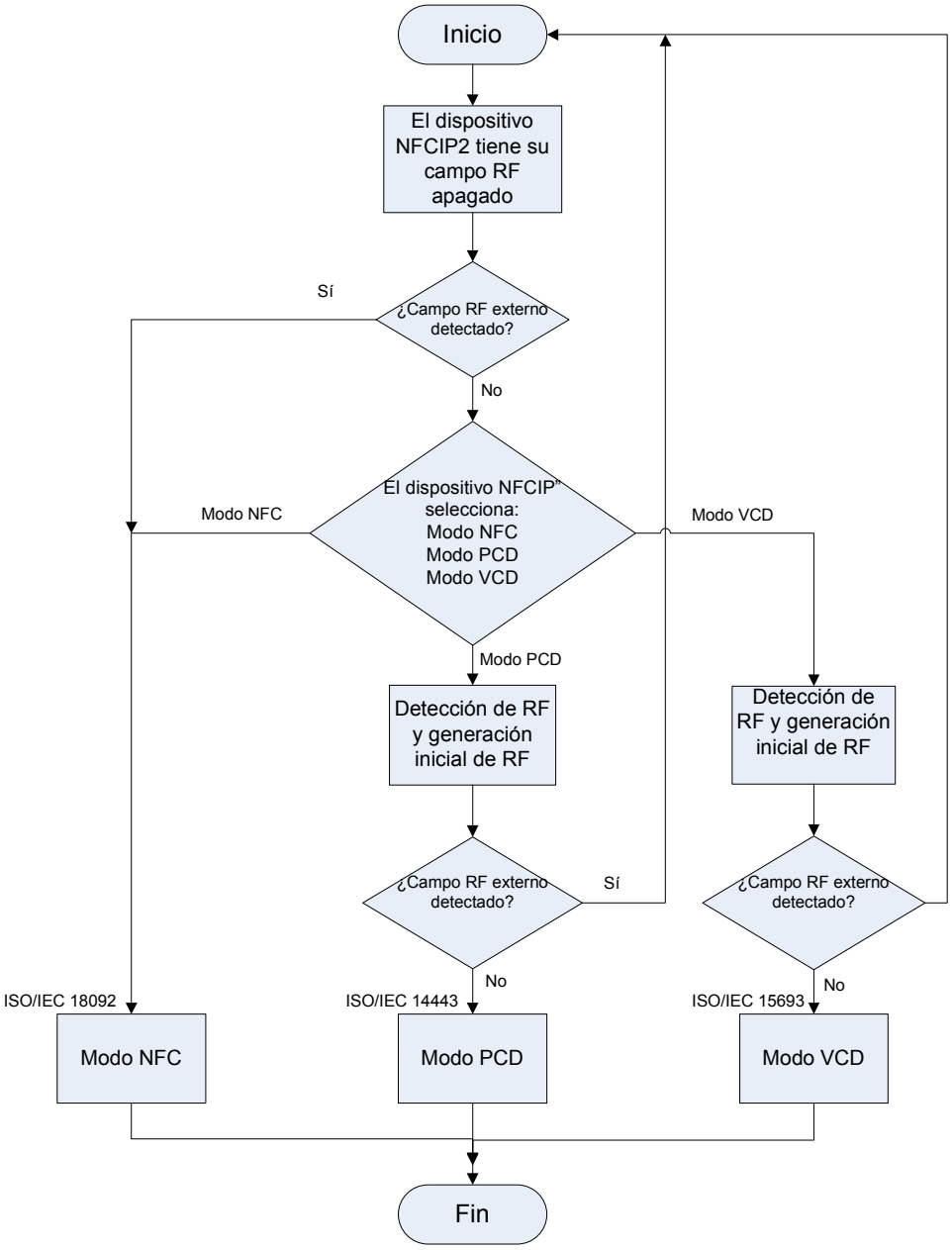


Fig 6. Detección de Radio Frecuencia y modo de selección de dispositivos NFCIP-2[21]

Cada uno de estos modos de selección trabaja en la banda de los 13,56 MHz y la diferencia de cada uno de estos es la distancia en la detección del campo de RF, los valores mínimos de sus campos para su detección y los procedimientos de inicialización que usan. Esto ayuda para prevenir posibles disturbios en las comunicaciones en curso como ya se lo mencionó.

[21] **www.ecma-international.org/publications/files/ECMA-ST/Ecma-352.pdf**

1.4.2 MODOS DE FUNCIONAMIENTO

Existen dos modos de funcionamiento: - Modo de comunicación Pasiva
- Modo de comunicación Activa

- **Modo de comunicación pasiva:** En este modo solo el dispositivo que inicia la conexión es el encargado de generar el campo electromagnético y el dispositivo de destino aprovecha de la modulación de la carga para poder transferir los datos. El dispositivo de destino podría dibujar su poder de operación desde el campo electromagnético que provee el dispositivo que inicia la comunicación, convirtiendo así al dispositivo de destino en un transponder.

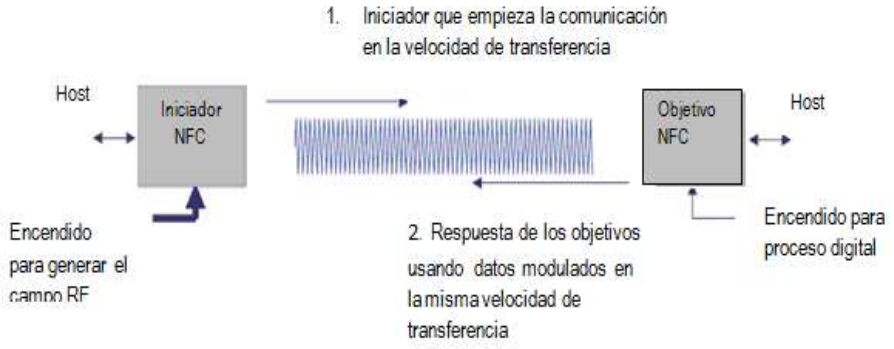


Fig 7. Modo de comunicación Pasiva[22]

- **Modo de comunicación activa:** Tanto el dispositivo iniciador de la comunicación como el de destino, se comunican alternadamente generando sus propios campos, es decir, un dispositivo desactiva su campo de RF mientras está esperando por una respuesta. En este modo, ambos dispositivos necesitan tener una fuente de energía para su funcionamiento.

[22] ***www.morelab.deusto.es/images/talks/****NFC****.ppt***

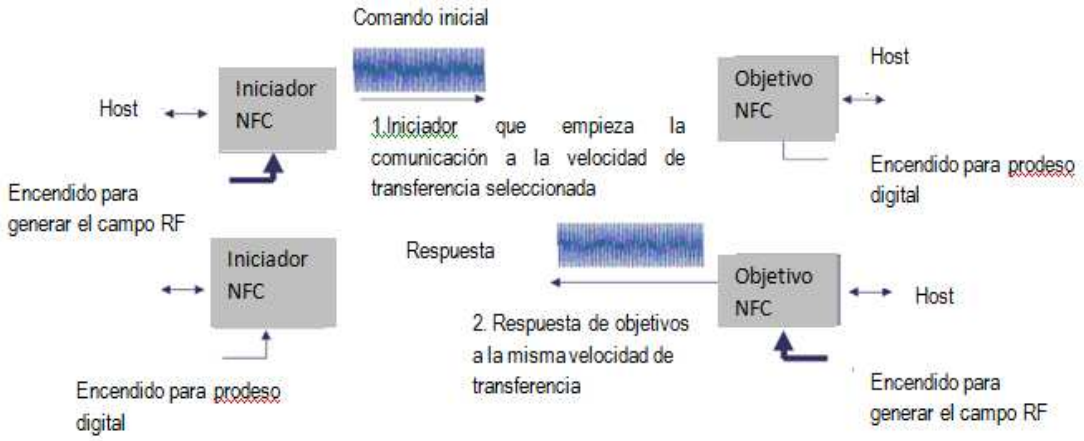


Fig 8. Modo de comunicación activa[23]

Baudios	Dispositivo Activo	Dispositivo pasivo
424 kbaud	Manchester, 10% ASK	Manchester, 10% ASK
212 kbaud	Manchester, 10% ASK	Manchester, 10% ASK
106 kbaud	Modified Miller, 100% ASK	Manchester, 10% ASK

Tabla 7. Códigos de transferencia de NFC

NFC emplea dos diferentes códigos de transferencia de datos. Por ejemplo, si un dispositivo activo transfiere datos a 106 kbit/s, se usa la codificación Miller Modificado con el 100% de modulación. En tanto que para una velocidad de transmisión de 212 y 424 kbit/s se usa el código Manchester con un índice de modulación de 10%.

[23] ***www.morelab.deusto.es/images/talks/****NFC****.ppt***

1.4.3 ESTABLECIMIENTO DE LA COMUNICACIÓN NFC

La comunicación NFC consta de cinco fases las cuales son importantes ya que tienen una función específica y siempre están presentes en el establecimiento de esta. Estas etapas son:

- Descubrimiento: En esta fase los dispositivos inician la etapa de rastrearse el uno al otro y posteriormente su reconocimiento.
- Autenticación: En esta parte los dispositivos verifican si el otro dispositivo está autorizado o si deben establecer algún tipo de cifrado para la comunicación.
- Negociación: En esta parte del establecimiento, los dispositivos definen parámetros como la velocidad de transmisión, la identificación del dispositivo, el tipo de aplicación, su tamaño, y si es el caso también definen la acción a ser solicitada.
- Transferencia: Una vez negociados los parámetros para la comunicación, se puede decir que ya está realizada exitosamente la comunicación y ya se puede realizar el intercambio de datos.
- Confirmación: El dispositivo receptor confirma el establecimiento de la comunicación y la transferencia de datos.

Cabe destacar que la tecnología NFC no está destinada para la transferencia masiva de datos, pero se puede utilizar para la configuración de otras tecnologías inalámbricas de mayor ancho de banda como Bluetooth o Wi-Fi con la ventaja de que si se utiliza NFC el tiempo de establecimiento de la comunicación es muy inferior que si se utilizaran estas otras tecnologías por sí solas para efectuar el enlace.

1.4.3 ASPECTOS DE SEGURIDAD NFC

En cuanto a los aspectos de seguridad, podemos decir que la tecnología NFC es inherentemente segura por la característica de su rango de alcance que es limitado a unos pocos centímetros, pero NFC por sí sola no asegura comunicaciones seguras.

NFC no ofrece protección contra los que se dedican a escuchar comunicaciones y es también vulnerable a modificación de datos. Las aplicaciones deben usar protocolos criptográficos de una capa superior para establecer un canal seguro.

Pero esto se contrarresta con la distancia de operación del NFC ya que al ser de tan sólo unos pocos centímetros, el espía debería estar dentro ese rango y el usuario podría darse cuenta fácilmente.

Un dispositivo pasivo, que no genera su propio campo de radio frecuencia, es mucho más difícil intervenir que un dispositivo activo.

1.5 ARQUITECTURA NFC (1) (7)

La arquitectura de la tecnología NFC es sólida y a pesar de que tiene características similares a RFID, podemos decir que NFC es una tecnología única ya que puede trabajar en tres diferentes configuraciones lo que la hace que sea más adaptable y eficiente que otras.

Fig 9. Arquitectura de la tecnología NFC[24]

[24] **www.nfc-forum.org/events/oulu_spotlight/Technical_Architecture.pdf**

En la figura se puede observar las tres diferentes configuraciones en las que esta tecnología puede trabajar:

- Modo Emulación de Tarjeta Inteligente NFC
- Modo de Comunicación Peer-to-Peer
- Modo Lectura / Escritura

La Capa de Radio Frecuencia en la que NFC trabaja está definida en los estándares ISO/IEC 18092 / ECMA – 340: NFCIP-1 e ISO/IEC 21481 / ECMA – 352: NFCIP-2; así como también es compatible con tecnologías ya existentes definidas en la ISO/IEC 14443 en ambos tipos, tipo A y tipo B, al igual que FeliCa.

- **Modo Emulación de tarjeta inteligente:** Este modo se utiliza para que el dispositivo NFC actúe como una etiqueta o una tarjeta inteligente. En este modo también se puede utilizar las características de seguridad avanzadas del elemento seguro, siendo útil para transacciones bancarias por ejemplo o para la gestión de entradas, en general para las gestiones de pagos rápidos, control de accesos, etc.

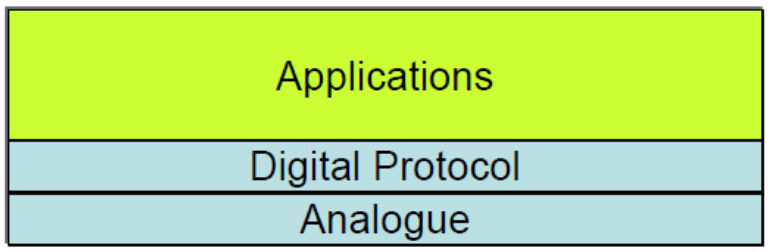


Fig 10. Modo Emulación de tarjeta inteligente[25]

- **Modo Peer-to-Peer:** Este modo sirve básicamente para el intercambio de pequeñas cantidades de datos utilizando el mismo protocolo de NFC. Pero si es necesario un intercambio de una mayor cantidad de información, la comunicación NFC se podría utilizar para establecer parámetros de una comunicación inalámbrica como Bluetooth o Wi-Fi.

[25] **http://www.nfc-forum.org/events/oulu_spotlight/Technical_Architecture.pdf**

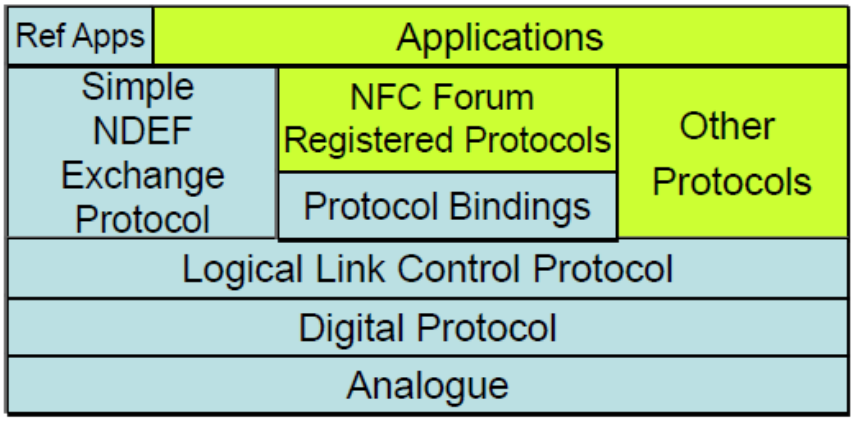


Fig 11. Modo Peer-to-Peer[26]

NFC utiliza a nivel de la capa de enlace el protocolo de control de enlace lógico (LLCP), el mismo que es usado para la activación, supervisión y desactivación de la comunicación. El modo de transferencia se lo hace de modo asincrónico balanceado, es decir que cualquier dispositivo puede iniciar la transmisión sin permiso de la otra.

El protocolo de intercambio simple NDEF se utiliza para enviar mensajes con el formato NDEF en el modo Peer-to-Peer, al igual que en las especificaciones de operación de los tipos de etiquetas NFC.

El Protocolo de conexión (Protocolo Bindings) proporciona enlaces estándar para protocolos NFC registrados y permite su uso interoperable.

Los Protocolos NFC registrados son aquellos que el Foro NFC define un enlace para el Protocolo de Control de Enlace Lógico, por ejemplo IP, OBEX[27], etc.

Las aplicaciones en modo Peer-to-Peer podrían ser por ejemplo imprimir desde una cámara, intercambiar una tarjeta de negocios, intercambiar imágenes entre dos celulares, etc.

---

[26] **http://www.nfc-forum.org/events/oulu_spotlight/Technical_Architecture.pdf**

[27] OBEX: **Es un acrónimo de OBject Exchange (Intercambio de Objetos). Es un protocolo que facilita el intercambio de objetos binarios entre dispositivos**

- **Modo Lectura / Escritura:** En este modo el dispositivo NFC puede leer los cuatro tipos de tarjetas NFC definidos en su Foro. Cuando se establece esta configuración los dispositivos NFC pueden intercambiar pequeñas cantidades de información como por ejemplo una información de texto en claro, una dirección web o un número telefónico. Este modo tiene compatibilidad de RF con la ISO/IEC 14443 y FeliCa.

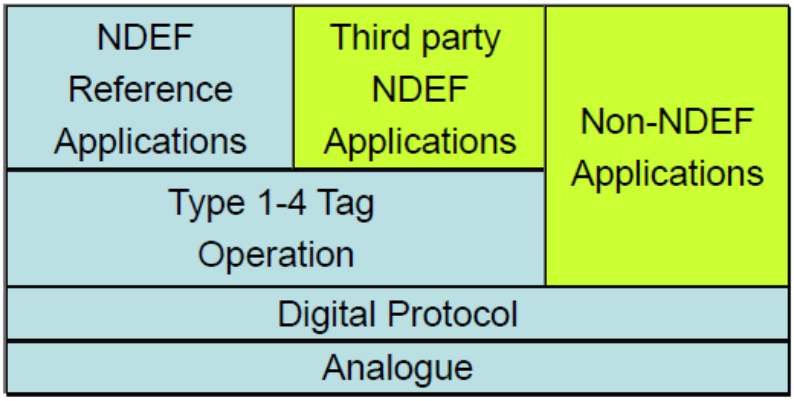


Fig 12. Modo Lectura / Escritura[28]

1.6 SITUACIÓN ACTUAL DE LA TECNOLOGÍA NFC (2) (8)

La tecnología NFC en la actualidad está destinada principalmente para ser usado con teléfonos móviles. A pesar de que aún no se ha logrado una masificación de la tecnología NFC como lo han logrado otras como Bluetooth, en cuanto a las tecnologías integradas en los móviles, NFC ha despertado un gran interés entre las empresas de comunicación, operadoras móviles y también dentro de las empresas de crédito por las oportunidades que brinda para su desarrollo y el sinnúmero de campos en los que sería de gran utilidad.

Por mencionar algunas aplicaciones que actualmente se podrían aplicar con NFC, están:

- Venta de entradas móviles en el transporte público, una extensión de la infraestructura contactless existente.

[28] **http://www.nfc-forum.org/events/oulu_spotlight/Technical_Architecture.pdf**

- Pago móvil: El dispositivo actúa como una tarjeta de pago de crédito/débito.
- Póster inteligente: El móvil es usado para leer tags de RFID en vallas al aire libre con el fin de obtener información.
- Emparejamiento de Bluetooth: En el futuro emparejamiento de dispositivos Bluetooth 2.1 con soporte NFC será tan fácil como acercarlos juntos y aceptar el emparejamiento. El proceso de activación de Bluetooth en ambos lados, buscar, esperar, emparejar y autorización será reemplazado por un simple "toque" de teléfonos móviles.

Al seguir en desarrollo NFC, su potencialidad aún no está en su máximo despliegue y podríamos mencionar por ejemplo las aplicaciones que en un futuro tendrían lugar con esta tecnología:

- Ventas de entradas electrónicas: entradas de aerolíneas, entradas de eventos/conciertos y otros.
- Dinero electrónico
- Tarjetas de viaje
- Llaves electrónicas: Llaves de carros, llaves de casa/oficina, llaves de cuartos de hotel, etc.
- Identificación de documentos
- Comercio Móvil
- NFC puede ser usado para configurar e iniciar otras conexiones de red wireless como Bluetooth, Wi-Fi o Ultra-wideband.

A más de las aplicaciones que se han mencionado se puede decir que NFC ayudará con la interacción de un sinnúmero de dispositivos electrónicos como cámaras, televisores, máquinas expendedoras, computadores, etc.

1.6.1 PROYECTOS NFC

La actualidad de NFC abre un escenario en donde se presentan proyectos atractivos tanto para los usuarios como para los inversionistas. Es así que cada vez va ganando más terreno y se presentan algunos proyectos algunos de ellos a gran

escala aunque como ya se mencionó todavía no se ha llegado a su masificación en el mercado, pero que por sus características prometen ser muy útiles y atractivos para los usuarios además de su interoperabilidad con tecnologías ya existentes. El sector del transporte es uno de los primeros beneficiados con esta tecnología.

