

Boletín Asesoría Gerencial*

Diciembre 2007

Radio Frequency Identification (RFID)
Identificación por Radio Frecuencia

Introducción

Principales usos
de RFID

Tecnología
de RFID

Seguridad
en RFID

Conclusiones

Créditos



*connectedthinking

ESPIÑEIRA, SHELDON Y ASOCIADOS

Firma miembro de

PRICEWATERHOUSECOOPERS 



Introducción

Principales usos de RFID

Tecnología de RFID

Seguridad en RFID

Conclusiones

Créditos

Introducción

Ante el ambiente competitivo global que nos encontramos hoy en día las empresas requieren cada día más de soluciones efectivas y eficientes que les permitan llevar un control y seguimiento de distintos elementos como inventarios, productos y usuarios, que les permita una identificación única de forma sencilla y rápida.

Entre las principales soluciones utilizadas se encuentran los códigos de barras, tarjetas magnéticas y los sistemas de identificación por proximidad, cada una con sus limitaciones: Los códigos de barra tienen poca capacidad para almacenar datos, son fáciles de forjar y requieren proximidad física para leerlos, de igual forma sistemas de bandas magnéticas y proximidad son susceptibles a desgastes, clonación y alteración magnética y requieren que la tarjeta se encuentre muy cercana o en contacto para poder realizar la lectura.

Para superar estas limitaciones se ideó emplear chips que pudieran transmitir los datos sin contacto físico o aproximación, lo cual incrementa la capacidad productiva e incorporar medidas de seguridad para prevenir su alteración o

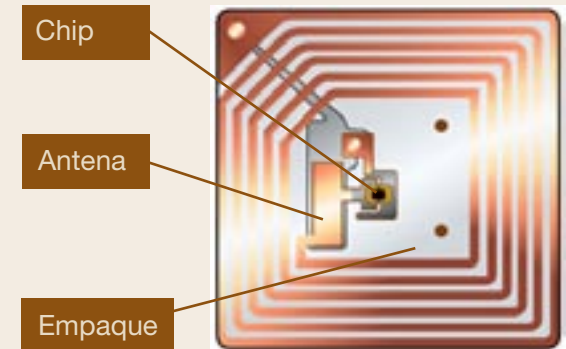
duplicación. En este sentido, el uso de radio frecuencias provee al mercado la posibilidad de diversificar su capacidad para integrar tecnologías y optimizar los procesos internos.

Identificación por Radio Frecuencia o RFID (por sus siglas en Inglés), es la tecnología de reconocimiento mediante de la cual datos digitales se codifican en una etiqueta de RFID o “smart label” (Chip) y que luego pueden ser capturados por un lector que utiliza ondas de radio. Una de las ventajas del uso de radiofrecuencia es que no se requiere visión directa entre emisor y receptor.

Una etiqueta RFID es un dispositivo pequeño (ver Figura 1), que puede ser adherido o incorporado a un producto. Contiene antenas para permitirles recibir y responder a peticiones por radiofrecuencia desde un transmisor RFID. Existen dos tipos de tecnologías: las etiquetas pasivas que no necesitan alimentación eléctrica interna y las activas que sí lo requieren.

El receptor de RFID consta, usualmente, de tres partes:

- 1.- Chip: almacena información acerca del objeto físico al cual está adherido.
- 2.- Antena: Transmite información a un lector (por ejemplo, un scanner de mano) a través de radio frecuencias.
- 3.- Empaque: Reune el chip y la antena y permite que sean adheridos al objeto físico.



Para ampliar, haga click en la imagen

Figura 1. Diagrama de un receptor de RFID



Principales usos del RFID

La tecnología ha encontrado usos en distintas aplicaciones, para diferentes sectores del mercado, sin embargo, ha sido quizás el sector de Retail, el que ha impulsado el mayor de la misma.

A continuación se listan algunos de los principales usos:

- Gestión de inventarios
- Gestión de logística y transporte
- Control de acceso
- Transporte público
- Pasaportes
- Información de los consumidores
- Control de pacientes

Tecnología de RFID

El esquema de funcionamiento de la tecnología está compuesto por tres elementos: Etiqueta RFID, Lector RFID y el Subsistema de Procesamiento de Datos.

