Control de Accesos
Elementos de Identificación

Ing. Luis Cosentino
Consultor Independiente
lcosentino@fibertel.com.ar

Diseñada como una ayuda para técnicos, instaladores y estudiantes, ofrecemos a nuestros lectores una serie de conceptos y fundamentos sobre el control de accesos, sus elementos y funciones. Un detallado estudio de mercado y un ejemplo de diseño son los complementos de esta obra que seguramente será de suma utilidad para nuestros lectores.

Indice

Resumen
En el número anterior *(Elementos de identificación, Cap. V, 1ra. Parte; RNDS nº46)*, comenzamos a describir los diferentes métodos para identificar a una persona. En esa oportunidad se ofreció la descripción de los teclados PIN y las tarjetas de código de barras, de banda magnética y de efecto Wiegand. Estas tecnologías, si bien todavía existen en el mercado, ya fueron reemplazadas por la de Proximidad y las Smartcards, que serán tratadas en el presente capítulo.

5.2.2.4. Tecnología de Proximidad.

Las tarjetas de proximidad se introdujeron popularmente en el mercado en la década del '90, época en la que el mercado de control de accesos era dominado por las tecnologías de tarjetas magnéticas y de efecto Wiegand. Con buen criterio, los fabricantes de proximidad, *HID Corp® y Motorola Indala®*, lanzaron sus productos de proximidad haciendo que los protocolos de comunicación de las lectoras de proximidad con los paneles de control de acceso *"emularan"* los protocolos de comunicación de las lectoras de banda magnética o de efecto Wiegand. De esta manera solo había que reemplazar las lectoras y tarjetas de un sistema existente sin necesidad de reemplazar el sistema completo. Esta estrategia favoreció enormemente la velocidad de introducción de la tecnología.

5.2.2.4.1. Principio de funcionamiento. Lectores y tarjetas como dispositivos periféricos de controles de accesos

La tecnología de proximidad parte de la base de tener una tarjeta pasiva, es decir un dispositivo que no posee batería ni alimentación propia, que es alimentado en forma externa. Una vez que recibe una carga deter-

Continúa en página 168

Viene de página 164

minada, transmite el número grabado en el chip. Para eso las tarjetas de proximidad tienen solamente una bobina y un chip.

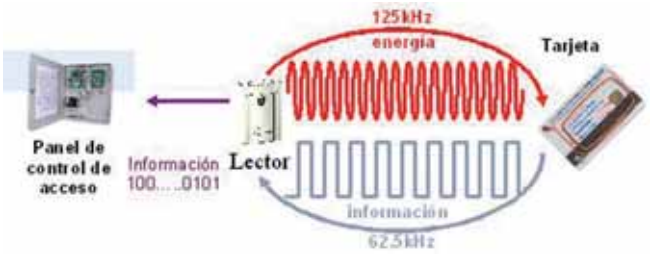
Analizando el esquema que se ofrece más abajo, podemos decir que la secuencia de la lectura de la información del chip de una tarjeta de proximidad es la siguiente:

a- La lectora genera un campo electromagnético que le entrega energía (imagen en rojo).

b- La tarjeta es colocada a la distancia adecuada para que reciba, por lo menos, la cantidad mínima necesaria de carga.

c- Una vez alcanzado este umbral de energía comienza a transmitir la información que tiene programada en su chip (imagen en gris)

d- El lector decodifica el mensaje recibido de la tarjeta y de acuerdo a su configuración transmite el código recibido de la tarjeta al panel del control de accesos.



Gracias a este principio de comunicación por radiofrecuencia, las tarjetas de proximidad funcionan sin que exista contacto entre éstas y el lector y la separación puede ser de hasta un par de metros. Esta característica novedosa hace que los lectores no necesiten mantenimiento, eliminando así los frecuentes problemas de desgaste que había con las tarjetas y lectores de banda magnética. Otra ventaja de no tener contacto es que las tarjetas tienen una increíble durabilidad y debido a esto los fabricantes líderes del mercado las garantizan de por vida.

Como ventaja adicional podemos citar que como la tarjeta no debe "*pasarse*" por ninguna ranura, de ancho determinado o posición específica, pueden tener varios factores de forma. Existen tarjetas de diferentes espesores, llaveros o etiquetas autoadhesivas (tags), las que en general tienen el mismo chip pero diferentes rangos de lectura según sea su área de bobina.



Las que poseen dimensiones de tarjeta normalizada vienen en dos variedades de tamaño: las más robustas y que no pueden imprimirse directamente llamadas "clam shell", que sólo respetan las dimensiones de ancho y largo de una tarjeta de crédito, y las más "elegantes", que admiten impresión en forma directa y respetan las tres dimensiones de las tarjetas de crédito (CR80), denominadas comúnmente "ISO".