Un programa de licencias de patentes para NFC está actualmente bajo desarrollo por Via Licensing Corporation, un subsidiario independiente de Dolby Laboratories.
Una biblioteca NFC de plataforma pública independiente está publicada bajo la Licencia pública General (GNU General Public License) libre por el nombre libnfc.
En diciembre del 2008 la aplicación eCLOWN fue publicada, la cual permite leer y copiar el contenido del chip de pasaportes biométricos.

StoLPaN (‘Store Logistics and Payment with NFC’) es un consorcio pan-Europeo apoyado por el programa de Tecnologías de la Sociedad de la Información de la Comisión Europea y está encargado de examinar el potencial aún sin explotar para fusionar el nuevo tipo de interfaz inalámbrica local, NFC y la comunicación móvil.

Motorola está realizando en Estados Unidos pruebas acerca de las seguridades en los teléfonos que incorporen esta tecnología para que sean capaces de guardar la confidencialidad de datos bancarios y que de esta manera se permita realizar transacciones financieras seguras con su uso.

En Londres se realizó un proyecto piloto en el cual participó la empresa TranSys de transportes de esa ciudad, de la mano con otras compañías como Visa Europe, Nokia, la operadora O2, el banco Barclaycard y AEG, para hacer realidad la interacción de NFC con el pago de billetes de viaje para el uso del Metro. Barcelona fue otras de las ciudades en las que se implementó un sistema parecido.

La Empresa Metropolitana de Transportes de Málaga desarrolló un proyecto en unión con la operadora Orange, Mobipay, Indra y Oberthur para el pago a bordo de los autobuses de esa ciudad a través del móvil NFC, además de que ofrece una

aplicación más al usuario para informar cuantos viajes más le resta y el número de usos que ha hecho.

Otro proyecto que ya es realidad llamado Smart Poster y tiene por objetivo el vender música a través de NFC. Esta iniciativa fue lanzada por Visa en conjunto con Universal Music y busca una mayor facilidad de venta a través de sus anuncios utilizando el modo Smart Poster.

Un proyecto lanzado en Japón por la operadora NTT DoCoMo ha puesto en marcha un servicio llamado DCMX mini, el cual le permite al público la compra de bienes a través de su teléfono móvil.

Otras localidades del mundo en donde se han realizado pruebas piloto incluyen Caen, Rhein-Main Verkehrsverbund, Atlanta, por mencionar algunas.

Lo más actual acerca de dispositivos con compatibilidad NFC para el uso de aplicaciones se lanzó a finales del 2009 por Wireless Dinamics y es más que un dispositivo, un accesorio para convertir al Iphone en un lector NFC / RFID. Este accesorio se llama iCarte y puede ser configurado como tarjeta de crédito, de débito o de prepago y tiene la capacidad de leer Posters Inteligentes (Smart Posters), es decir utilizar las características que presta NFC.

CAPÍTULO 2. TECNOLOGÍAS DE CORTO ALCANCE

Las tecnologías inalámbricas se desarrollan a un paso agigantado y tienen cada vez más aceptación en el mercado por las características que brindan frente a las tecnologías alámbricas. De estas características las que más resaltan y le dan ventaja respecto a las tecnologías cableadas son la mayor escalabilidad y flexibilidad que tienen, además que para su implementación el costo es relativamente menor. Las tecnologías alámbricas también tienen características que hacen que la balanza vaya a su favor respecto a las tecnologías inalámbricas, por ejemplo tienen mayor velocidad llegando inclusive a las decenas de Gbps, una mayor confiabilidad frente a las interferencias y definitivamente mayor seguridad respecto a intervenciones no autorizadas.

Indudablemente tanto una como otra tiene consigo ventajas y características a su favor, pero no se puede ocultar el atractivo que tiene y el interés que despiertan las tecnologías inalámbricas logrando incursionar en más sectores y permitiendo que se cristalicen ideas que ofrezcan una mayor ayuda y comodidad a los usuarios y parecería que su campo de aplicación no tuviera fin.

Las tecnologías inalámbricas de corto alcance tienen una gran aceptación en la actualidad y están tan inmersas en nuestra sociedad que casi pasan desapercibidas aunque sean tan útiles. La importancia que tienen se la han ganado por la ayuda y por la manera en que facilitan la vida cotidiana de las personas que es casi imposible imaginarnos por ejemplo un teléfono móvil sin Bluetooth con el que podamos transferir y receptar archivos inclusive a las PCs u otros dispositivos como cámaras digitales haciendo que nos olvidemos de los molestosos cables.

Así es como se presenta el escenario de las tecnologías inalámbricas de corto alcance, un ambiente que cada vez presenta más aplicaciones en las que puedan encajar, con innovaciones llamativas que las diferencian y que las hacen competir

entre ellas para ganar más popularidad pero también brindando compatibilidad con las ya existentes.

2.1 TECNOLOGÍA BLUETOOTH (11) (12) (13)

Bluetooth es una tecnología inalámbrica de corto alcance que forma parte de las llamadas WPAN (Wireless Personal Area Network) cuyo estándar es IEEE 802.15.1 y que permite el intercambio de información entre algunos dispositivos como computadores, teléfonos móviles, PDAs (Asistentes Personales Digitales), etc. A su vez permite una fácil sincronización entre ellos y hoy en día es ampliamente usado.

Fue creado como una alternativa para tecnologías cableadas como RS-232 con la intención de reducir costos y con la finalidad de que exista interoperabilidad entre dispositivos de diferentes fabricantes especialmente fue orientado desde su inicio a los teléfonos celulares.

2.1.1 ESPECIFICACIONES GENERALES

Bluetooth es un estándar que fue designado para un consumo bajo de potencia pues desde un principio la idea era permitir a sus usuarios movilidad y facilidad para comunicar sus dispositivos e intercambiar información, y esto apuntaba hacia personas que continuamente viajan por lo que debía funcionar en todo el mundo. A continuación se presentan las generalidades de esta tecnología:

- La frecuencia de operación está dentro de la banda de los 2.4 GHz.
- Una red de dispositivos Bluetooth tiene el nombre de Piconet y el número máximo de dispositivos interconectados es ocho, un dispositivo máster que inicia y controla la comunicación y los siete restantes toman el nombre de esclavos.
- Otros dispositivos a más de los ocho también pueden formar parte de la Piconet pero en estado inactivo llamado estado Parked.
- A su vez el conjunto de Piconets se le conoce con el nombre de Scatternet.
- Una unidad puede participar en distintas Piconets por medio de TDD (Duplexación por División de Tiempo).

- Posee 79 canales cada uno con un ancho de banda 1 MHz.
- Su modulación es FSK Gaussiana (GFSK).
- Existen tres clases de transmisores Bluetooth y se detallan en la siguiente tabla:

Transmisor	Potencia Máxima de transmisión (mW)	Potencia Máxima de transmisión (dBm)	Alcance
Clase 1	100 mW	20 dBm	100 m
Clase 2	2,5 mW	4 dBm	10 m
Clase 3	1 mW	0 dBm	10 cm

Tabla 8. Clases de transmisores de Bluetooth

- Se han definido dos tipos de enlaces para la transferencia de datos:
  - Enlace Sincrónico Orientado a Conexión (SCO).
  - Enlace Asincrónico no Orientado a Conexión (ACL).
- Ya que las comunicaciones inalámbricas están expuestas al ruido externo pudiendo ocasionar interferencias y perdidas de información, fue diseñado con la finalidad de que pueda operar en ambientes con ruido y para ello realiza un rápido emparejamiento y utiliza saltos de frecuencia en la transmisión para garantizar una conexión robusta.

2.1.2 VERSIONES DE BLUETOOTH

En el proceso de desarrollo de esta tecnología, se han lanzado algunas versiones y mientras más reciente sea esta, es más sólida que su anterior haciendo que Bluetooth mejore considerablemente.

2.1.2.1 Bluetooth 1.0 y 1.0B

Esta fue la primera versión lanzada y tuvo muchos problemas, uno de los tantos fue que los fabricantes de estos dispositivos tenían problemas para hacerlos interoperables. Estas versiones también traían consigo un hardware obligatorio para dirección del dispositivo o realizaban la transmisión en el proceso de conexión lo cual hizo que más bien hubiera un retraso en el funcionamiento de dispositivos en ambientes Bluetooth.

2.1.2.2 Bluetooth 1.1

Esta mejora logró remediar muchos de las fallas de la versión 1.0B y fue ratificada en el estándar IEEE 802.15.1-2002.
Dentro de esta versión se implementó soporte para canales no encriptados así como un Indicador de Fuerza de la Señal Recibida (RSSI, Received Signal Strength Indicator).

2.1.2.3 Bluetooth 1.2

La versión Bluetooth 1.2, ratificada como el estándar IEEE 802.15.1-2005, brindaba compatibilidad con su antecesora pero con una conexión y modo de descubrimiento más rápido. Otras mejoras incluían:

- Velocidades de transmisión más rápidas, sobre los 721 kbps.
- Control de Flujo y modos de retransmisión para L2CAP[29]
- Introduce una mejora en la resistencia contra ambientes ruidosos y con interferencia, a través de Salto de Frecuencia Adaptado (AHF, Adaptive Frequency – Hopping Spread Spectrum), ya que evita el uso de frecuencias congestionadas en la secuencia de salto, de esta manera Bluetooth puede coexistir con otras tecnologías como Wi-Fi en la banda de 2,4 GHz sin que puedan interferirse.
- También ofrece una mejora en la calidad de voz en enlaces de audio permitiendo la retransmisión de paquetes corruptos.
- Soporta la Interfaz de Controlador de Host (HCI). Esta interfaz permite un Controlador de Host para comunicar con el sistema operativo de una computadora personal.

[29] L2CAP: por sus siglas Logical Link Control and Adaptation Protocol (Protocolo de Control y Adaptación del Enlace Lógico). Es un protocolo que tiene por objetivo comunicar y adaptar los protocolos superiores al protocolo de banda base.

2.1.2.4 Bluetooth 2.0

Esta versión mejorada tiene compatibilidad con la v1.2 y su principal característica es la implementación de Índice de Datos Mejorados (EDR, Enhanced Data Rate) que da un incremento en la velocidad de transmisión de hasta 3 Mbps aunque en la práctica llega hasta 2,1 Mbps, y además utiliza Modulación por desplazamiento de Frecuencia Gaussiana (GFSK) para obtener el ancho de banda adicional para el incremento de la velocidad de transmisión. Otra mejora de esta versión es un menor consumo de energía pues tiene un ciclo de servicio reducido.

2.1.2.5 Bluetooth 2.1

Esta versión también tiene EDR y soporta teóricamente velocidades de transmisión superiores a 3 Mbps, además de ser completamente compatible con la versión 1.2.
Las características que esta versión trae son:

- COOPERACIÓN CON LA TECNOLOGÍA NFC. Cuando un campo NFC también está disponible, automáticamente se crea una conexión Bluetooth segura.
- Permite un Emparejamiento Simple y Seguro (SSP, Secure Simple Pairing) y con esta característica se mejora la experiencia de emparejamiento entre dispositivos Bluetooth e incrementa su uso y la seguridad.
- Respuesta de Investigación Extendida (EIR, Extended Inquery Response), esto provee más información en el proceso Inquery, proceso en el cual se envían solicitudes y respuestas entre los dispositivos para establecer la comunicación, permitiendo un mejor filtrado antes de la conexión. Esta información podría ser nombre del dispositivo, el nivel de transmisión que necesitan estas respuestas de Inquery, los servicios que soporta este dispositivo, etc.
- Se introduce también una encriptación Pause / Resume (EPR, Encryption Pause / Resume) pues antes cuando se renovaba una clave de encriptación, el dispositivo que renueva esta clave debía parar la transmisión de datos que necesitaban ser encriptados con esta clave mientras esta nueva clave era

generada, pero EPR el controlador Bluetooth asegura que los datos no encriptados se transfieran mientras la nueva clave es generada.

- El consumo de potencia es 5 veces menor.

2.1.2.6 Bluetooth 3.0

La idea de la creación de esta versión es que Bluetooth aumente considerablemente la velocidad de transferencia hasta 24 Mbps teóricamente y que trabaje con Wi-Fi para que sobre todo los smartphones tengan más velocidad de conexión.

2.1.3 SEGURIDAD DE BLUETOOTH

La seguridad para Bluetooth se lo realiza a través de procedimientos y claves de encriptación. Antes de la versión 2.1 no existía una seguridad de encriptación. Existen tres modos de seguridad en los que puede operar:

- **Modo 1 Sin seguridad:** Todos los mecanismos de seguridad están deshabilitados y el dispositivo permite que cualquier otro dispositivo Bluetooth se conecte a él.
- **Modo 2 Seguridad a nivel de Servicio:** Este modo se activa después del establecimiento del canal y es el modo más apropiado para la ejecución de algunas aplicaciones al mismo tiempo que necesiten diferentes requerimientos de seguridad.
- **Modo 3 Seguridad a nivel de Enlace:** Este modo se activa antes del establecimiento del canal y es el mayor nivel de seguridad ya que la información va cifrada desde antes de establecer la comunicación.

También se puede establecer una seguridad de emparejamiento entre los dispositivos para que puedan acceder entre sí. La autenticación se realiza mediante un número PIN[30] de 16 dígitos como máximo y para que puedan comunicarse ambos dispositivos deben ingresar el mismo número PIN.

[30] **PIN: Personal Identification Number o Número de Identificación Personal**

2.2TECNOLOGÍA RFID (14) (15)(16)(17)(18)

La tecnología RFID por sus siglas en inglés Identificación por Radio Frecuencia es una tecnología inalámbrica cuyo objetivo es enviar la identificación de personas u objetos a través de ondas de radio.

A pesar de que no se sabe cuando empezó su desarrollo, hay antecedentes que apuntan que se inició en el transcurso de la Segunda Guerra Mundial para la identificación a distancia de aviones amigos o enemigos. La implementación de Sistemas RFID recién ha empezado a desarrollarse y a conocerse debido a su reciente masificación y abarate de costos.

2.2.1 ESPECIFICACIONES GENERALES

Básicamente RFID es una tecnología para la identificación, localización, rastreo y monitoreo de personas u objetos, formando parte de las llamadas Auto ID (Auto Identification o Identificación Automática). Frente a otras tecnologías de identificación existentes como el código de barras, RFID presenta características que la hacen más eficiente y llamativa que éstas. Entre las características que presenta RFID están:

- Trabaja en diferentes bandas de frecuencias que van desde bandas de baja frecuencia (KHz) hasta bandas de alta frecuencia (GHz).
- Existen tres tipos de tags (etiquetas): activos, pasivos y semi-pasivos.
- Para los tags activos, su fuente de alimentación es propia mediante baterías de larga duración, generalmente compuestas de Litio o Dioxido de Manganeso. La duración de estas depende del modelo de tag y de la actividad que tenga, pero suele ser de varios años. Además generalmente los tags activos envían la información del estado de las baterías para que pueda haber un control de éstas.
- Tiene distintas distancias para la lectura y escritura de sus tags (etiquetas) y pueden llegar generalmente hasta los 100m.
- La memoria interna generalmente es de 4 y 32 kbytes.

- No es necesaria una línea de vista para el funcionamiento como lo necesita por ejemplo el código de barras.
- Otra ventaja respecto al código de barras es la velocidad con la que se puede usar y un mayor almacenamiento de datos por parte de RFID.

2.2.2 BANDAS DE FRECUENCIA

Las bandas de frecuencia en las cuales trabaja depende del tipo de aplicación y en la región en donde se encuentre, agrupando en cuatro rangos de frecuencia:

- **Banda de Baja Frecuencia LF (9 – 135 KHz):** Su principal ventaja es que esta banda se la puede utilizar en todo el mundo. Debido a su corto alcance de operación que es de menos de 1 metro, es útil para algunas aplicaciones como el control de acceso, identificación de animales, identificación de objetos, etc.

- **Banda de Alta Frecuencia HF (13,56 MHz):** Esta frecuencia le permite tener compatibilidad con otras tecnologías como el caso de NFC y trabaja sin restricción en todo el mundo. Se utiliza para aplicaciones como control de equipaje en aviones o acceso a edificios, etc.

- **Banda de Frecuencia Ultra-Alta UHF (433 MHz y 860 – 960 MHz):** Este rango de frecuencias tiene restricción ya que no hay una regulación mundial y su aplicación depende de cada región o país donde se utilice.

- **Banda de Frecuencia de Microondas (2,45 – 5 GHz):** Estas frecuencias no tienen ninguna restricción y pueden ser usadas a nivel global, además estas frecuencias son usadas por etiquetas activas ya que permiten distancias de lectura lejanas así como altas velocidades de transmisión. Se lo utiliza para la logística y trazabilidad de personas u objetos.

País/ Región	LF	HF	UHF	Microondas
EE.UU.	125-134 KHz	13.56 MHz 10W ERP	902-928 MHz, 1W ERP or 4W ERP	2400-2483.5 MHz, 4W ERP 5725-5850 MHz, 4W ERP
Europa	125-134 KHz	13.56 MHz	865-865.5 MHz, 0.1W ERP, LBT. 865.6-867.6 MHz, 2W ERP, LBT. 867.6-868 MHz, 0.5W ERP, LBT.	2.45 GHz
Japón	125-134 KHz	13.56 MHz	N/A.	2.45 GHz
Singapore	125-134 KHz	13.56 MHz	923-925 MHz. 2W ERP.	2.45 GHz
China	125-134 KHz	13.56 MHz	N/A.	2446-2454 MHz, 0.5W ERP

Tabla 9. Regulación de las Bandas de frecuencias en diferentes regiones[31]

2.2.3 SISTEMAS RFID

Los sistemas RFID están compuestos básicamente de un Lector, un tag o etiqueta, middleware RFID que es un subsistema de procesamiento de datos y su antena, a continuación se aprecia estos componentes de una manera un poco más detallada:

- **Lector RFID:** El lector está compuesto por una antena, una unidad de control, un transceptor y un decodificador. El comportamiento de éste se basa enviando periódicamente señales, rastreando de esta manera si existe en su alrededor etiquetas con las cuales pueda interactuar. Una vez que se realiza el enlace con una etiqueta, el lector extrae la información de ella y lo pasa hacia el middleware RFID. Éste también se encarga de la alimentación de las etiquetas (pasivas y semiactivas).

- **Middleware RFID:** Este subsistema brinda los medios para el procesamiento y almacenamiento de datos.

- **Etiqueta RFID:** Conocida también como tag o transponder, está formado por una antena, un transductor de radio, un microchip en el cual se guarda la información y en ocasiones una batería. Este elemento es el encargado de llevar la identificación del objeto de aplicación así como de transmitir dicha información. Existen diferentes modos de trabajo de las etiquetas que depende básicamente del tipo de memoria que contengan:

[31] **PUPIALES ANGAMARCA, Pablo Walter: Tesis de Grado, 2009**

- **Solo de lectura:** La información se la almacena durante el proceso de fabricación y no puede ser modificada.
- **Lectura y escritura:** Este tipo de etiqueta es la más útil y usada pero su costo es mayor respecto a la anterior. Esta memoria permite la lectura y modificación de la información contenida en esta.
- **Anticolisión:** Este tipo de etiquetas tiene una característica especial que permite que un lector pueda leer varias etiquetas de este tipo al mismo tiempo sin que ocurran errores ni colisiones durante este proceso.

- **Antena:** Ésta es un factor importante en la transmisión ya que de ella depende el alcance, la cobertura y la precisión de los datos enviados, también depende de su ubicación y del tipo de diseño que tenga.

2.2.4 SEGURIDAD

Mucho se ha especulado acerca de la seguridad que brinda esta tecnología a la hora de transmitir información. RFID, al igual que otras tecnologías inalámbricas, también tiene sus vulnerabilidades pero no por eso se va a dejar de desarrollar. A la hora de su implementación y uso hay que sopesar si las ventajas que brinda y las facilidades que presta son mayores o menores cuando se compara con sus debilidades.