Etiqueta RFID o Tag. Este componente de la tecnología en su descripción básica está compuesto por una antena y el chip contenedor de los datos.

Las etiquetas RFID de “Sólo Lectura” o “Lectura y Escritura” pueden ser de varios tipos:

- **Pasivas.** Estas no poseen fuente de alimentación eléctrica y la información puede llegar a ser extraída con una mínima corriente que sea inducida a través de la antena, la cual provee de la suficiente energía para que el chip transmita una respuesta. Este tipo de etiquetas puede no contener gran cantidad de información por lo cual su uso se destina a elementos en serie de producción masiva.
- **Semi Pasivas.** Poseen una micro batería lo cual reduce la complejidad de diseño de la antena trasmisora y mejora la respuesta a consultas.

- **Activas.** Funcionan bajo la conexión a una fuente de energía de larga duración, lo cual les permite tener rangos de lectura y mayor capacidad de almacenamiento de datos y procesamiento.

Lector RFID. Compuesto por una antena, un transceptor y un decodificador, el cual recibe del entorno la respuesta a sus peticiones transmitiéndolas posteriormente al Sub-Sistema de datos.

Almacenamiento de Datos

La implementación de RFID requiere que el fabricante defina a través del organismo internacional EpcGlobal características únicas que identifique al producto creado. Estas características son resumidas en un Código Electrónico de Producto, EPC (por sus siglas en Ingles), el cual identifica a un artículo.

Actualmente, el EPC de 96 bits es la versión predominante y contiene información acerca del fabricante, el tipo de objeto y un número de serie





Introducción	Principales usos de RFID	Tecnología de RFID	Seguridad en RFID	Conclusiones	Créditos
--------------	--------------------------	--------------------	-------------------	--------------	----------

Tecnología de RFID (cont.)

específico que relaciona al objeto y el como debe ser tratado, sin embargo dependiendo del requerimiento existen de hasta 1024 bits conservando el mismo aspecto en cuanto al tamaño promedio. Las bondades de implementar este tipo de codificación permiten no sólo gestionar la cadena de distribución de forma local sino también de manera global dado que muchos productos están involucrados con la importación, pasando por muelles internacionales donde un estándar debe ser necesario.

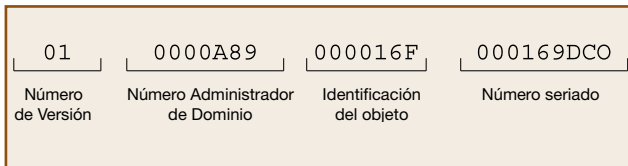


Figura 2. Estructura EPC (Código Electrónico de Producto)

Fuente: <http://www.rapidradio.co.in/rfid.html>



Producto, Lectura de Tags, Métodos Anticolisión y Regulaciones ante la exposición Humana. ISO resume su aporte bajo el estándar 18000, mientras que EpcGlobal muestra un esquema estructurado llamado “Architecture Framework”, el cual se divide en tres áreas: Intercambio, Captura e Identificación (Exchange, Capture, Identify).

Cada organización ha desarrollado las especificaciones para la Frecuencia Alta de 13.56 MHz y para la Frecuencia Ultra alta entre 860 MHz y 930 MHz, ambas compiten por establecer un modelo eficiente y rentable para productores y empresas consumidoras de la tecnología, sin embargo EpcGlobal logró establecer como estándar intermedio al concepto “Gen2” el cual puede interoperar con los estándares ISO.

Ultra alta (UHF: 868 - 928 MHz) es regulada por los diferentes organismos que designe cada nación con al apoyo y dirección de EpcGlobal.

Para el caso Venezuela, La Comisión Nacional para las Telecomunicaciones CONATEL es el organismo encargado de normar el uso seguro de esta frecuencia. El rango bajo el cual particulares, Estado y empresas pueden operar con sistemas de Frecuencia Ultra alta está en la banda 922-928 MHz, sin embargo, sus definiciones técnicas con respecto a la potencia máxima y mínima, así como las técnicas de lectura, no han sido publicados a la fecha de redacción este Boletín.