Como ejemplo podemos decir que en una empresa es perfectamente posible entregar tarjetas de tipo ISO a los empleados administrativos, tarjetas de tipo *clam shell* a los que desempeñan tareas más rudas y llaveros o *tags* a los dueños, todos ellos programados con el mismo formato y numeración correlativa.

Dado que la comunicación es por radio frecuencia, siempre que no exista un blindaje metálico, es posible interponer entre el lector y la tarjeta cualquier material no magnético. Esto ofrece una insuperable capacidad de resistencia al vandalismo. Como ejemplo: un lector con un rango de 20 centímetros puede ser colocado detrás de la pared exterior de 15 centímetros de espesor y todavía tener otros 5 centímetros de rango de lectura. Si la pared fuese de 30 centímetros, se la podría colocar dentro de la misma pared y hasta rellenar con concreto para dejar el mismo aspecto anterior.

La tecnología de proximidad no tiene ningún inconveniente para funcionar en ambientes con polvos o agentes químicos (mientras no ataquen al plástico), detrás de vidrios, paredes, etc.

Inherentemente las bobinas irradian campo electromagnético en ambos direcciones, por lo que los lectores proximidad son capaces de leer, casi con la misma efectividad, hacia delante como hacia atrás del eje de la bobina. A pesar de ello y en esta situación, no son capaces de reconocer si la tarjeta está ubicada delante o detrás del mismo, por lo que no podrá utilizarse la misma lectora para saber si alguien está abriendo la puerta desde adentro o desde afuera.

En algunos casos, que la lectora pueda ser utilizada por ambos lados es una ventaja, pero si es necesario identificar desde dónde se quiere acceder, el colocar dos lectoras a ambos lados de la misma pared puede provocar inconvenientes.

Bajo todo concepto se deberá evitar instalar las lectoras "espalda con espalda", aunque exista una pared de por medio, a menos que se respete la regla de separarlas más de 5 veces el rango. Por ejemplo, para poder colocar 2 lectoras de 10 centímetros de rango espalda con espalda, deberá dejarse una separación entre ellas de 50 centímetros. En el caso de no respetar estas indicaciones, podrán producirse interferencias en las lecturas de ambas lectoras. Es decir, al presentar una tarjeta frente a la lectora de un lado de la pared, dicha lectura se produce en la del otro lado también.

A las frecuencias utilizadas de 125KHz se acepta que el campo que genera un lector de un metro de rango de lectura es inofensivo para una persona que está expuesta permanentemente a dicha radiación, incluso en el caso de mujeres embarazadas. Los fabricantes de lectores de largo alcance poseen los certificados pertinentes a disposición de los clientes.

Si bien la tecnología de proximidad permite que la información almacenada en el chip pueda ser leída y grabada muchas veces, la baja frecuencia de la portadora que se utiliza (125 KHz) hace que no sea práctico utilizar esta tecnología ya que una transacción completa demora un par de segundos y si durante ese período la tarjeta es quitada del campo, no se podrá garantizar exactamente el contenido de la información del chip. Por eso, si bien la mayoría de las tarjetas son de lectura y escritura, en realidad se utiliza la característica de escritura para la programación inicial y luego se las utiliza como lectura solamente. De hecho los chips poseen un bit denominado "bit de seguridad" que hace las veces de un fusible, de forma tal que una vez programada la información deseada se puede "quemar" este bit para que la información grabada dentro de él quede inalterable.

Si bien las marcas líderes del mercado de proximidad *(como HID, Indala, FarPoint Inc, AWID, Rosslare y Texas Instruments)* tienen productos en la banda de 125 Khz a 132 Khz, no todos son compatibles entre sí debido a que utilizan diferentes técnicas de modulación.

Por ejemplo, no es posible leer una tarjeta *Indala* en una lectora *HID o AWID y viceversa*. Si bien es cierto que últimamente los fabricantes están agregando a sus líneas de productos lectores que permiten leer tarjetas de 125KHz de múltiples fabricantes, nunca se alcanzará una solución definitiva dado que no existen normas que regulen las comunicaciones entre la tarjeta y el lector. Este inconveniente se resuelve con las *Smartcards*, tecnología para la que casi todo el funcionamiento está regulado por normas.

intuitivamente se puede entender que un lector que genera un campo electromagnético más intenso será capaz de leer una tarjeta a una distancia mayor. Y que una tarjeta que tenga un área de bobina mayor será leída a una mayor distancia que una de menores dimensiones.