Los ataques a la seguridad de estos sistemas se basa principalmente a que no tienen ningún tipo de codificación ni encriptación, lo que es fácil, dependiendo de la distancia en que se esté operando, de que se interfiera la señal y se pueda tener acceso a información que pueda ser privada. Sin embargo esto se ha tomado en cuenta y se está tratando de dar una encriptación para la información, tratando de evitar que se ésta se modifique y se capture sin la debida autorización.

En cuanto al campo de comercio y negocios otra vulnerabilidad de seguridad, más bien un fraude, sería que se cambien las etiquetas que indican la calidad y precio de los productos, por las de otros. Por ejemplo en un supermercado a la hora de elegir

un producto, el cliente elija el de mejor calidad pero cambie su etiqueta con la de otro de la misma línea pero de menor precio. Sin duda este tipo de fraude sería el mejor de los casos, ya que simplemente se podría desprender la etiqueta del producto y a la hora de la detección de las compras por los sensores para su pago, el producto lógicamente pasaría desapercibido, pues no hay necesidad de identificar uno por uno los productos para su pago mediante etiquetas anticolisión.

Otro ataque es la modificación de datos, que puede llevar a que simplemente se dé información errada de un objeto o hasta la suplantación de identificación de personas. No existe un control para esta irrupción ya que la tecnología se desarrolla de una manera imparable y rápidamente que inclusive se puede modificar la información con PDA, o computadores de bolsillo que con la ayuda de paquetes de software arremeten contra las seguridades de RFID y se puede tener una modificación o invalidez de la información retenida en una etiqueta. Pero la solución de este problema sería la encriptación que evitaría o por lo menos dificultaría mucho más un ataque como este.

Sin duda la posibilidad de ataques a RFID podrían ser muchas. Pero algunos estudios demuestran que ha sido una tecnología con un gran crecimiento en cuanto a aplicaciones y ha dado millones en ganancias, entonces si bien tiene limitaciones y no es un sistema perfecto, siempre habrá ideas y soluciones para evitar la interferencia de intrusos y sus ataques en contra de los sistemas RFID.

2.3TECNOLOGÍA ZIGBEE (13)(19)(20)(21)

La tecnología ZigBee es una alianza no lucrativa de un conjunto de 70 empresas que buscan la creación y desarrollo de un estándar inalámbrico que a más de prestar las ventajas de una tecnología inalámbrica sea de bajo consumo y de bajo costo.

Es una tecnología basada en el estándar IEEE 802.15.4 que pertenece a las redes inalámbricas de área personal (WPAN). La finalidad con la que se creó esta nueva tecnología es para aplicaciones principalmente en el campo de la domótica ya que entre otras características, las que la diferencian entre otras similares a ésta son:

- El bajo consumo de potencia
- Fácil integración en plataformas ya estructuradas
- Topología de Red en Malla

2.3.1 ESPECIFICACIONES GENERALES

ZigBee es una alianza que pretende estandarizar una nueva tecnología que aproveche las características que otras tecnologías no brindan, entre estas están:

- Sin duda ZigBee pretende que sus sistemas sean más amigables con el ambiente ya que entre sus finalidades está un consumo mínimo de energía que aporte un ahorro a los usuarios y optimice la energía de funcionamiento.
- Ya que ZigBee pretende ser una tecnología de bajo consumo de energía, la vida útil de las baterías es significativamente mayor que en otras tecnologías, lo cual provoca que el mantenimiento respecto a esta característica sea mínima y por ende menos costosa.
- ZigBee utiliza diferentes frecuencias de operación dependiendo del lugar de trabajo. Así tenemos que para Europa se usa la Banda de los 868 MHz, en cambio para norte América y Australia se asignó la banda de 915 MHz y para el resto del mundo se determinó el uso de la frecuencia de 2,4 GHz, aceptada a nivel global.
- Sin duda alguna, al momento de desarrollar e implementar circuitos y aplicaciones ZigBee, se va a preferir sobre todas la banda de 2,4 GHz ya que es una frecuencia libre que está regulada a nivel mundial.
- Los sistemas ZigBee deben estar conscientes de la energía que tienen sus sistemas, para su óptimo mantenimiento.

- Su tasa baja de transmisión hace que esta tecnología sea útil en campo como la domótica, lo que va de la mano de un consumo mínimo de energía de operación.
- La velocidad de transferencia de datos varía dependiendo de la frecuencia de operación, así para la banda de 2,4 GHz se tiene una velocidad de 250 kbps, mientras que para la banda de 915 MHz se tiene una velocidad de 40 kbps y para la frecuencia de 868 MHz, 20 kbps.
- El rango de operación de ZigBee es de 10 a 75 m teóricos.
- Otra característica que resalta sobre las ya existente es que a favor de su bajo consumo de energía y su baja transferencia de datos, su costo es relativamente mínimo.
- Soporte de nodos desde 32 hasta 255 nodos.
- La seguridad que esta tecnología ofrece es la encriptación de datos.

2.3.2 SISTEMAS ZIGBEE

En un sistema ZigBee se pueden identificar tres tipos de dispositivos, los cuales se definen por la función que desempeñan dentro de la red:

- **Coordinador de Red:** Es el más sofisticado de todos los demás dispositivos ya que requiere memoria y capacidad computacional ya que es el encargado de controlar en todo momento el sistema y también es el que guía a los dispositivos por las diferentes rutas para que puedan comunicarse. Debe existir solamente uno por Red.

- **Router ZigBee:** Este es el encargado de interconectar los dispositivos que se encuentran fuera de la topología de la red.

- **Dispositivo Final:** Este es el dispositivo destinado para el usuario. Tiene la capacidad para conectarse con un nodo en donde se encuentre un dispositivo superior a éste, ya sea un router o un coordinador ZigBee, ya que el dispositivo final no tiene la capacidad de transmitir información a otros dispositivos, por lo

que necesita la conexión con otros dispositivos superiores. Debido a esta característica esta clase de dispositivos pueden permanecer la mayor parte de tiempo en reposo hasta el momento en que deban ser usados, lo cual permite que la vida de sus baterías sea más larga en comparación con las de un coordinador que siempre debe estar activo, por lo que indudablemente un dispositivo final es mucho más económico.

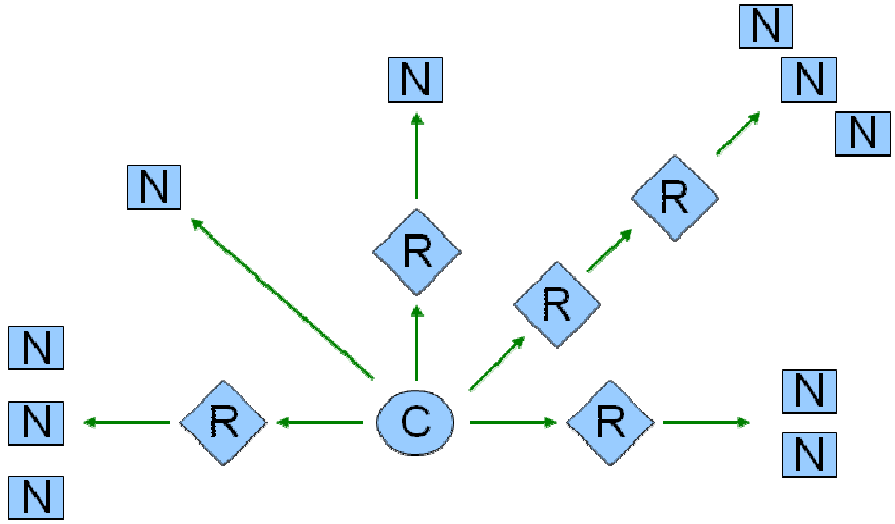


Fig. 13 Esquema de funcionalidad ZigBee[32]

Así mismo se puede hacer una clasificación de dispositivos de acuerdo a su funcionalidad:

- **Dispositivo de Funcionalidad Completa (FFD):** Son también conocidos como nodos activos. Éstos son capaces de recibir mensajes del estándar 802.15.4, tienen memoria adicional y capacidad para realizar tareas de computación por lo que pueden actuar como coordinadores o routers, o a su vez si el nodo coordinador falla, éste podría ocupar su lugar y convertirse en un nuevo coordinador.

[32] **http://www.isig.es/index.php?in=localizacion_grupos&l=productos**

- **Dispositivo de Funcionalidad Reducida (RFD):** Son conocidos como nodos pasivos. Como su nombre lo dice, tienen capacidades limitadas pero esto hace que sean más baratos y de simple funcionamiento. Estos dispositivos son los sensores dentro de una Red.

2.3.3 TOPOLOGÍAS DE RED ZIGBEE

Las diferentes topologías que ZigBee posee, le dan ventaja respecto de otras tecnologías inalámbricas. Así, la implementación de una cierta topología depende de la aplicación que se requiera. Dentro del estándar de ZigBee se definen tres tipos de topologías:

- **Topología tipo Estrella**

La comunicación que se tiene en este tipo de topología es centralizada, ya que todos los dispositivos están conectados a mismo dispositivo que se encuentra en el centro de la red y si desean comunicarse con otro dispositivo, se lo debe hacer a través de este dispositivo central. Lógicamente, el dispositivo central es el Coordinador ZigBee.

- **Topología Cluster Tree**

Básicamente esta topología tiene asociada a ella varias redes, lo cual permite que su alcance sea más amplio. Naturalmente el nodo coordinador debe estar bien identificado como Cluster Head (CH).

- **Topología tipo Malla**

Esta es la topología que ha despertado más interés para la implementación y desarrollo de la tecnología ZigBee y sin duda es la que le da ventaja frente a otras.
Dentro de esta topología todos los dispositivos FFD están conectados entre sí, mientras que los dispositivos RFD que forman parte de la red solo tienen una sola conectividad ya que no tienen capacidad de enrutamiento.

La topología en malla es la más interesante y es la que puede hacer que ZigBee pueda sobresalir pues la hace más robusta, ya que si una ruta se daña o se cae, existen más rutas alternativas por las que pueden seguir conectados los dispositivos y no haya necesidad de parar la transmisión mientras se arregla el camino que falló.

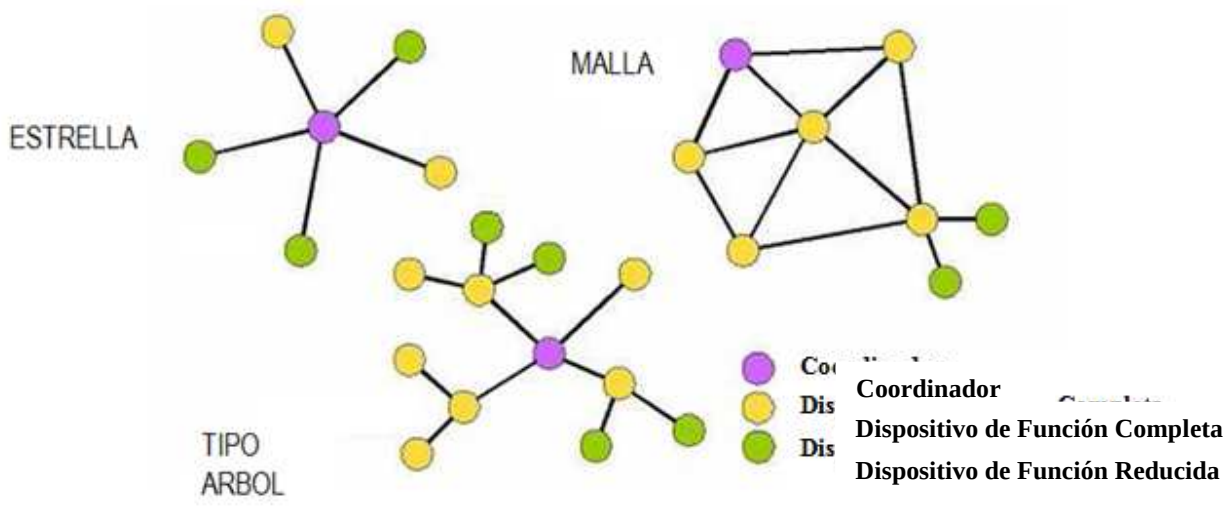


Fig. 14 Topologías de Comunicación ZigBee[33]

2.4 VENTAJAS Y DESVENTAJAS ENTRE TECNOLOGÍAS DE CORTO ALCANACE

Las diferentes tecnologías inalámbricas de corto alcance nos dan la oportunidad de ayudar no solo en cuanto se refiere a la comunicación entre personas, sino también de facilitar los procesos mediante su aplicación dentro de un sin número de escenarios.

Cada una de éstas compite con las otras brindando sus mejores características para ganarse un espacio y triunfar a la hora de elección entre los usuarios. Sus diferentes configuraciones y modos de funcionamiento así como características como velocidad, alcance, tiempo de establecimiento de la comunicación, seguridades, etc.,

[33] **http://www.seccperu.org/files/ZigBee.pdf**

hace que se ajusten a las distintas necesidades que las personas tienen. A continuación se presenta un cuadro en el que se compara las distintas características que las tecnologías de corto alcance antes tratadas nos ofrecen:

	NFC	BLUETOOTH	RFID	ZIGBEE
Establecimiento de la comunicación	Menor a 0,1 s	6 s	Menor a 0,1 s	30 ms
Velocidad de transmisión	424 kbps 848 kbps	Sobre los 2,1 Mbps La versión 3.0 soportará sobre los 24Mbps	424 kbps	250 kbps
Alcance	10 cm	10 m (depende de la versión)	Más de 3 m	70 m
Consumo de baterías	Bajo	Alto	Bajo	bajo
Costo de equipos	Mediano	Relativamente Mediano	Bajo	Bajo
Seguridad	Alta	Alta con encriptación	Vulnerable	----------
Experiencia de conexión	Simplemente con un toque	Necesita Configuración	Sin configuración	Sin configuración

Tabla 10. Comparación entre las principales tecnologías de corto alcance

En este cuadro se resumen las principales características de estas cuatro tecnologías de corto alcance. Sin embargo no puede existir un juzgamiento tomando en cuenta solo uno de estos factores sino de toda la infraestructura de cada tecnología.

Lo que se ha tratado de hacer es ver las ventajas que tiene NFC respecto a otras tecnologías ya existentes y otras igual en desarrollo para que se logre una justificación de su creación.

Por ejemplo con respecto a las velocidades de transmisión, si bien NFC no es tan rápida como Bluetooth o es similar a las tasas con las que se maneja RFID, podemos sopesar con la seguridad innata que trae al tener un rango de cobertura pequeño,

razón por la que vendría a contrapesar o si se menciona acerca de su tiempo de establecimiento para la comunicación da una ventaja sobre Bluetooth.

Lo que sí se puede asegurar es cada una de estas tecnologías fueron creadas con el propósito de cubrir las deficiencias de las otras, si bien es cierto que se puede comparar cuantitativamente algunas características, debemos principalmente tomar en cuenta las necesidades que tengamos y elegir cuál de estas encaje mejor de acuerdo con nuestras demandas.

NFC sin lugar a dudas tendrá un crecimiento rápido por las características que posee y porque no ha dejado de lado el tema de la compatibilidad que le permitirá que su implementación no sea tan brusca y que haya una mayor facilidad para que comparen los usuarios.

CAPÍTULO 3. DISEÑO E IMPLEMENTACIÓN DEL SISTEMA DE CONTROL DE ACCESO DE PERSONAS, MEDIANTE EL USO DE LA TECNOLOGÍA NFC

El Prototipo diseñado a lo largo de este capítulo tiene la finalidad de realizar un control automático en el acceso de personas dándole un uso más a un dispositivo tan necesario y difundido como el teléfono celular, sin la necesidad del manejo y control de persona alguna, sino más bien que sea un sistema que opere por sí sólo y permita el ingreso solamente a las personas autorizadas a un determinado lugar, ya sea una casa, una oficina, una habitación, es decir orientado a la domótica o a sitios más exclusivos, más personales contrario a lugares de acceso masivo como estadios, paradas de transportación pública, plazas, etc., en donde si sería necesaria la intervención de una persona que controle no solo al momento del ingreso sino que gestione también la venta o administración de las entradas y su instalación en los equipos móviles.

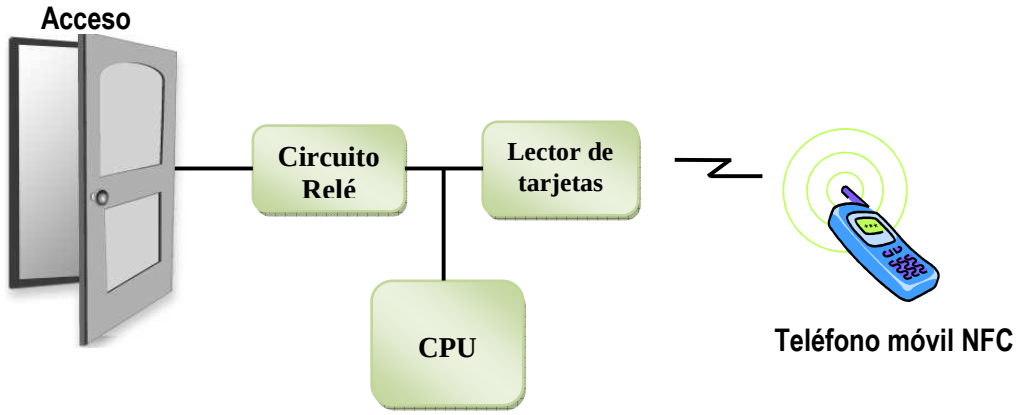


Diagrama General del Prototipo

Para el funcionamiento automático del sistema, se debe realizar un programa que una vez que se lo haga arrancar, continúe funcionando las 24 horas del día, los 7 días de la semana, ya que si hablamos por ejemplo de la instalación de este

prototipo en el ingreso de una casa, el usuario no va a estar satisfecho con limitación en los horarios de ingreso y salida de su casa, contrario a una oficina por ejemplo que se trabaja con horarios y en los que se puede y en algunos casos se debe restringir el ingreso a determinadas horas. Para que el sistema funcione en la manera que se desea, se recomienda que se tomen medidas de prevención de aspectos que salgan del alcance del desempeño mismo del prototipo, como por ejemplo suspensiones del servicio eléctrico, por lo que para este caso particular se recomienda el uso de una fuente propia para evitar que el sistema deje de funcionar.

3.1 ESPECIFICACIONES TÉCNICAS

El prototipo para el control de acceso consta de dos clases de requerimientos, la parte que corresponde al hardware se refiere a los equipos que necesitan para la implementación física del sistema y los requerimientos de software son la parte lógica del sistema, es decir, la parte que corresponde al sistema operativo en el cual corre la aplicación para que funcione el sistema.

3.1.1 REQUERIMIENTOS DE HARDWARE

El Sistema de control de acceso se conforma de un lector RFID/NFC el cual es el encargado de receptar la comunicación de equipo emisor NFC, y este último permitirá al usuario interactuar y dando la oportunidad para que pueda comunicarse con el sistema.

El equipo emisor NFC será un teléfono móvil que sea compatible con la misma, cuya función será la de permitir el ingreso a los usuarios autorizados, mediante la validación de una contraseña, la cual será validada dentro del mismo equipo y posteriormente a su validación exitosa procederá a la comunicación con el lector el cual enviará la información al programa de aplicación.

Sin lugar a dudas, dentro de los requisitos de hardware se necesitaría también una etapa de potencia la cual será la encargada, una vez enviada una señal después de una validación exitosa de usuario, controlar el voltaje que permitirá la activación del acceso para permitir el ingreso y en el caso contrario de no recibir estimulación alguna, por causa de que no se completó una comunicación exitosa puesto que se trató de un usuario restringido o no válido, el acceso seguirá bloqueado (cerrado).

Para un mejor entendimiento del sistema y la descripción de las herramientas necesarias para su ideal desempeño, se explicará cada uno de los dispositivos que se utilizan en la implementación, características de los equipos y su funcionamiento.

3.1.1.1 Lector OMNIKEY 5321 USB

Este es un lector dual ya que maneja tanto interfaces sin contacto, para aplicaciones de proximidad, e interfaces de contacto. La frecuencia de trabajo es de 13,56 MHz y es un dispositivo óptimo para aplicaciones enlazadas a la computadora.

Soporta 3 estándares para la comunicación sin contacto como la ISO 14443 A y B y 15693.