Estándares y entes regulatorios

Existen dos organizaciones destinadas a normar el uso de las diferentes frecuencias donde la tecnología RFID puede funcionar. ISO y EpcGlobal definen actualmente los estándares para fabricantes de Chips y lectores. Estas especificaciones incluyen aspectos relativos al uso de la Interfaz Aérea, Código Electrónico del

Transmisión de Datos

La transmisión de datos en esta tecnología emplea diferentes frecuencias dependiendo del sector o uso que se pretenda, en tal sentido, los sistemas de Baja Frecuencia deberían operar entre 125 - 134 kHz y 140 - 148.5 kHz. Los sistemas de Alta Frecuencia están situados en 13.56 MHz. Ambos pueden utilizarse de forma global sin necesidad de licencia. La Frecuencia





Introducción

Principales usos
de RFID

Tecnología
de RFID

Seguridad
en RFID

Conclusiones

Créditos

Seguridad en RFID

Amenazas relacionadas con RFID

La tecnología RFID, como toda tecnología basada en el uso de radio frecuencia esta expuesta a un conjunto de amenazas como las siguientes:

- **Espiar (Eavesdropping):** Debido a su naturaleza, las ondas de radio pueden ser interceptadas por cualquier persona que se encuentre dentro del rango de transmisión, permitiéndole escuchar información que pudiese ser confidencial. Para el caso RFC, en términos generales un atacante debe estar a una distancia aproximada de diez (10) metros para un dispositivo activo y a un (1) metro en caso de un dispositivo pasivo.
- **Corrupción de datos:** Este tipo de ataque se caracteriza por cuando el atacante solo esta en interesado en “dañar” los datos enviados por el dispositivo, lo cual se puede lograr enviando señales por los rangos de frecuencia validos en el momento correcto.
- **Modificación de datos:** Un atacante puede estar interesado en alterar o insertar datos adicionales en la comunicación entre el dispositivo y el lector, lo cual se pueda lograr enviando señales dentro del espectro antes de la comunicación (inserción), o durante (Modificación) para buscar alterar los valores recibidos por el lector.

- Adicionalmente, a nivel de control de inventarios existe el riesgo asociado con la duplicación de los identificadores EPC en un producto particular, para facilitar su robo.

Privacidad

Un tema adicional relacionado con la seguridad que ha generado polémica en torno a RFID es el tema de la “privacidad”. La tendencia mundial ha logrado establecer patrones únicos de identificación para muchos productos, un ejemplo de esto es el EPC, el cual en muchos casos permanece en la etiqueta y del producto o tarjetas de identificación. Imaginar el caso de una persona que se encuentra en un centro comercial y sin su consentimiento esta siendo escaneado con lectores RFID de mediano alcance. El atacante podrá obtener con mucha facilidad el patrón de compras lo cual podría ser usado como un nuevo método para la investigación de mercado o realizar espionaje industrial. De igual forma, la persona podría ser víctima de un atraco si sus compras generan algún tipo de interés en el delincuente.

Adicionalmente la inclusión de tecnología RFID en pasaportes y tarjetas de crédito, ha incrementado en la población los riesgos asociados a la privacidad de su información.

En marzo de 2007, Adam Laurie experto en seguridad informática, logró descifrar la información contenida en un pasaporte auténtico emitido por el gobierno Británico. La experiencia duró alrededor de 4 horas y en líneas generales las debilidades que permitieron romper el esquema de seguridad no eran imputables a la tecnología sino al método de cifrado de la información. Es por ello que los expertos sostienen que no se debería incorporar esta tecnología en la emisión de este tipo de documentos hasta establecer mecanismos robustos de protección, puesto que pueden ser leídos cuantas veces sea posible de manera inalámbrica sin que su portador lo sepa, facilitando su falsificación.