La interfaz estándar de aplicación es PC/SC, la cual permite interactuar con aplicaciones sobre sistemas operativos como Windows o Linux dentro de una computadora.

Es por esta razón que dentro de nuestro sistema también se va a necesitar de un CPU el cual permitirá la instalación de los controladores que manejan el funcionamiento del lector.

Para más detalle del funcionamiento de este lector se adjuntará la hoja de datos como un anexo a este proyecto.

3.1.1.2 Teléfono móvil NFC

Dado que este sistema está orientado a la aplicación de la tecnología NFC mediante el uso de teléfonos celulares que sean compatibles, el dispositivo transmisor de la comunicación del prototipo es un teléfono celular de la marca Nokia serie 6212 Classic, el cual viene incorporado el módulo y la antena NFC internamente.

Al momento del desarrollo de este proyecto aún se encuentra esta tecnología en desarrollo y en negociaciones para su masificación, por lo que adquirir este tipo de equipos dentro del país es imposible, ya que ni siquiera se tiene un conocimiento de la misma, y en países de Europa se están implementando algunos proyectos prueba que darán inicio a la introducción de esta tecnología en el mercado. Países de Asia, como el Japón, son los que tienen un adelanto en el manejo y uso de esta tecnología.

En el mercado existen algunas marcas de teléfonos móviles en los cuales viene incorporada la tecnología NFC como por ejemplo Motorola con su serie L7 (SLVR), Nokia con las series 6131, 6212 Classic y 6216 Classic, Samsung con el S5230, la serie SGH-X700 NFC y el D500E, BenQ con su serie T80, LG con su modelo 600V contacless, Sagem Cosyphone, además de accesorios para incorporar en teléfonos

que ya fueron lanzados al mercado y que tuvieron una gran aceptación como la carcasa NFC Shell para el modelo 3220 de Nokia.

Para la elección del modelo de teléfono NFC con el cual trabajar y realizar la implementación del sistema se tomó en cuenta algunos aspectos como facilidad de adquisición, aplicaciones reales en las que hayan sido probados los dispositivos, nivel de desarrollo y compatibilidad con otros equipos, etc.

Finalmente escogí el teléfono móvil 6212 Classic de Nokia y su adquisición posterior ya que Nokia es uno de los promotores y principales actores dentro del escenario de desarrollo de esta tecnología, formando parte del foro NFC como patrocinador en su progreso, foro el cual fue abierto sin fines de lucro para el desarrollo de esta tecnología y además dentro de su foro mismo, www.forum.nokia.com, ha dado un espacio amplio para el contacto con personas de distintos campos como la programación y expertos dentro de la Corporación de Nokia para que siga su perfeccionamiento. Además de su la información que provee y la implementación de NFC en algunas series ya de sus terminales móviles, Nokia ha creado herramientas que permiten el manejo y el desarrollo de aplicaciones para cada uno de sus terminales móviles como el Kit de desarrollo de Software para el Nokia 6131, el SDK 6131 NFC o la plataforma Series 40 Platform SDK para el equipo que escogí. En la sección 3.1.2 de requerimientos de software dentro del presente capítulo se describirá mejor esta herramienta de software.

3.1.1.3 Sistema de Control de Recepción

El Sistema de Control de la Recepción es el que recibe la información que la computadora envía al exterior por medio de uno de los puertos seriales y su función será verificar constantemente el envío de una determinada trama que será la que indique si se ha realizado correctamente la autenticación del usuario y si ésta ha ocurrido. Será el encargado de generar el impulso de voltaje para activar el acceso y permitir el ingreso.

Está conformado por un MAX232, el cual es el encargado de convertir la señal recibida de la computadora con niveles RS-232 a una señal TTL que pueda recibir un microcontrolador.

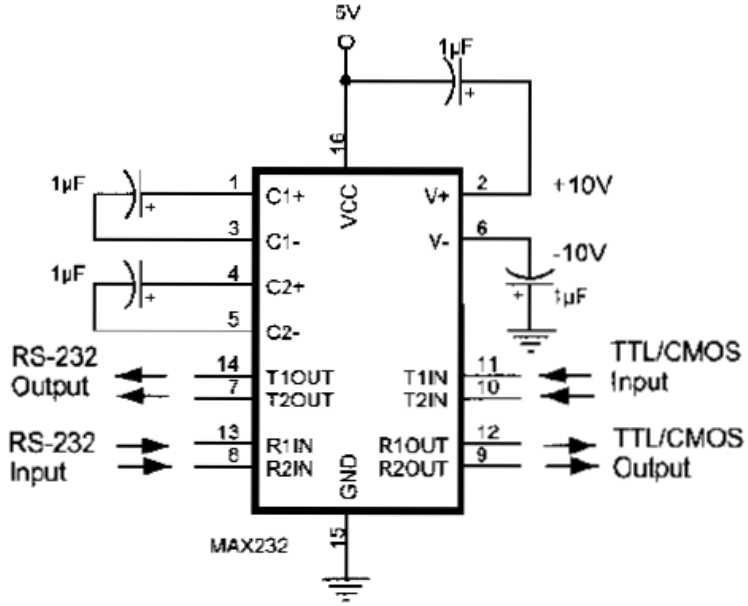


Fig. 15 Conexión de Max232

Una vez adecuada la señal a niveles TTL se conecta la salida del MAX232 (salida de señal TTL, Pin 12) a un PIC el cual está encargado de verificar el byte que indique una autenticación correcta de un usuario y cuando lo lea inmediatamente genere un impulso de voltaje por uno de sus pines, que permitirá activar la apertura del acceso. El PIC utilizado en el prototipo es el PIC 16F877A, un Pic de 40 pines cuyas características se detallan en su datasheet en los anexos de este proyecto. La entrada de la señal que va a ser leída por el PIC es por el pin 26, y si es la señal que indica una correcta validación de un usuario se enviará una señal de uno lógico al bit 0 del puerto B que corresponde al pin 33; éste a su vez activará el circuito de potencia para que se abra el acceso y el pin 34 encenderá un led verde indicando un proceso exitoso. Mientras no ocurra nada por medio del pin 35 se mantendrá encendido un led rojo que indicará que el acceso está cerrado.

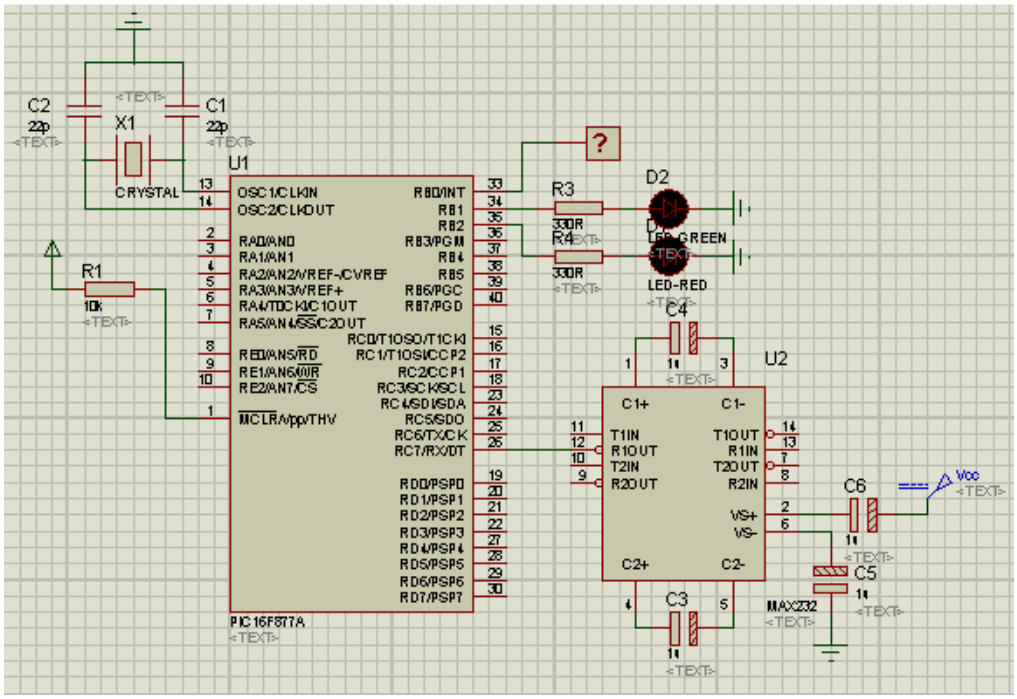


Fig. 16 Sistema de Control de Recepción

3.1.1.4 Etapa de Control de Potencia

Esta parte del sistema tiene por objetivo el control de potencia para lograr accionar la cerradura del acceso si ha ocurrido una validación exitosa. Esta etapa consta básicamente de un relé que se active con 5 VDC que son producidos por la salida del PIC (Pin 33). A continuación se muestra el diagrama de la conexión de esta etapa

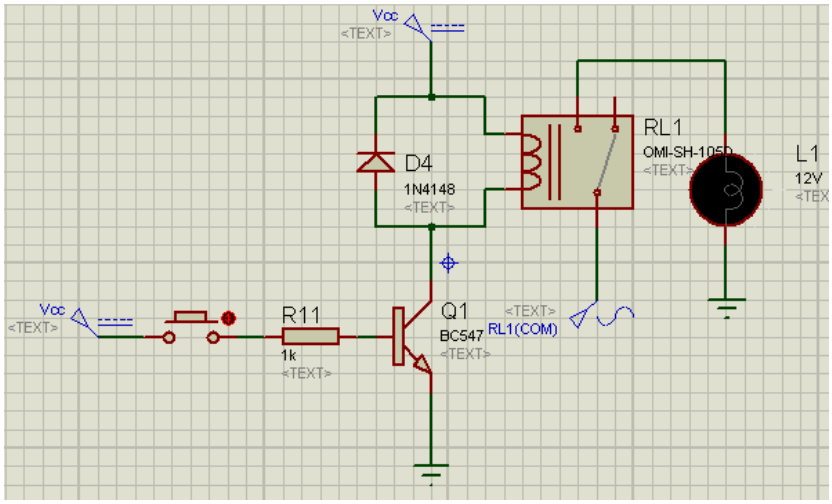


Fig. 17 Conexión Relé

3.1.2. REQUERIMIENTOS DE SOFTWARE

La aplicación de Software se orienta más hacia una aplicación que sea autónoma y no necesite la operación y el control del funcionamiento del sistema de alguna persona salvo el caso de un mantenimiento periódico o casos fortuitos que salgan fuera de los límites de una correcta operación del sistema, puesto que el acceso para el que se trata de diseñar es exclusivo, de tipo personal, como el acceso a una casa, un departamento e inclusive una oficina, a diferencia de sitios de acceso masivo como estadios o teatros de similar concurrencia que podrían necesitar de personal para el manejo y administración del sistema. Tomando en cuenta esta consideración, el sistema debe:

- Estar en funcionamiento en todo momento.
- Debe verificar a los usuarios que intenten el ingreso y validar correctamente solo a usuarios permitidos.
- La validación se lo realizará a través del ingreso de una contraseña.
- Mediante el teléfono celular, una vez realizada la correcta autenticación de usuario, se realizará la comunicación con el lector conectado a la computadora, transmitiendo determinadas tramas que permitirán posteriormente el ingreso.
- Al momento de la recepción, se procederá a la lectura de las tramas y al ser las correctas se transmitirá una señal hacia el exterior de la computadora a través de uno de los puertos seriales.
- A continuación la señal viajará a través de las etapas de control y potencia hasta llegar al acceso, permitiendo su apertura.

Además del uso del teléfono móvil, se ha tomado en cuenta también el poder realizar la autenticación de un usuario a través del uso de etiquetas NFC/RFID, pero programándolas a través del uso del teléfono móvil, es decir, el proceso será el siguiente:

Se realizará una aplicación gráfica en el teléfono móvil la cual pedirá de la misma manera el ingreso de una contraseña que validará al usuario. Esto hará que ninguna persona que no esté autorizada o no sea dueña del equipo pueda manipular las etiquetas a través del mismo.

Una vez ingresada la contraseña correcta se deberá acercar la etiqueta para que el teléfono pueda enviarle un código el cual la habilitará para el ingreso solamente una vez. Después de su uso el lector será el que borre y modifique este código, deshabilitándola para el futuro y necesariamente se deberá repetir el proceso con el móvil para que esté apta una vez más y permita el ingreso.

Para lo expuesto anteriormente se necesitará diseñar una aplicación tanto en el celular como en la PC, para permitir el envío y recepción, además se necesitará la programación del PIC que manejará la señal de salida de la computadora y éste a su vez controlará la activación de la etapa de potencia.

3.2 PLATAFORMAS DE SOFTWARE E INTERFACES

3.2.1 APLICACIÓN J2ME PARA EL MÓVIL

La aplicación necesaria para la comunicación del móvil con el módulo lector será hecha en lenguaje Java 2 Micro Edition, que es una plataforma en Lenguaje Java la cual permite el desarrollo de aplicaciones para teléfonos móviles puesto que sus características las hacen óptimas para que corran en dispositivos con baja capacidad de procesamiento y de memoria.

Esta plataforma es escogida puesto que el móvil soporta aplicaciones JAVA y también porque la comunicación entre la aplicación que corre dentro del móvil y el módulo NFC integrado en él, se lo realiza mediante la especificación JSR – 257 que es una interfaz creada por Java para Comunicaciones sin contacto.

El ambiente de desarrollo utilizado para la programación en el móvil es Netbeans 6.0 pues a más de brindarnos las características necesarias para la implementación de la aplicación Midlet en el celular, también nos permitirá simular la comunicación NFC mediante su configuración para integrar la Plataforma Series 40 SDK creada por Nokia.

3.2.2. INTERFAZ DE PROGRAMACION DE APLICACIONES PARA COMUNICACIONES SIN CONTACTO (17) (22) (23)

El API para Comunicaciones Contacless está basado en la especificación JSR-257 de Java, cuyo desarrollo ha sido dirigido por Nokia con el objetivo de implementar su uso dentro de sus equipos.

3.2.2.1 Descripción y manejo de la API para Comunicaciones sin Contacto

Esta interfaz permite el descubrimiento e intercambio de datos entre etiquetas NFC, etiquetas RFID y Smart Cards mediante el uso de paquetes o librerías que están definidas de acuerdo a la función que se desea realizar.

Paquetes de Java	Interfaces	Clases
javax.microedition.contacless	tagConnection TargetListener TargetProperties TransactionListener	DiscoveryManager TargetType
javax.microedition.contacless.ndef	NDEFRecordListener NDEFTagConnection	NDEFMessage NDEFRecord NDEFRecordType
javax.microedition.contacless.rf	PlainTagConnection	
javax.microedition.contacless.sc	ISO 14443Connection	
javax.microedition.contacless.visual	ImageProperties VisualTagConnection	SymbolgyManager

Tabla 11. Paquetes de Java para manejo de API para Comunicaciones sin Contacto

Este conjunto de paquetes permite manejar, controlar y comunicarse mediante una interfaz entre la aplicación y el módulo NFC, permitiendo así la salida de la comunicación o receptando comunicaciones sin Contacto desde dispositivos

externos. Para dar lugar a la comunicación, la interfaz sigue un determinado flujo, en orden, para el establecimiento de la misma, el cual se detalla a continuación:

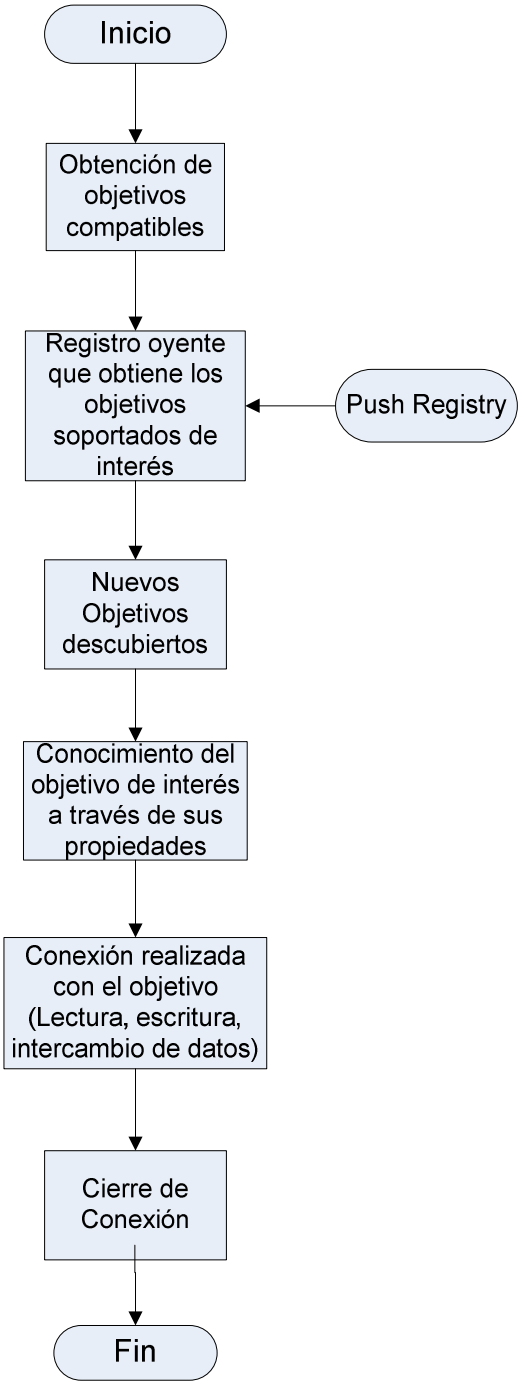


Fig. 18 Procedimiento de interacción de la interfaz de programación para Comunicaciones sin contacto

Cada uno de estos paquetes permite realizar una función específica para la Comunicación sin contacto y se los hace trabajar a través del uso de sus clases.

- **javax.microedition.contactless:** Este paquete es mandatorio, es decir para realizar cualquier tipo de comunicación sin contacto, este paquete debe estar presente y básicamente permite el descubrimiento de los objetivos a usar. Las interfaces que este paquete provee son:
    - **tagConnection** define una interfaz básica para todas las conexiones, RFID, NFC, Smart Cards.
    - **TargetListener** es una interfaz que escucha el medio en busca de objetivos que soporta la plataforma y devuelve un arreglo, la clase *TargetTypes* que muestra los tipos de los objetivos encontrados.
    - **TargetProperties**, una vez que se ha asignado un registro de escucha (listener) al objetivo de interés, se invoca al método *TargetListener.targetDetected(TargetProperties[])* el cual recibe de la interfaz TargetProperties, las propiedades del objetivo.
    - **TransactionListener** es una interfaz que permite el intercambio de APDUs entre la aplicación Midlet y el elemento seguro del dispositivo. Esta interfaz es útil cuando a nuestro dispositivo lo hacemos emular como una tarjeta, modo en el cual es posible realizar transacciones entre dispositivos NFC.
- **javax.microedition.contactless.ndef:** Da soporte para el intercambio de datos con formato NDEF[34] con etiquetas.
- **javax.microedition.contactless.rf:** Este paquete permite la interacción con dispositivos de radio frecuencia físicos (RFID, sin formato NDEF).
- **javax.microedition.contactless.sc:** Paquete que ayuda en la comunicación con Smart Cards externas.
- **javax.microedition.contactless.visual:** Este es un paquete especial ya que permite leer la información almacenada en etiquetas visuales (códigos de barra) y de generar dichas etiquetas.

[34] Son las siglas de NFC Data Exchange Format, que es el formato común para la comunicación NFC.