El mercado de tarjetas de crédito también ha incurrido en fallas en la adopción de RFID, como consecuencia de la forma en que establecieron los estándares. Según estudios independientes, parte de las tarjetas emitidas durante el año 2006 y 2007 en Estados Unidos y Europa, transmiten el nombre del propietario, el número de la tarjeta de crédito y su fecha de caducidad pero no el código de seguridad de tres dígitos, a cualquiera que se encuentre en las proximidades con un detector de RFID. Esto ha generado objeciones e inconvenientes para la industria, la cual ha comentado que durante una transacción, los

[Introducción](#)[Principales usos de RFID](#)[Tecnología de RFID](#)[Seguridad en RFID](#)[Conclusiones](#)[Créditos](#)

Seguridad en RFID (cont.)

lectores del comercio usasen un código de seguridad cifrado y dinámico que hace a la transacción única en ese momento, por lo cual se disminuye altamente las posibilidades de fraude; sin embargo, esto no evita que cualquiera pueda extraer el nombre y el número de una tarjeta usando la información posteriormente para clonar la tarjeta.

Soluciones

En contramedida a todas estas vulnerabilidades, se han diseñado productos que eliminan la exposición de los datos personales que contienen estos documentos, a través del control de la entrada o salida de señales de radiofrecuencia basado en el fenómeno “Faraday” de cancelación electromagnética.

Existen propuestas para la utilización de un esquema de “autorización” para la lectura de las etiquetas RFID pertenecientes a un usuario, utilizando por ejemplo dispositivos electrónicos como el celular o PDA, donde llegase un mensaje cada vez que un lector tratase de acceder a la información de algún dispositivo, requiriendo la autorización del usuario antes de poder enviar la información.

En relación con el tema de la clonación existen propuestas para la autenticación de los productos, que permitan detectar cualquier intento de clonación, ya sea a través del control histórico del producto, (Ej. El mismo producto no puede estar en dos lugares al mismo tiempo, o no puede estar en el almacén si su estatus es despachado), o través de características de seguridad propuestas por cada fabricante.

Conclusiones

La tecnología RFID aporta innumerables ventajas para los usuarios y las empresas, proveyendo un mecanismo eficiente y cómodo para el control y logística. Sin embargo, para el momento los riesgos relacionados con la privacidad de la información, constituyen el mayor punto de atención hasta que no se desarrolle un estándar común que permita el control de acceso a la misma.

Fuentes

- “RFID and Security”. Sanjay Sarma. MIT Institute
- “Building RFID Application with Security and Privacy”. Kevin Fu
- “From Identification to Authentication – A Review of RFID Product Authentication Techniques”. Mikko Lehtonen, Thorsten Staake, Florian Michahelles, and Elgar Fleisch.
- “Privacy, Data Protection Law, and RFID. Irreconcilable Differences?”. Marc Langheinrich.
- “Security in Near Field Communication (NFC)”. Ernst Haselsteiner and Klemens Breitfuß.

[Introducción](#)[Principales usos
de RFID](#)[Tecnología
de RFID](#)[Seguridad
en RFID](#)[Conclusiones](#)[Créditos](#)

Boletín Asesoría Gerencial

El Boletín Asesoría Gerencial es publicado mensualmente por la Línea de Servicios de Asesoría Gerencial (Advisory) de Espiñeira, Sheldon y Asociados, Firma miembro de PricewaterhouseCoopers.

El presente boletín es de carácter informativo y no expresa opinión de la Firma. Si bien se han tomado todas las precauciones del caso en la preparación de este material, Espiñeira, Sheldon y Asociados no asume ninguna responsabilidad por errores u omisiones; tampoco asume ninguna responsabilidad por daños y perjuicios resultantes del uso de la información contenida en el presente documento. *connectedthinking es una marca registrada de PricewaterhouseCoopers. Todas las otras marcas mencionadas son propiedad de sus respectivos dueños. PricewaterhouseCoopers niega cualquier derecho sobre estas marcas

Editado por Espiñeira, Sheldon y Asociados
Depósito Legal pp 1999-03CS141
Teléfono master: (58-212) 700 6666

Si está interesado en recibir en su correo electrónico este Boletín, por favor envíenos su dirección de e-mail a:
advisory.venezuela@ve.pwc.com



© 2007. Espiñeira, Sheldon y Asociados. Todos los derechos reservados. "PricewaterhouseCoopers" se refiere a la firma venezolana Espiñeira, Sheldon y Asociados, o según el contexto, a la red de firmas miembro de PricewaterhouseCoopers International Limited, cada una de las cuales es una entidad legal separada e independiente. RIF: J-00029997-3