3.2.2.2 Proceso de Comunicación de la API para manejo de dispositivos sin contacto

El esquema de trabajo de esta interfaz corriendo en el interior del móvil es:

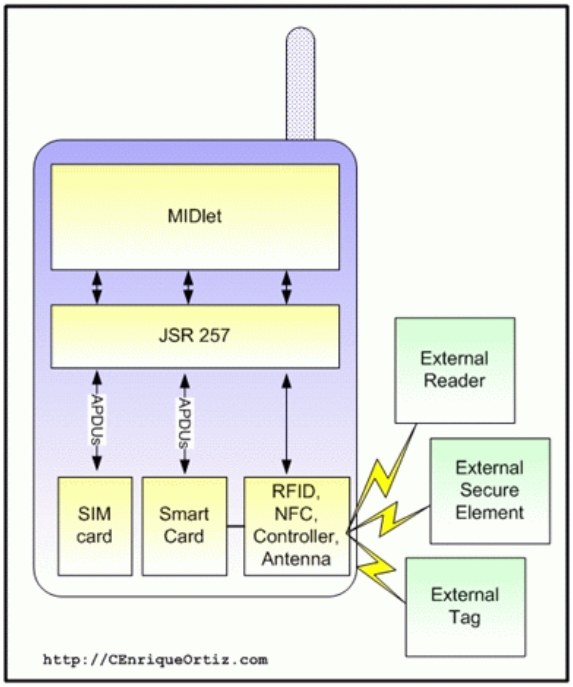


Fig. 19 Esquema Interno del manejo de la API de Comunicación sin Contacto en un móvil[35]

Este esquema muestra el manejo de un Midlet trabajando en el teléfono móvil, el cual a través de las especificaciones JSR-257 se comunica con el elemento seguro, en este caso una tarjeta SIM, por medio de unidades APDU[36] o se comunica directamente con el módulo NFC/RFID el cual está compuesto por un transponder (antena y receptor) y su controlador.

Una vez que se completa este proceso de comunicación interna, el dispositivo es capaz de interactuar con dispositivos externos, como etiquetas, smart cards, lectores externos y otros dispositivos compatibles NFC/RFID.

---

[35] **http://java.sun.com/developer/technicalArticles/javame/nfc/**

[36] **APDU: Aplication Protocol Data Unit, es el nombre que se le da a las unidades de datos del Protocolo Aplicación.**

3.3 DISEÑO DE LA APLICACIÓN MIDLET PARA LA COMUNICACIÓN NFC

El programa para la transmisión de la comunicación NFC es instalado en el teléfono móvil, pues será éste el que realiza la autenticación de un usuario y después de una aprobación exitosa, se comunicará con el receptor, que en este prototipo es el lector externo el cual recibe la trama y a través de otro programa que es el de recepción de la comunicación, la compara y si es válida procede al envío de una señal a través del puerto serial para la activación del acceso. Es decir que el sistema tiene dos tipos de validaciones, una en la parte de transmisión la cual autentica a un usuario mediante una contraseña y en la parte de recepción se valida que el flujo de datos que es recibido a través del lector sea el correcto para poder abrir el acceso. Si cualquiera de los dos no tiene una respuesta o validación correcta, el acceso permanece cerrado.

Tanto el teléfono móvil, como el lector Omnikey vienen con etiquetas, las cuales sirven de prueba para las primeras interacciones con la tecnología. Por lo tanto, durante el desarrollo de este proyecto se vio la importancia de incorporarlas tanto para entender mejor el funcionamiento de los diferentes modos de comunicación de NFC, como para explotar al máximo los recursos adquiridos.

Lo antes mencionado da lugar a que la transmisión pueda tener dos etapas, la comunicación directa entre el teléfono móvil y el receptor para el ingreso y la otra etapa es una comunicación indirecta entre el móvil y el lector a través de las etiquetas. Si bien se realiza en la segunda parte una comunicación indirecta entre los 2 dispositivos NFC, el móvil sigue siendo el principal actor para la comunicación NFC ya que es el responsable de escribir sobre la etiqueta una trama que valida a esta y la autoriza para el ingreso de un usuario solamente una vez, entonces la idea del proyecto tampoco se pierde porque sin el móvil la etiqueta no tendría ninguna validez para el ingreso.

La estructura del programa de transmisión se muestra a continuación:

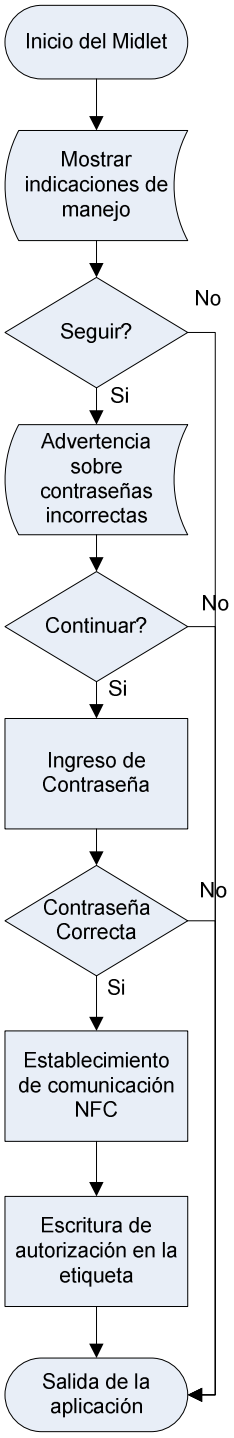


Fig. 20 Diagrama de Flujo de la aplicación del Teléfono móvil

3.3.1 UTILIZACIÓN DEL MÓDULO NFC INTERNO A TRAVÉS DE LA APLICACIÓN

El descubrimiento de las etiquetas y el establecimiento de la comunicación con el celular se lo realizaron a través de la interfaz de Comunicación sin contacto, la especificación JSR-257 antes mencionada. Como se explicó, permite la comunicación interna entre el módulo NFC y la aplicación. Para permitir el establecimiento de la comunicación NFC, la aplicación primero ejecuta la autenticación de los usuarios a través del ingreso de una contraseña. Esta contraseña es escrita en el cuerpo de la aplicación para que sea comparada con la ingresada. Esta puede ser números, caracteres o la combinación de estos. Para este prototipo se eligió la frase “dav1302” para que sea difícil de adivinarla.

3.3.2 INICIALIZACIÓN DE LA COMUNICACIÓN NFC

El primer paso para establecer la comunicación NFC es importar al Programa las librerías que habilitarán esta comunicación. Como se mencionó, el paquete principal para la comunicación NFC es javax.microedition.contactless, por lo que se procede:

```
import javax.microedition.contactless.*;
```

Permitiendo así habilitar las funciones principales para el manejo de NFC. Además de esto se necesita primero descubrir los objetivos soportados, en este caso las etiquetas que serán usadas; esto se lo realiza a través de la interfaz *TargetListener()* por medio del siguiente código establecido:

```
import javax.microedition.contactless.TargetListener;
:
TargetType[] targets = DiscoveryManager.getSupportedTargetTypes();
        // Get DiscoveryManager instance
```

```
DiscoveryManager dm = DiscoveryManager.getInstance();
try {
        dm.addTargetListener(this, TargetType.NDEF_TAG);
}

catch (ContactlessException ce) {
        // handle exception
}
```

Este código permite descubrir y registrar las etiquetas que estén al alcance del dispositivo, pero solamente se puede establecer una sola comunicación con una etiqueta. Al utilizar la clase TargetType(), estamos pidiendo que se busque los tipos de etiquetas soportadas, retornando un arreglo TargetType.

Una vez que la etiqueta ha sido descubierta y registrado el targetListener de interés, la aplicación invoca el método *targetDetected(TargetProperties[])*, el siguiente código permite ver mejor este método:

```
import        javax.microedition.contactless.TargetListener;
:
:
public void targetDetected(TargetProperties[] prop) {
            //Provoca que si no se encuentra ninguna etiqueta encuentre el final del
método
      if (prop.length == 0) {
         return;
      }

      // Crear una nueva Conexión NDEF
      NDEFTagConnection ndconn = null;
      try {
         // crea una conexión ndef tag
         String ur =
prop[0].getUrl(Class.forName("javax.microedition.contactless.ndef.NDEFTagConnecti
on"));

         //Abre la Conexión NDEF
         ndconn = (NDEFTagConnection) Connector.open(ur);

          //Se crea el Registro NDEF
```

```
NDEFRecord nuevo = new Text ("Diego Alejandro 1302");

NDEFMessage mensaje=new NDEFMessage(new NDEFRecord[] {nuevo});

            // write Information to Tag
            ndconn.writeNDEF(mensaje);

        } catch (Exception e) {
            //Se establece la excepción en caso de que no ocurrió la escritura en la
etiqueta
        }
        try {
            ndconn.close();
        } catch (Exception e) {
        }
        :
    }
```

Una vez que se invoca este método, se puede establecer la comunicación con la etiqueta. Ahora es cuando se puede realizar transacciones entre el teléfono móvil y la etiqueta, como lectura, escritura. El objetivo de la aplicación es habilitar una etiqueta mediante la escritura de un código que permita el ingreso al usarse, entonces la transacción que interesa es la escritura de la misma. Mediante el código anterior se puede realizar la escritura de una etiqueta compatible. El código de autorización para el ingreso es en este caso “Diego Alejandro 1302”, el cual al momento de la correcta validación será escrito en la etiqueta a través del celular.

Para la comunicación directa entre el teléfono móvil y el lector solamente se necesita acercarlo al lector e inmediatamente pedirá la contraseña que validará o no la comunicación. Una vez realizada la correcta autenticación se enviará la trama para ser leída y comparada por el software de recepción y después se realizará la comunicación serial para la activación del acceso. La trama correcta entre la comunicación directa del móvil con el lector es 8B E3 1D 02 (trama hexadecimal) la cual permitirá el ingreso del usuario.

3.4 DISEÑO DEL SOFTWARE PARA LA RECEPCIÓN DE LA COMUNICACIÓN NFC (24) (25) (26)

La parte de recepción está conformada por el Lector OMNIKEY 5321, el cual irá conectado a un computador (CPU) que a más de tener instalados los drivers de funcionamiento del lector mismo, permitirá correr una aplicación que estará encargada de la recepción de las tramas enviadas al lector.

La función de este software es manejar las distintas tramas que el lector recoge desde los dispositivos NFC/RFID que se acercan y procesarlas. Si al comparar una trama, coincide con la trama válida, este será también el encargado de enviar hacia el exterior del CPU, a través de comunicación serial para abrir el acceso.

Al momento del arranque del programa, se va a preguntar al usuario o a la persona encargada de instalar el sistema, por cuál de los puertos seriales que estén habilitados, será el envío de la comunicación serial al exterior. Hay que tomar en cuenta que mientras el sistema esté en funcionamiento y la aplicación esté corriendo, el puerto serial estará ocupado, por lo que no estará disponible o podría generar conflictos si se lo quiere usar con otra aplicación. A través de Visual Basic se puede manejar los controladores que permiten la comunicación entre el lector y la PC de una manera más sencilla así como manejar la comunicación serial.

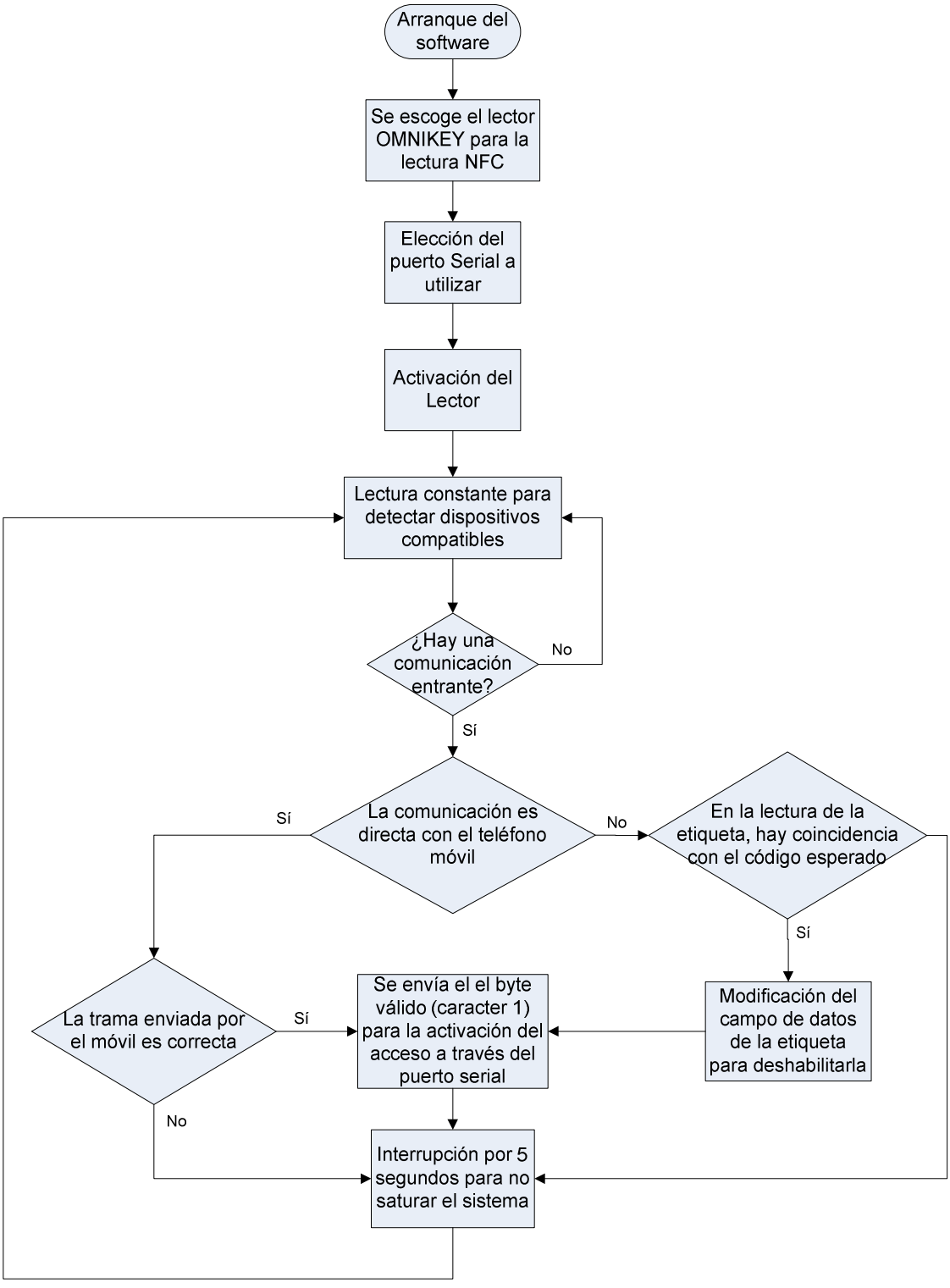


Fig. 21 Diagrama de flujo de la aplicación de Recepción

Para el manejo del puerto serial primero se debe llamar a una función que permita el manejo de entrada y salida de datos a través de puertos, por lo que es necesario:

```
Imports System.IO.Ports
```

Esta línea habilita las funciones para la comunicación a través del puerto serial. Para la comunicación serial se establecen los siguientes parámetros:

- Velocidad: 9600 Baud
- Bits de datos: 8 bits
- Paridad: ninguna
- Bits de parada: 1

Para que el programa realice el envío de la trama correcta por el puerto serial para que posibilite el ingreso, al comparar las tramas entrantes tanto en el caso de las tramas enviadas por el celular o en el otro caso las tramas enviadas por la etiqueta, deben ser iguales a las que el software lee internamente, por ejemplo en el caso de que la etiqueta envíe en su campo de datos la frase “Diego Alejandro 1302”, se tendría una comunicación exitosa y se enviaría la señal para activación del ingreso. Para mayor facilidad y para que al momento de receptar el PIC la comunicación serial no tenga que realizar mucho procesamiento, se eligió como el byte correcto el caracter 1 (31 en número hexadecimal y en binario 00110001). Para el envío de datos hacia el puerto serial primero se debe abrir el puerto serial que va a ser utilizado; una vez abierto se envían los datos a través del comando SerialPort.Write() y una vez terminado el envío de la trama, se debe cerrar el puerto para evitar errores de comunicación. La programación sería de esta manera:

```
Try
        SerialPort.Open()
        Catch ex As System.Exception
        MessageBox.Show(ex.ToString())

End Try
```

SerialPort.Write(“Byte que contiene los datos a transmitir”, “miembro del byte que contiene los datos”, “contador para transmitir el número de datos”)

SerialPort1.Close()

Para realizar la comunicación entre el lector y la PC se utilizó 2 clases ya creadas, Scard y ScardCL, las cuales declaran y manejan las librerías de los controladores del lector, pero las que nos interesan para nuestra aplicación son:

Librerías de la clase Scard:

- SCardEstablishContext Lib "WINSCARD" (ByVal dwScope As Integer, ByVal pvReserved1 As Integer, ByVal pvReserved2 As Integer, ByRef phContext As Integer) As Integer

  Establece un contexto para Manejar los recursos
  Sus parámetros son:

  - dwScope = Alcance
  - pvReserved1 = Reservado para uso futuro
  - pvReserved2 = Reservado para uso futuro
  - phContext = Puntero de contexto

- SCardListReaders Lib "WINSCARD" Alias "SCardListReadersA" (ByVal hContext As Integer, ByVal mszGroups As Byte, ByRef mszReaders As Byte, ByRef pcchReaders As Integer) As Integer

  Maneja toda la lista de los lectores disponibles.
  Sus parámetros:

  - hContext = Contexto Actual
  - mszGroups = Contiene el grupo de nombres de lectores. Si este parámetro no es nulo, entonces solamente los lectores que pertenecen a un grupo son enlistados
  - mszReaders = Contiene los nombres de los lectores disponibles
  - pcchReaders = Longitud de mszReaders en Bytes

- SCardConnect Lib "WINSCARD" Alias "SCardConnectA" (ByVal hContext As Integer, ByVal szReader As String, ByVal dwShareMode As Integer, ByVal dwPreferredProtocols As Integer, ByRef hCard As Integer, ByRef dwActiveProtocol As Integer) As Integer

  Conecta a un Lector específico.

Sus parámetros:
- hContext = Contexto actual
- szReaders = Nombre de un lector
- dwShareMode = Modo compartir
- dwPreferredProtocols = Protocolo preferido
- hCard = Manejo de tarjeta
- dwActiveProtocol = Protocolo retornado

Librerías de la clase ScardCL:

- SCardCLGetUID Lib "scardsyn" (ByVal ulHandleCard As Integer, ByRef pucUID As Byte, ByVal ulUIDBufLen As Integer, ByRef pulnByteUID As Integer) As Integer

  Permite obtener el UID de una tarjeta

  Sus parámetros:
  - ulHandleCard = Manejador provisto desde “El administrador de recursos de la Smart card” después de conectar la tarjeta (ScardConnect).
  - pucUID = Es el identificador único de la tarjeta sin contacto.
  - ulUIDBufLen = Longitud del buffer donde se guarda el UID.
  - pulnByteUID = número de bytes del UID.

- SCardCLMifareStdRead Lib "scardsyn" (ByVal ulHandleCard As Integer, ByVal ulMifareBlockNr As Integer, ByRef pucMifareDataRead As Byte, ByVal ulMifareDataReadBufLen As Integer, ByRef pulMifareNumOfDataRead As Integer) As Integer

  Permite la lectura de los bloques de una tarjeta soportada.

  Sus parámetros:

  - ulHandleCard = Manejador para Mifare card provisto desde “El administrador de recursos de la Smart card” después de conectar la tarjeta (ScardConnect)
  - ulMifareBlockNr = El número del bloque Mifare el cual va a ser leído, para Mifare 1K es de 0 a 63, para Mifare 4K es de 0 a 255 y para Mifare Ultra Light es de 0 a 15.
  - pucMifareDataRead = Puntero al búfer asignado para la lectura de los datos de la tarjeta
  - ulMifareDataReadBufLen = El tamaño del búfer, deber ser 16 o mayor.
  - pulMifareNumOfDataRead)= Retornará el número de bytes recibidos de la tarjeta y siempre será 16 si la lectura fue exitosa.

- SCardCLMifareStdWrite Lib "scardsyn" (ByVal ulHandleCard As Integer, ByVal ulMifareBlockNr As Integer, ByRef pucMifareDataWrite As Byte, ByVal ulMifareDataWriteBufLen As Integer) As Integer

  Permite la escritura en los bloques de una tarjeta Mifare

  Sus Parámetros:

  - ulHandleCard = Manejador para Mifare card provisto desde “El administrador de recursos de la Smart card” después de conectar la tarjeta (ScardConnect).
  - ulMifareBlockNr = El número del bloque Mifare el cual va a ser escrito, para Mifare 1K es de 1 a 63, para Mifare 4K es de 1 a 255 y para Mifare Ultra Light es de 2 a 15.
  - pucMifareDataWrite = El puntero para un búfer de 16 bytes, los datos a ser escritos.
  - ulMifareDataWriteBufLen = El tamaño del búfer de datos, debe ser 16.

Para el manejo del lector, el programa continuamente debe estar llamando a estas librerías una vez que se lo active a través del botón “activar lector” en la pantalla principal del programa y puesto que el programa deberá estar en continuo uso después del arranque, no deberá detenerse y deberá estar llamando a las subrutinas que controlan estas librerías y así controlar al lector.

Fig. 22 Pantalla principal de la aplicación de Recepción

3.5. PROGRAMACIÓN DEL PIC 16F877A

El PIC es el encargado de la recepción de la comunicación serial enviada a través del puerto de la PC elegido por el usuario y recepta los bytes que le llegan a través del puerto 26, los compara para ver si es el byte correcto (el caracter 1) para enviar la señal de activación del acceso y permitir el ingreso.

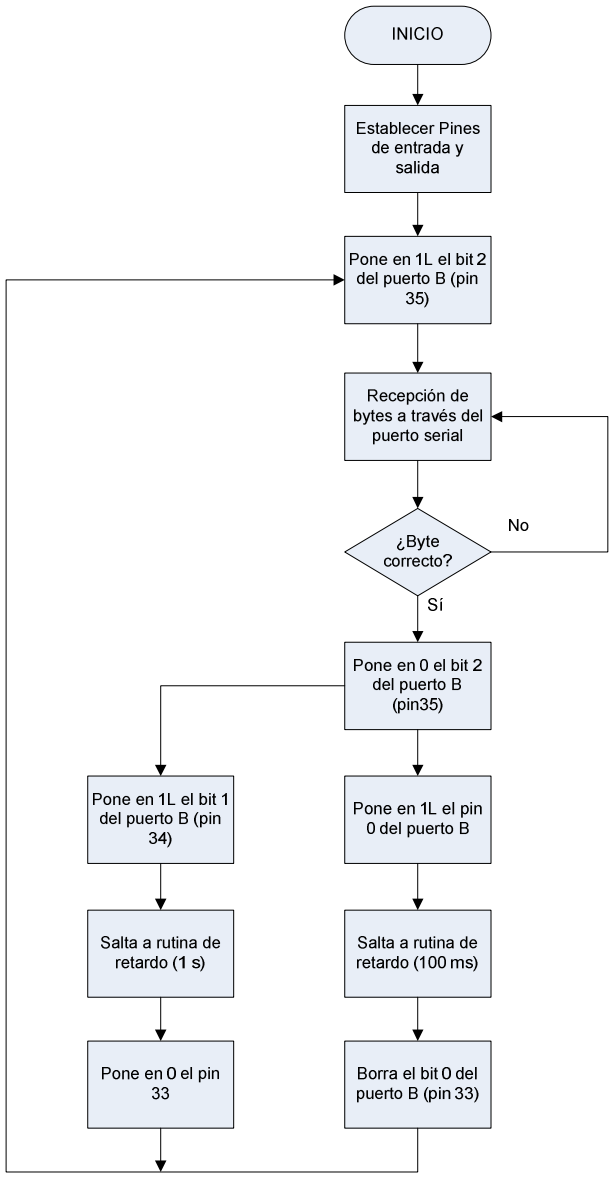


Fig. 23 Diagrama de trabajo del PIC

El PIC al igual que el programa en la computadora debe seguir trabajando continuamente para estar dispuesto a recibir datos del puerto serial y activar el acceso, si fuera el caso, en cualquier momento.

Mientras el acceso permanece cerrado, es decir si no llega el byte correcto que permita su apertura, el PIC encenderá un led rojo a través de su pin 35, indicando al usuario que está cerrado. Al momento de envío del byte correcto por el puerto serial (carácter 1), el PIC lo leerá y comparará y dará una respuesta positiva enviando un pulso para permitir el ingreso a través del pin 33 y encenderá un led verde por medio del pin 34 indicando al usuario que se realizó una correcta autenticación y durante un segundo, tiempo en el cual se apagará el led rojo al poner en 0L el pin 35.

3.6. SIMULACIÓN DEL PROTOTIPO

Para entender mejor el funcionamiento del prototipo y para corregir los errores que puedan ocurrir antes de la implementación, es importante realizar simulaciones. Para lograr esto es necesario de herramientas que simulen los equipos y elementos usados en el proyecto.

Una herramienta que permite el manejo del teléfono móvil Nokia 6212 es la Plataforma Series 40 SDK, creada por Nokia el cual nos dará facilidad para experimentar el manejo NFC en un ambiente virtual.

La etapa de recepción de la comunicación serial y de potencia se puede simular a través de Proteus, herramienta que permite el manejo de componentes eléctricos y electrónicos y también la interacción con equipos de manejo y evaluación de estos.

3.6.1. PLATAFORMA SERIES 40 SDK (27)

La plataforma Series 40 de Nokia es un Software Development Kit (SDK), una herramienta que permite la simulación y el desarrollo de aplicaciones NFC mediante el uso de teléfonos móviles de la serie 6212 Classic, brindando una interfaz gráfica, amigable con el usuario para una más fácil relación con la tecnología y dejando ver la interacción entre NFC y el dispositivo en un ambiente virtual. Los requisitos para la instalación de esta plataforma son:

- Sistema Operativo Microsoft Windows XP Professional con Service Pack 2
- Memoria de 512 MB
- Procesador Pentium 1 GHz
- Espacio Libre de Disco Duro de 150 MB
- Capacidad de Color de 16-bit en resolución de 1024 x 768 pixeles

Estos requisitos fueron los que limitaron el uso por ejemplo de otro sistema operativo a la hora de desarrollo de la aplicación del prototipo ya que la interfaz gráfica de la plataforma SDK de Nokia no es soportada por el sistema operativo Microsoft Windows Vista y sin esta plataforma no se podría cumplir con los requisitos de simulación del proyecto.

Este SDK puede funcionar por si solo como un Kit de desarrollo o puede servir de soporte para ambientes de desarrollo integrados (IDE). Por medio de esta característica final, se puede utilizar su emulador para probar de una manera rápida aplicaciones de la plataforma Java sobre Teléfonos celulares (J2ME). Los ambientes de desarrollos soportados por esta plataforma son:

IDEs de Navegadores	IDEs de Mensajería	IDEs de Desarrollo MIDP
Adobe GoLive CS2	Adobe GoLive CS2	Eclipse 3.3.1 with EclipseME 1.7.6
Adobe Dreamweaver 8		Netbeans 6.0

Tabla. 12 Ambientes de Desarrollo soportados por la plataforma Series 40 SDK

Por esta característica de soporte a IDEs, esta herramienta fue de mucha utilidad para realizar pruebas de la aplicación en Netbeans de este proyecto ya que a través de su simulación se pudo verificar fallas y de haberlas, lograr solucionarlas antes de la implementación y así tener una mayor eficacia al desarrollarla. Además este SDK puede interactuar con dispositivos reales ya que utiliza de cómo interfaz de salida lectores que estén conectados a la misma computadora de trabajo y que sean compatibles con esta herramienta. Los Lectores externos que soporta esta plataforma SDK son los siguientes:

- OMNIKEY CardMan 5321
- MFRD701 Mifare Pegoda

Es por esta razón que se escogió el lector OMNIKEY 5321 USB, por su compatibilidad con el SDK y para poder obtener las simulaciones necesarias para el proyecto.

El Series 40 SDK está formado de 2 partes, el emulador y el Administrador de Conexiones NFC:

- **Emulador:** El emulador es una herramienta gráfica que permite la emulación de un teléfono móvil 6212 Classic real, cumpliendo las mismas funciones y las mismas prestaciones del dispositivo real.

Fig. 24 Emulador SDK

- **NFC Manager:** El Administrador de Conexiones NFC permite al NFC interactuar con etiquetas, Smart Cards y lectores externos compatibles NFC.

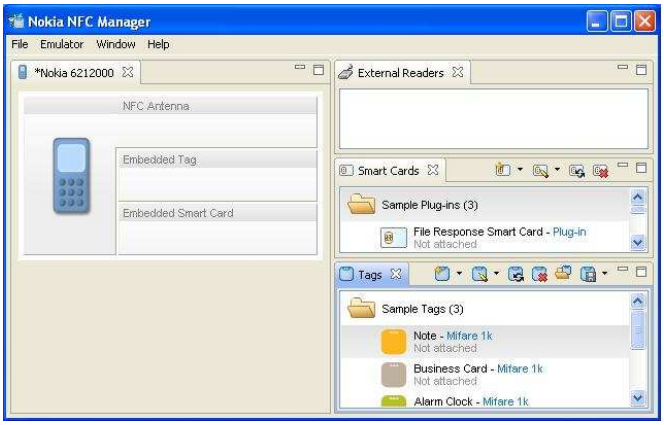


Fig. 25 Nokia NFC Manager

3.6.2. SIMULACIÓN DEL SISTEMA

Debido a que no se pueden integrar entre si las herramientas necesarias para el manejo de los equipos y las simulaciones, no se puede realizar una simulación completa de todo el sistema por lo que se va a realizar la simulación por partes para ver el funcionamiento en un ambiente virtual y corregir errores de haberlos.

3.6.2.1 Simulación del la aplicación del teléfono

Se debe conectar primero el lector a la computadora para que al momento de ejecutar la simulación, el lector sea reconocido por el SDK de Nokia y permita la interacción del mismo así como nos permita comunicarnos con el exterior a través de la simulación (por ejemplo al escribir una etiqueta).

Fig. 26 Selección del Lector

Una vez elegido el lector, arranca la simulación del midlet.

3.6.2.2 Simulación del la aplicación de recepción

La aplicación de recepción empieza con la elección del puerto serial que va a estar en constante uso mientras el sistema este en funcionamiento

Fig. 27 Mensaje al arrancar el software de recepción

Fig. 28 Selección del puerto Serial

Una vez que se elige el puerto serial que va a utilizar el sistema, lo único que falta es hacerlo funcionar para que el lector empiece a recibir datos y el programa los compare para ver si son válidos, entonces presionamos el botón “Activar Lector” para arrancar el software.

Fig. 29 Activación del Lector

3.6.2.3 Simulación del la etapa de recepción de la comunicación serial

Como se comentó anteriormente, el PIC al momento de iniciar su funcionamiento, encenderá un Led rojo el cual indicará al usuario que el acceso se encuentra cerrado.

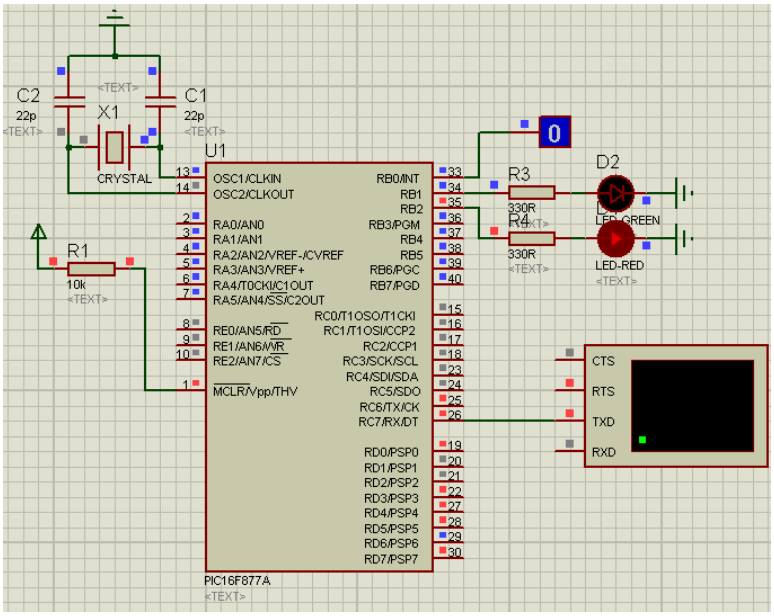
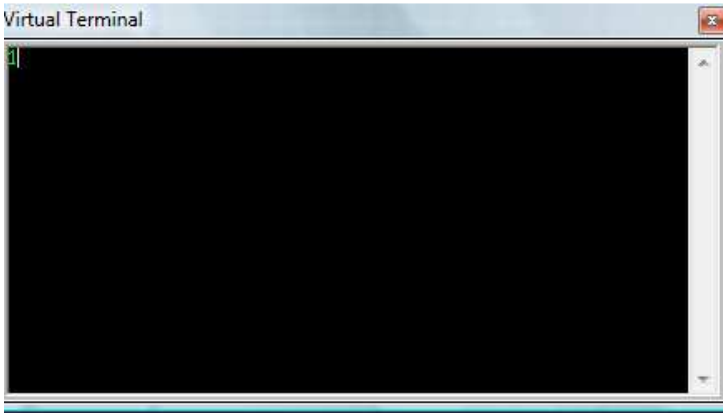


Fig. 30 Inicio de la simulación del PIC

Puesto que no se puede integrar la herramienta de simulación que maneja el lector y el celular a Proteus para mostrar su interacción con el circuito, se utilizó un terminal virtual el cual tomará el lugar de la computadora en la cual está corriendo el programa de recepción y cuando sea correcta la comunicación, enviará el carácter 1.



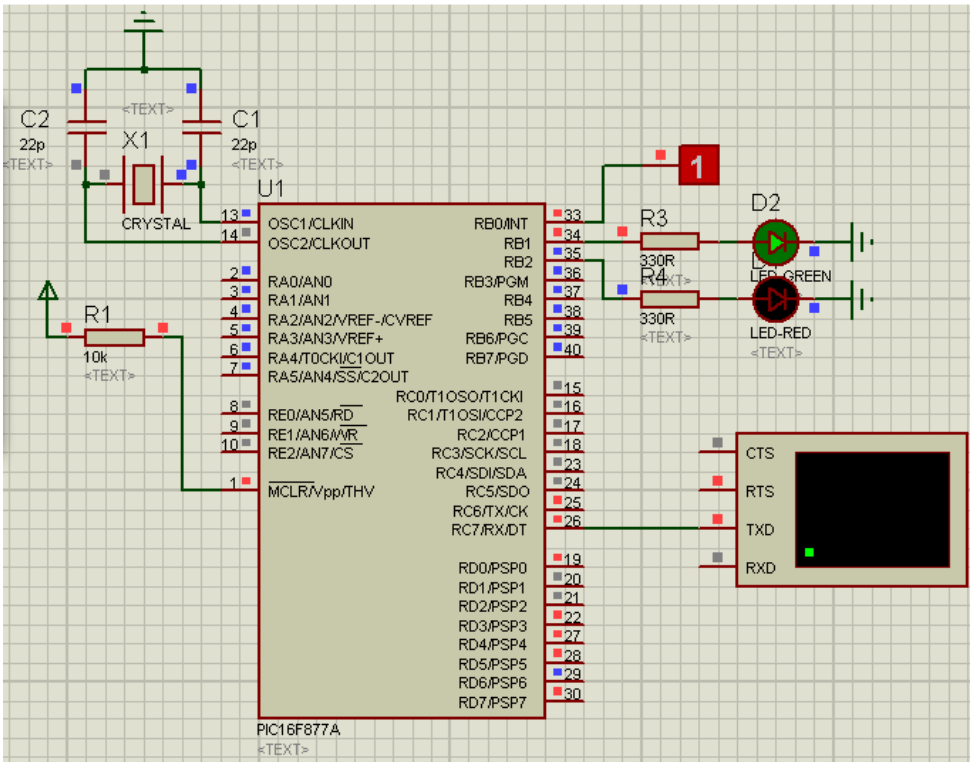


Fig. 31 Salida de señal a través del PIC

Podemos comprobar que después de que la computadora envía la señal correcta es decir el byte 00110001 (carácter 1), apaga el Led rojo y enciende el Led verde al igual que envía un 1L hacia el pin 33 que es la salida del PIC y que va conectado a la etapa de potencia para la activación de la puerta, por lo tanto la programación del PIC es la correcta y su funcionamiento es el esperado.

3.6.2.4 Simulación de la etapa de potencia

Esta es la etapa final del sistema ya que permite el acceso a través de una señal que permite activar el relé y mediante éste abrir el acceso. La señal de activación del relé es producida por el pin 33 del PIC después de un proceso de validación correcto.

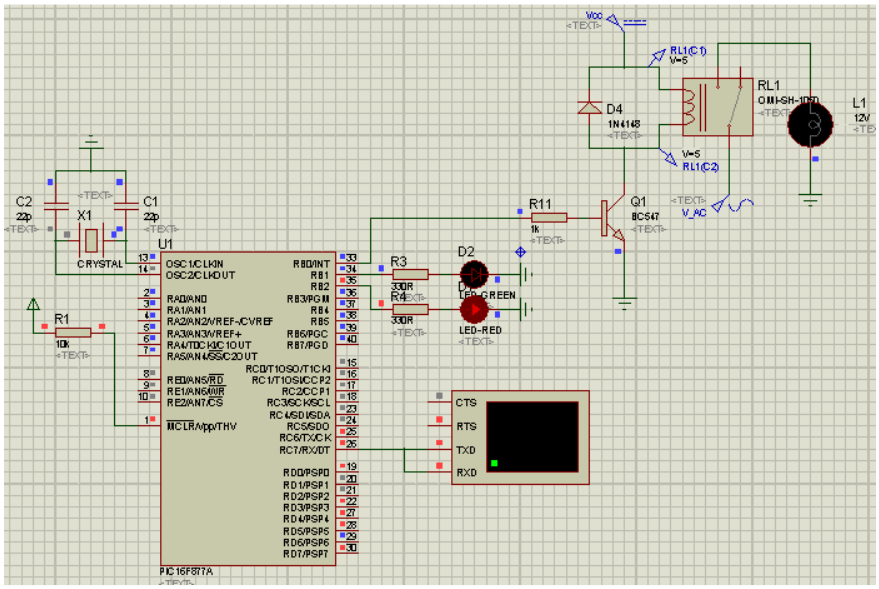


Fig. 32 Etapa de potencia sin estimular

Como se puede observar, mientras no existe una estimulación en el pin 33, no se activará el relé y por lo tanto no permitirá abrir el acceso. Para esta simulación en lugar de un acceso se intenta encender una lámpara de igual voltaje de funcionamiento que el acceso. Y a continuación se puede ver como al momento de enviar un 1L al pin 33 la lámpara se enciende demostrando así el funcionamiento correcto del sistema.

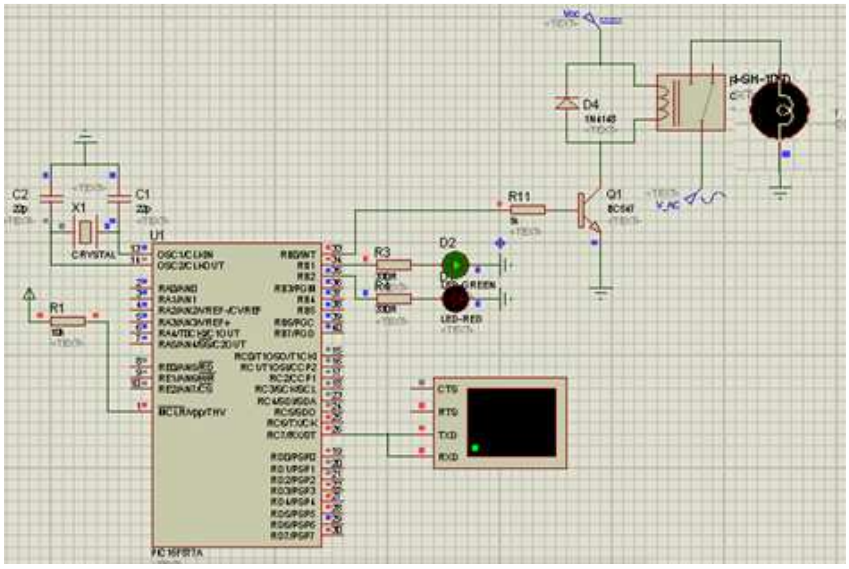


Fig. 33 Estimulación de la etapa de potencia y activación del acceso

CAPITULO 4. PRUEBAS, RESULTADOS Y COSTOS DEL PROYECTO

Este capítulo muestra los resultados que se han obtenido del funcionamiento del sistema después de la implementación y después de la corrección de los errores.

Cada etapa, al igual que con las simulaciones, fue probada antes de conectar el sistema por completo, ya que si alguna de éstas tenía un desenvolvimiento inesperado o producía un error, podría ocasionar que todo el conjunto del sistema sufriera daños.

Para la realización de las pruebas se utilizó:

- Una computadora en la que corra la aplicación de recepción y que soporte los controladores del lector OMNIKEY, con las siguientes características:
  - Intel Core 2 Duo
  - 512 MB de memoria RAM
  - Procesador de 2.20 GHz
  - Sistema Operativo Windows XP Service Pack 2

Cabe mencionar que el transcurso y diseño del proyecto se diseño en una máquina virtual obteniendo los mismos resultados que una máquina real.

- Lector OMNIKEY 5321
- Teléfono Móvil Nokia 6212 Classic con tecnología NFC
- PIC 16F877A
- Maqueta de una puerta con cerradura eléctrica como el acceso de nuestra aplicación. La cerradura eléctrica trabaja con un voltaje de 12 VAC por lo que para conectarla a la red eléctrica se necesitó de un transformador que diera ese voltaje de salida. Además un relé que permita la activación de la puerta mediante

una señal de 5 VDC de entrada y que sus contactos soporten ese voltaje de corriente alterna o superior.

- Etiquetas Mifare 1K y RFID para realizar las pruebas de la aplicación para habilitarlas y acceder con ellas

4.1 PRUEBAS EN LA ETAPA DE POTENCIA

Para las pruebas de esta etapa se armó el circuito diseñado en el capítulo anterior, tomando en cuenta tanto la señal de salida del PIC, 5 VDC como el voltaje requerido para abrir la cerradura eléctrica, 12 VAC.

Se conectó un pulsador entre la fuente que genera la señal de entrada y el circuito de potencia, para simular los impulsos que el PIC envíe cuando tenga éxito la autenticación.

Se utilizó un relé que se estimule con 5 VDC de entrada y que soporte hasta un voltaje de 125 VAC, cumpliendo con los requisitos del sistema.

4.2 PRUEBAS EN LA ETAPA DE RECEPCIÓN DE LA COMUNICACIÓN SERIAL

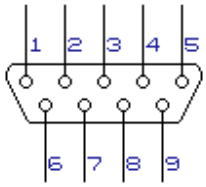
Para estas pruebas con la comunicación serial se utilizó el Hiperterminal, herramienta que viene dentro del paquete del sistema operativo Windows XP y permite comunicaciones seriales y manejo de sus puertos. Se lo configura según la configuración de la comunicación serial establecida en nuestro sistema, que es la configuración predeterminada del Hiperterminal:

Velocidad: 9600 Baudios
Bits de datos: 8 bits
Paridad: Ninguna
Bits de parada: 1 bit

Primero probamos que el Hiperterminal y el puerto que se escogió para la comunicación estén funcionando y una vez probado con éxito se conecta el puerto

serial escogido al pin 13 del MAX-232 que será el que convierta la señal RS-232 para adaptarla al PIC con señales TTL.

El conector DB-9 que se utiliza para el puerto serial tiene la siguiente distribución de pines:



1. CD - Carrier Detect
2. RXD - Receive Data
3. TXD - Transmit Data
4. DTR - Data Terminal Ready
5. GND - Ground
6. DSR - Data Set Ready
7. RTS - Request To Send
8. CTS - Clear To Send
9. RI - Ring Indicator

De esta lista, para mi aplicación, sólo necesito el pin 3 para transmitir datos desde la PC y el pin 5 que es la referencia. La salida del MAX-232 hacia el PIC es el pin 12 el cual transmite señales TTL y este va conectado al pin 26 del PIC que es el pin de recepción.

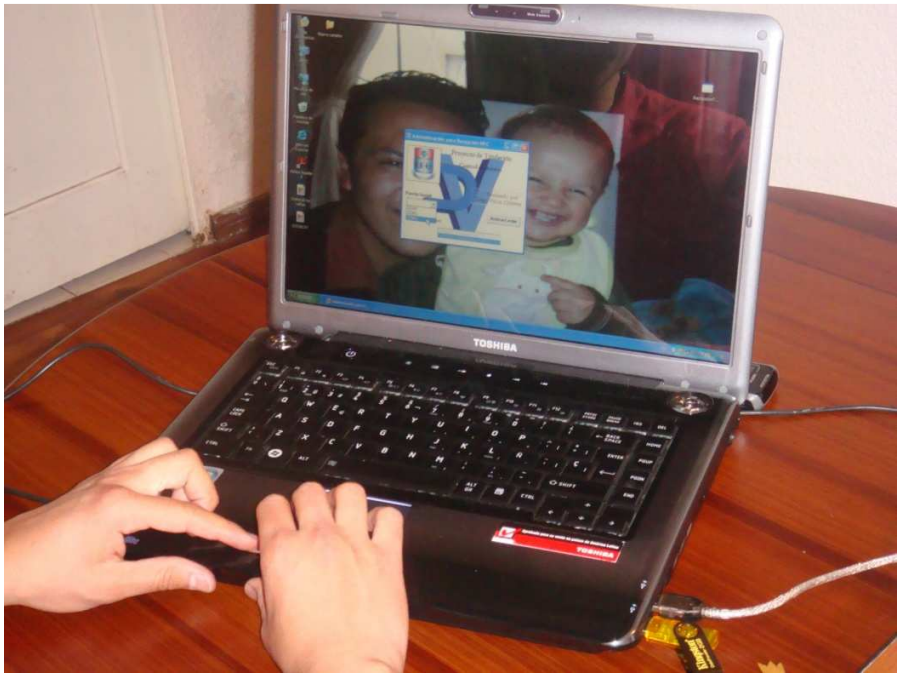
Para probar el funcionamiento sólo se conectan los Leds a la salida del PIC que nos indicarán si realmente está receptando las señales transmitidas a través del puerto serial ya que la programación del PIC comprobamos que era correcta en las simulaciones del capítulo anterior.

Se alimenta el circuito con 5 VDC e inmediatamente debe encenderse el led rojo conectado al pin 35 del PIC. En la pantalla del Hiperterminal se pulsa la tecla del número 1 y se observa si hay algún cambio en el encendido de los leds, es decir se debe encender el led verde y apagarse el led rojo.

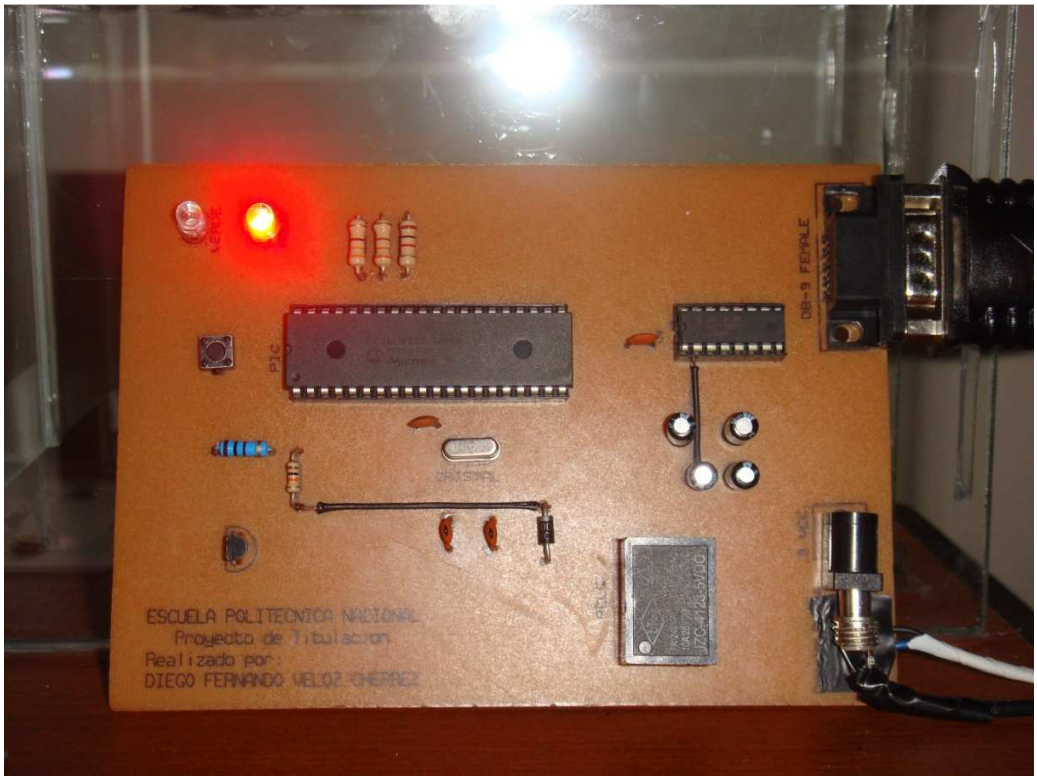
4.3PRUEBA DE FUNCIONAMIENTO DE TODO EL SISTEMA

Una vez que se comprobó la recepción de la comunicación serial y la etapa de potencia, se puede determinar que el funcionamiento de la parte de circuitería es correcto, por lo tanto se procede a la conexión total del sistema.

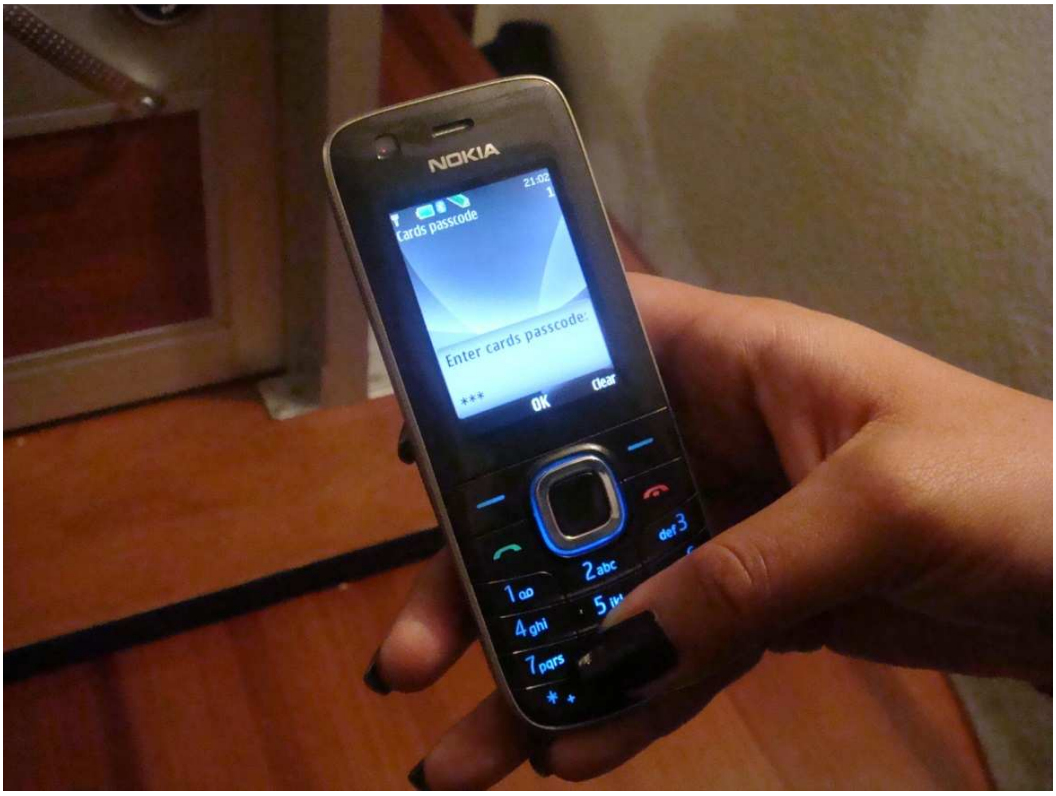
A continuación se muestran imágenes de la interacción con el prototipo:
Primero se pone en funcionamiento la aplicación de recepción para de esta manera activar el lector y esté apto para acoger las tramas.

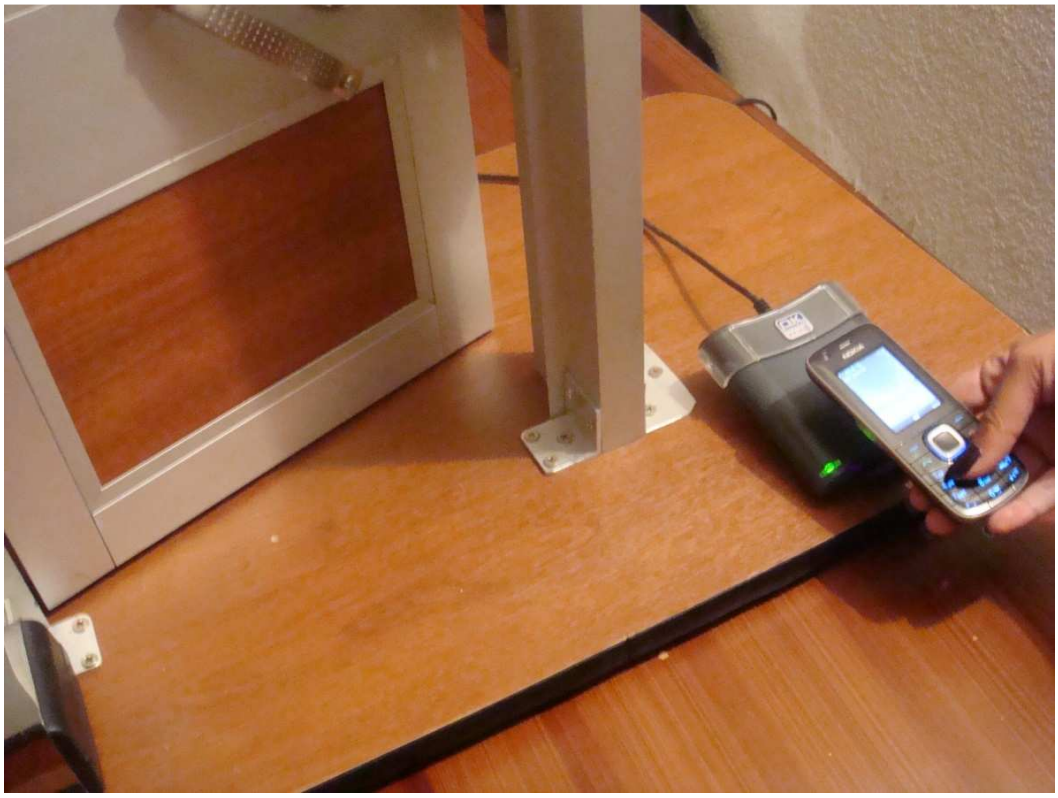


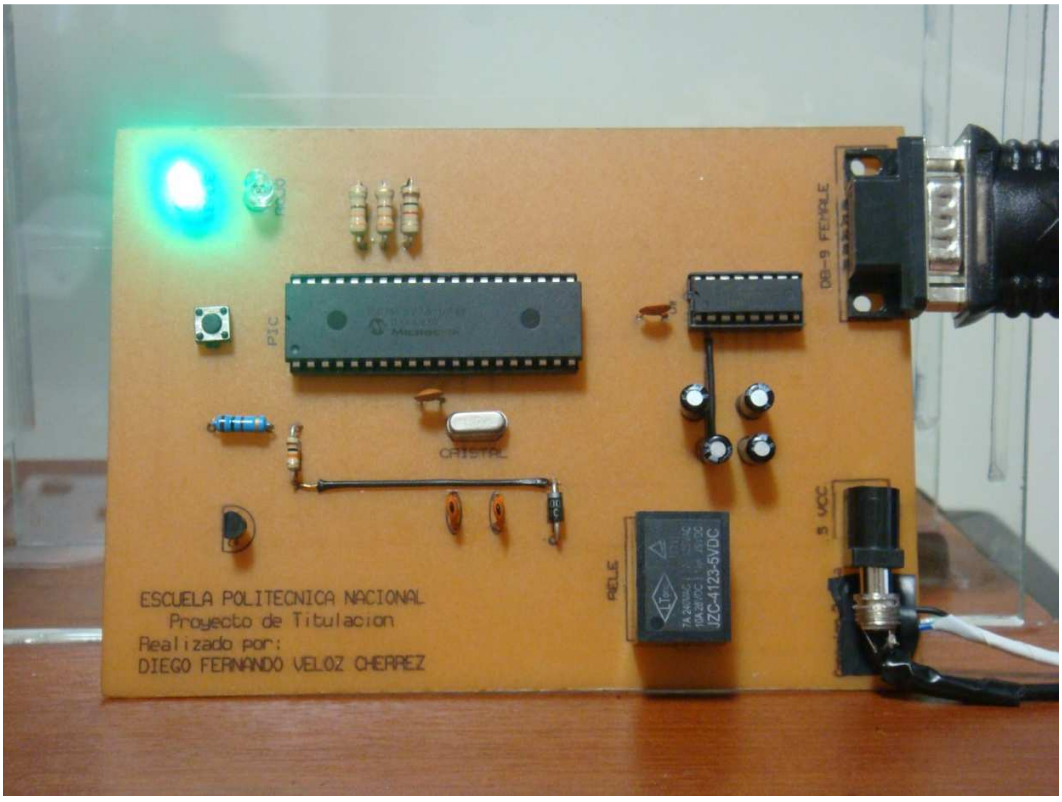
Una vez elegido el puerto y activado el lector se alimenta el circuito total del sistema, y se observa el led rojo encendido indicando que la puerta está cerrada.



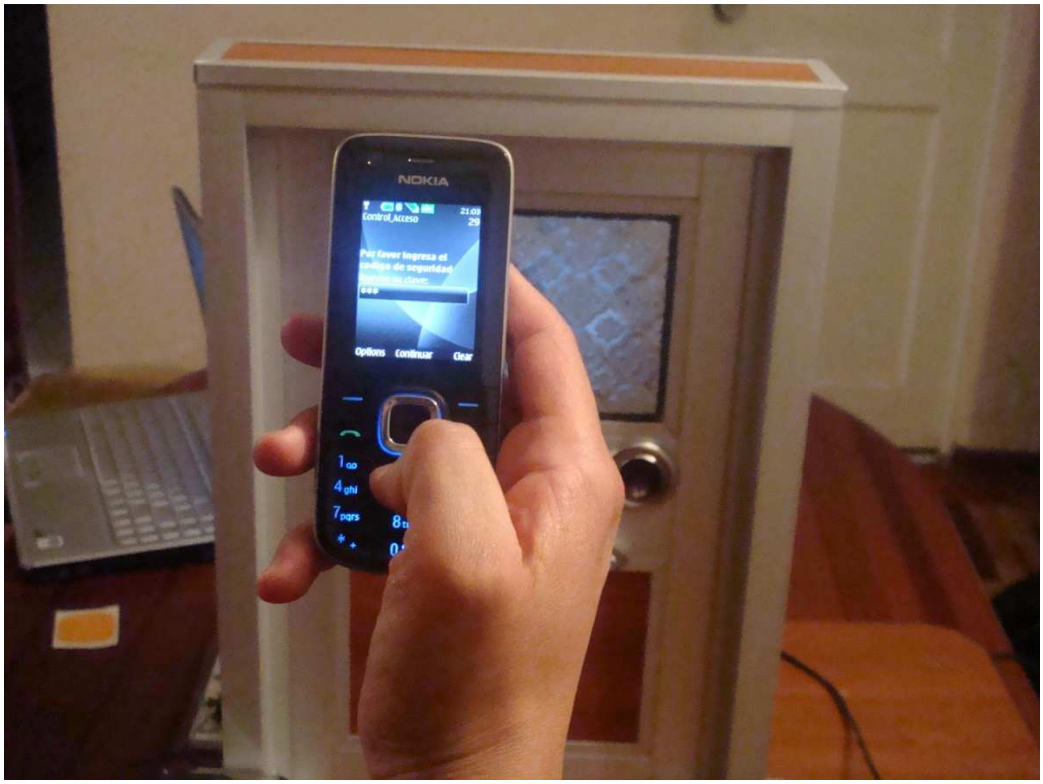
Se utiliza el celular para la validación y envío de información al lector.

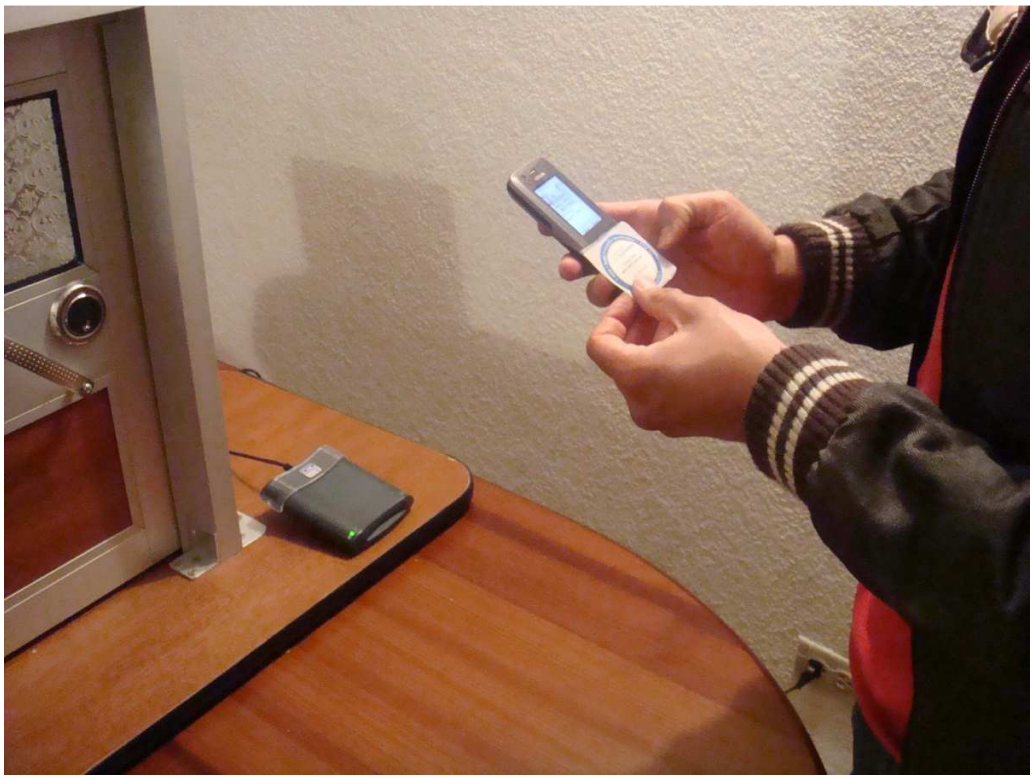

NOKIA
21:02
Cards passcode
Enter cards passcode:
***
OK
Clear

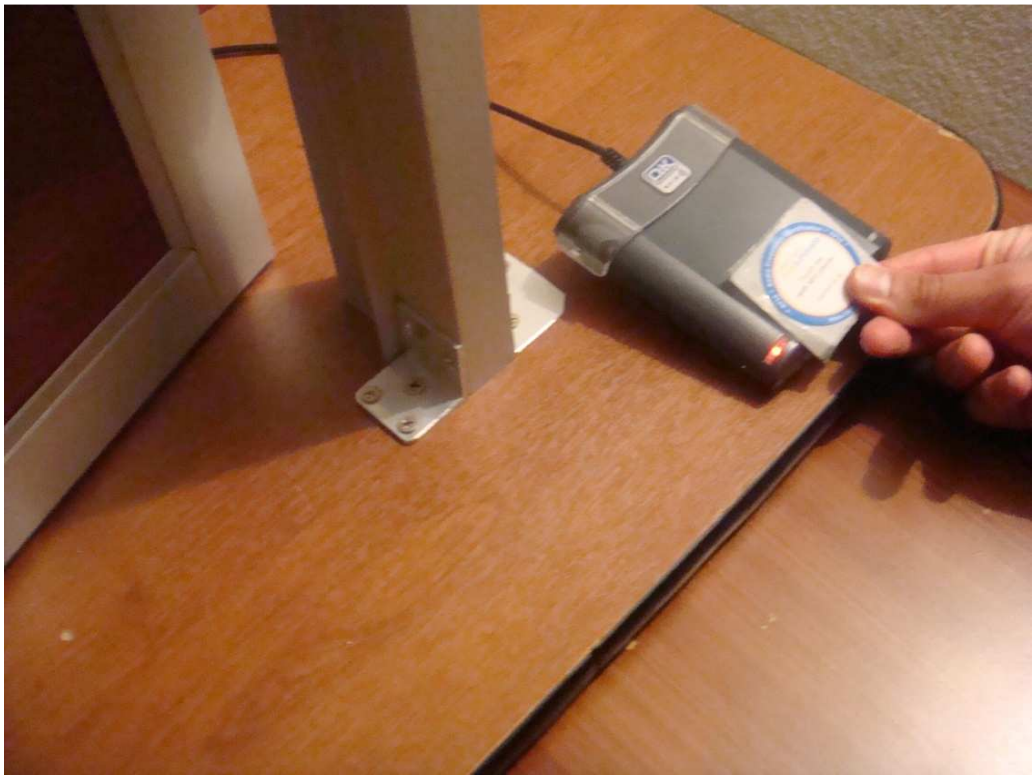



DB-9 FEMALE
PIC
CRISTAL
RELE
JZC-4123-5VDC
5 VCC
ESCUELA POLITECNICA NACIONAL
Proyecto de Titulacion
Realizado por:
DIEGO FERNANDO VELOZ CHERREZ

Ahora se utiliza la aplicación para habilitar etiquetas para el ingreso:







Como se puede observar en las imágenes, el prototipo dio los resultados esperados interactuando tanto en forma directa entre el celular y el lector así como indirectamente a través de las etiquetas. Así mismo las simulaciones realizadas en el capítulo anterior nos dieron un adelanto del funcionamiento real con mínimas diferencias, tal vez por ejemplo en la velocidad con que trabaja la tecnología ya que por ejemplo en las simulaciones se podía ver todos los mensajes que mostraba el celular a la hora de escribir una etiqueta y en la realidad casi no se percibe. Esto es entendible ya que depende del procesamiento de la computadora en la cual se corre la herramienta. Pero en las demás funciones arrojan grandes similitudes.

4.4 COSTOS DEL PROYECTO

Dado que la tecnología NFC está en desarrollo en algunos países de Europa y de Asia y en el país se tiene muy poco conocimiento de ello, los principales equipos para el desarrollo del proyecto se debieron buscar en el exterior a través de internet.

Para dar un enfoque acerca del costo total para la implementación de este proyecto se debe tomar en cuenta no sólo el precio en sí de los productos si no también el costo de envío, las horas de programación e implementación de las aplicaciones, el costo de la maqueta del acceso y de la circuitería.

El pedido de el teléfono se lo hizo por internet en Finlandia, en cambio el lector se lo encontró en Estados Unidos; por esta razón los costos subieron con respecto a si se los encontrara en el mercado nacional.

En el siguiente cuadro se detalla el costo total del proyecto:

Detalle	**Cantidad**	**Valor Unidad ($)**	**Valor Total ($)**
Lector OMNIKEY 5321 USB	1	105 $	105 $
Envió Lector		35 $	35 $
Nokia 6212 Classic	1	344.99 $	344.99 $
Envío Teléfono		69,95 $	69,95 $
PIC 16F877A	1	6,80 $	6,80 $
Circuitería		12 $	12 $
Maqueta	1	109 $	109 $
Costo de Software	480 horas	10 $	4800 $
Total			5482,74 $

Tabla 13. Costos de implementación del proyecto

CAPÍTULO 5. CONCLUSIONES Y RECOMENDACIONES

5.1CONCLUSIONES

- Durante el desarrollo del proyecto, se cumplió con los objetivos expuestos en el plan de titulación al realizar un control de acceso con tecnología NFC y usando un teléfono móvil como dispositivo para la autenticación y transmisión hacia el receptor.

- El sistema implementado funciona de una manera autónoma para la implementación en lugares donde no se necesite el control adicional de una persona, por ejemplo una casa, una habitación, un laboratorio, etc.

- Se introdujo un conocimiento básico de la tecnología NFC, detallando sus características principales, así como de las ventajas y desventajas respecto a otras tecnologías.

- Las aplicaciones mediante el uso de NFC pueden ser ilimitadas, no sólo con su actuación directa sino que puede ser una vía para que se comuniquen o para el establecimiento de otras como el caso de Bluetooth.

- Su compatibilidad con otras tecnologías permite que NFC entre al mercado ganando terreno fácilmente y permite que el cambio a ésta sea de una manera más suave sin la necesidad de la sustitución de toda una infraestructura en uso.

- Respecto a sistemas de control de acceso utilizando por ejemplo RFID se puede ver una enorme ventaja que NFC implementa ya que una simple tarjeta no permite una interacción con el usuario y cualquiera que la posea puede tener acceso a dicho lugar. Mediante el uso del celular se puede crear aplicaciones que

permiten una mayor seguridad a través de la autenticación, antes de establecer la comunicación NFC.

- Su corto alcance es importante pues brinda una mayor seguridad, ya que para realizar una intercepción a una comunicación NFC quién lo trate de hacer debería estar a menos de 10 cm. Además de esto, cuando dos dispositivos NFC se los acerca entrando al campo de operación, se está automáticamente aceptando la comunicación, lo que permite mayor rapidez en su establecimiento.

- Se realizó dos tipos de comunicaciones para permitir el acceso, la una directamente a través del lector y el celular y la otra a través de etiquetas, pero habilitándolas a través del mismo teléfono, es decir que en cualquiera de los 2 casos el teléfono era el principal actor. Esto permitió que se aproveche al máximo todos los recursos adquiridos.

- Sin duda alguna el celular es una herramienta indispensable en la vida cotidiana de todas las personas, pues es difícil imaginar que un trabajador o un empresario no tengan un celular para realizar sus contacto o para ser localizado para los mismos; entonces darle un uso más, lo hace más eficiente.

- El mayor obstáculo en la realización de este proyecto fue el desarrollo de las aplicaciones ya que se requiere por lo menos un conocimiento básico de los lenguajes de programación para entender los comandos y las instrucciones que se utilizan para lograr la comunicación y la posterior recepción.

- La limitación durante el proyecto la hizo la herramienta de simulación del móvil, ya que necesitaba requerimientos tanto de hardware como de software, pues no permitía su uso en Windows Vista o solo tiene compatibilidad con dos tipos de lectores externos, es por eso que se realizó la elección del lector OMNIKEY uno de los 2 lectores compatibles y por eso se trabajó en una máquina virtual donde

se utiliza el sistema operativo Windows XP. Pero con esto se logró cumplir uno de los requisitos del proyecto que era la parte de simulación.

- Java es un lenguaje con un alcance muy alto y su orientación hacia el software libre hace que a más de ser una herramienta muy poderosa sea más difundida y que cada vez se desarrollen aplicaciones mediante su uso.

- Fue importante tener una base del comportamiento del sistema mediante las simulaciones ya que podíamos comprobar de una manera más fácil si había errores durante el desarrollo y poder remediarlos antes de su implementación. De igual manera nos daba una visión del comportamiento que podía esperarse en la realidad.

- Sin duda alguna que la adquisición de los principales equipos, el lector y el teléfono móvil, fue difícil y además costoso, pero esto puede cambiar a medida que se popularice la tecnología y que se logre una masificación en su producción.

- Una mejora que se puede realizar al sistema por ejemplo es no utilizar comunicación serial ya que los nuevos computadores no viene con un carcasa que contenga el tipo de conector DB-9 para comunicaciones seriales, especialmente las computadoras portátiles, por lo que se puede realizar la comunicación USB lo que haría que sea más rápida, pero se necesitaría un mayor conocimiento, manejo de protocolos USB.

5.2 RECOMENDACIONES

- Sin lugar a dudas el sistema implementado puede en algún momento provocar alguna falla como cualquier otro sistema electrónico, entonces es recomendable una revisión periódica para descartar errores que pudieran ocurrir.

- Dado que existen factores externos al sistema que pueden ocasionar un mal funcionamiento o peor aún que deje de funcionar, por ejemplo corte de energía eléctrica, es importante y se recomienda que se utilice una fuente alterna que inicie su funcionamiento cuando ocurre una suspensión de energía.

- Así mismo se recomienda que se conecte un regulador de corriente ya que los sobre voltajes pueden provocar que el PIC deje de funcionar o inclusive que ingrese a través del computador y apague o dañe al lector.

- Se recomienda también que el usuario tenga acceso a la conexión del lector o al circuito principal ya que si existiese una falla, simplemente se podría remediarla al resetear el PIC o volver a conectar el lector y no sería necesario llamar a una persona especialista que implementó el sistema.

- Se recomienda también que al momento de la implementación se utilice para la etapa de potencia otro tipo de elementos que brinden más seguridad a posibles sobrecargas que el acceso pueda generar hacia el circuito, por ejemplo el uso de triacs y optoacopladores que aíslan y protegen el circuito y así evitan que provoquen fallas en el sistema. Se utilizó un relé en la implementación del sistema únicamente para cumplir con el plan de proyecto.

GLOSARIO DE TÉRMINOS

APDU: Aplication Protocol Data Unit, es el nombre que se le da a las unidades de datos del Protocolo Aplicación.

Bluetooth: especificación industrial para Redes Inalámbricas de Área Personal (WPAN) que permite la transmisión de voz y datos entre diferentes dispositivos por medio de radiofrecuencia en la banda ISM de los 2,5 GHz.

CF (Chunk Flag): Bandera que indica si la trama pertenece a una cadena

ECMA: European Computers Manufacturers Association

GNU (General Public License): Licencia para la publicación de información.

IDE: Ambiente de Desarrollo Integrado

ISM: (Industrial, Scientific and Medical)

J2ME: Java 2 Micro Edition

L2CAP: por sus siglas Logical Link Control and Adaptation Protocol (Protocolo de Control y Adaptación del Enlace Lógico). Es un protocolo que tiene por objetivo comunicar y adaptar los protocolos superiores al protocolo de banda base.

LLCP: Protocolo de Control de Enlace Lógico

MIME: Por sus siglas Multipurpose Internet Mail Extensions (Extensiones de Correo de Internet de Propósitos Múltiples)

NDEF: por sus siglas en inglés NFC Data Exchange Format

NFC: siglas de Near Field Communication

NFCIP: Protocolo e Interfaz NFC.

PC/SC: Personal Computer/Smart Card, estándar para la comunicación entre tarjetas inteligentes y una computadora.

PDA: Personal Digital Assistant.

Piconet: Conjunto de dispositivos (máximo 8) dentro de la red Bluetooth.

RFID: es un sistema de almacenamiento y recuperación de datos remotos que usa dispositivos denominados etiquetas, tarjetas, transpondedores o tags RFID.

RTD: Por sus siglas en inglés Record Type Definition (Definición del Tipo de Registro)

Scatternet: Conjunto de Piconets en la Red Bluetooth.

SDK: Software Development Kit, es un conjunto de elementos para desarrollo de aplicaciones de software.

SMS: Son las siglas de Short Message Service o Servicio de Mensajes Cortos. Están destinados especialmente para teléfonos móviles.

SR (Short Record): Esta bandera se usa cuando un registro no es grande, se detalla más adelante en el formato del Registro NDEF en este capítulo.

StoLPaN: Store Logistics and Payment with NFC.

URI: Por sus siglas en inglés Uniform Resource Identifier (Identificador de Recurso Uniforme)

URL: Por sus siglas Uniform Resource Locator (Localizador de Recursos Uniforme)

URN: por sus siglas en inglés Uniform Resource Name (Nombre de Recurso Uniforme), son identificadores de recursos en la web.

VCC: Voltaje de Corriente Continua

WPAN: Wireless Personal Area Network.

XML: siglas en inglés *Extensible Markup Language* (Lenguaje de Marcas Extensible), un metalenguaje extensible de etiquetas que permite definir la gramática de lenguajes específicos para varias necesidades

ZigBee: especificación de un conjunto de protocolos de alto nivel de comunicación inalámbrica para su utilización con radios digitales de bajo consumo, basada en el estándar IEEE 802.15.4 de redes inalámbricas de área personal WPAN. Orientado más a su uso como sensores.

BIBLIOGRAFÍA

(1) http://www.terra.es/personal/ccossio/tecnologiaNFC.htm

(2) http://en.wikipedia.org/wiki/Near_Field_Communication

(3) http://www.nfc-forum.org/specs/spec_list/

(4) www.morelab.deusto.es/images/talks/NFC.ppt

(5) http://www.ecma-international.org/activities/Communications/2002tg19-010.pdf

(6) http://www.ecma-international.org/publications/files/ECMA-ST/Ecma-352.pdf

(7) www.nfc-forum.org/events/oulu_spotlight/Technical_Architecture.pdf

(8) http://muycomputer.com/FrontOffice/ZonaPractica/Especiales/especialDet/_wE9ERk2XxDA0vdjPfH3oxhGPTaF5ZlQt5tjimH6gLfyQcwsieDSF7cHlrr1APS5j

(9) http://www.idnoticias.com/2009/12/01/un-accesorio-convierte-al-iphone-en-un-dispositivo-nfc

(10) http://www.emtmalaga.es/portal/page/portal/EMT/Pago%20por%20m%C3%B3vil%20NFC

(11) http://en.wikipedia.org/wiki/Bluetooth

(12) ARIAS PILAQUINGA, Diego Bolívar: “Estudio comparativo entre las tecnologías Bluetooth y Wi-Fi en ambientes de corto alcance a través de la implementación de dos prototipos y de su simulación”, Tesis de Grado, Escuela Politécnica Nacional, Quito 2007.

(13) ACOSTA PONCE, María Catalina: “Estudio del estándar IEEE 80.15.4 "ZIGBEE" para comunicaciones inalámbricas de área personal de bajo consumo de energía y comparación con el estándar IEEE 802.15.1 "BLUETOOTH"”, Tesis de Grado, Escuela Politécnica Nacional, Quito 2006.

(14) PAREDES PAREDES, Martha Cecilia; PUGA PLACENCIA, Diego Fernando: “Diseño y construcción de un prototipo de red para el control de ingreso a sitios de acceso masivo utilizando la tecnología de identificación por radio frecuencia (RFID) “, Tesis de Grado, Escuela Politécnica Nacional, Quito 2007.

(15) GORDÓN DÍAZ, Nathaly Yessenia: “Control de acceso en la entrada del Instituto Geofísico utilizando tecnología RFID”, Tesis de Grado, Escuela Politécnica Nacional, Quito 2009.

(16) PUPIALES ANGAMARCA, Pablo Walter: “Diseño de un sistema de control de acceso utilizando la tecnología RFID para la empresa soluciones G4 del Ecuador Cia. Ltda.”, Tesis de Grado, Escuela Politécnica Nacional, Quito 2009.

(17) http://www.laflecha.net/canales/ciencia/articulos/fraude_con_rfid

(18) http://es.wikipedia.org/wiki/RFID

(19) http://es.wikipedia.org/wiki/ZigBee

(20) http://www.seccperu.org/files/ZigBee.pdf

(21) SINCHE Soraya: Apuntes de Comunicaciones Inalámbricas, Escuela Politécnica Nacional, 2008.

(22) http://java.sun.com/developer/technicalArticles/javame/nfc/

(23) http://jcp.org/en/jsr/detail?id=257

(24) http://msdn.microsoft.com/es-co/library/default.aspx

(25) http://www.pcscworkgroup.com/

(26) http://electronicapic.iespana.es/manual/PicRS232_vcpp_y_vb.pdf

(27) http://www.forum.nokia.com/Tools_Docs_and_Code/Tools/Platforms/Series_40_Platform_SDKs/

ANEXOS

ANEXO 1
ESTÁNDAR ISO/IEC 14443

ANEXO 2
ESTÁNDAR ISO/IEC 18092

ANEXO 3
VISIÓN GENERAL DE LA ESPECIFICACIÓN JSR-257

ANEXO 4
DATASHEET NOKIA 6212 CLASSIC

ANEXO 5
DATASHEET LECTOR OMNIKEY 5321

ANEXO 6
DATASHEET PIC 16F877A

ANEXO 7
DATASHEET MAX 232