Los fabricantes de lectores de proximidad ofrecen diferentes rangos de lecturas, generalmente concentrados en tres categorías:

a- Los de bajo rango (8 a 12cms): Se utilizan en la mayoría de las

Continúa en página 172

Viene de página 168

aplicaciones de puertas y molinetes. Se los suele ofrecer para ser ubicados en cajas de luz de 10x5 cms (Wall Switch) o para marcos de puertas (Slim).

b- Los de rango medio (25 a 30 cms): Se utilizan para aplicaciones en las que se pretende leer las tarjetas y tags sin tener que sacarlas de las carteras o maletines, típicamente en aplicaciones domiciliarias o en estacionamientos de bajo costo.

c- Los de largo alcance (más de 50 cms): Se utilizan generalmente para estacionamientos.

Como ejercicio práctico podríamos plantearnos los siguientes interrogantes:

1- ¿Cuál es el lector adecuado para la puerta de ingreso exterior de una empresa?

El análisis se puede hacer desde varios ángulos: por ser un lector de exterior, debe ser a prueba de vandalismos e intemperie y por tratarse del ingreso a una empresa no es necesario buscar un rango de lectura mayor a 10 centímetros, dado que probablemente el empleado una vez que abrió la puerta deba portarla en un lugar visible.

Desde el punto de vista estético no debe seleccionarse una lectora muy llamativa para evitar los actos de vandalismos.

Con estás consideraciones llegamos a una lectora de 10 centímetros de rango, que debe estar inyectada en resina epoxi para soportar adecuadamente la intemperie y tener "tapa" para que en caso de sufrir daños sólo sea necesario reemplazar la tapa. Prácticamente todos los fabricantes de lectores los ofrecen con estas características, a excepción de los muy económicos.

2- ¿Cuál es el lector adecuado para la puerta de ingreso exterior de una casa o edificio de viviendas?

En este caso las consideraciones son similares con la sola excepción de que muchas veces sus habitantes pretenderán ganar el acceso con las manos ocupadas con paquetes y/o bolsas. Por lo tanto, una lectora de rango de lectura medio (30 centímetros) permitirá un acceso más cómodo, sobre todo si la lectora se coloca por debajo de la altura de la cintura de manera de facilitar la aproximación de carteras, maletines, mochilas, etc.

3- ¿Cuál es el lector adecuado para un molinete?

Los molinetes generalmente poseen dos lectoras y eventualmente una más para el buzón recolector. Si este es el caso y debido a que generalmente son metálicos, es conveniente utilizar lectores de bajo rango de lectura (<5 cms) para evitar la interacción de las lectores y minimizar las lecturas cruzadas eventuales.

4- ¿Cuál debería ser la lectora adecuada para un acceso vehicular?

Se cree que lo importante de una lectora que debe ser accedida desde el interior de un vehículo es la distancia de lectura. Sin embargo debe tenerse en cuenta otro factor: el "ancho" de la misma. Si la lectora es muy angosta el vehículo debe estacionarse justo frente de la lectora, no teniendo tolerancia hacia adelante o hacia atrás. Es por esto que las lectoras de largo alcance también son las de mayor área de bobina.

Comúnmente en este tipo de lectoras se observan dos inconvenientes que suelen disminuir el rango de lectura: uno es de montaje, dado que nunca se las debe montar sobre metal; y el otro está relacionado con la alimentación de 24 voltios, donde frecuentemente se cometen errores en las conexiones de tierra.

Si por algún motivo se decide no utilizar lectoras de largo alcance para los estacionamientos, debe utilizarse una lectora de rango medio antes que una de rango corto, ya que su mayor superficie facilita notablemente el uso.

5.2.2.4.2. Lectores de tarjetas proximidad como dispositivos autónomos de controles de accesos

La mayoría de los equipos autónomos para control de accesos actuales están basados en tecnología de proximidad y, fundamentalmente, en el principio de que las tarjetas poseen numeración diferente, por lo que se los vende con una capacidad limitada de base de datos de tarjetas y se prevé un procedimiento por el cual pueden darse altas, bajas y modificaciones (ABM) en esta base de datos, de manera simple, *in situ* y casi por cualquier persona. Entre los métodos más comunes de ABM podemos citar los que poseen un teclado incorporado o conectable, mediante la conexión del teclado de un teléfono o, el método más popular, que utiliza tarjetas maestras. De esta forma es posible modificar la base de datos de tarjetas en el sitio, de manera muy simple y sin necesidad de equipos adicionales.

Generalmente estos equipos tienen capacidad para una puerta con lector de entrada y pulsador de salida o de dos lectoras, una para la entrada y otra para la salida (o dos puertas independientes), por lo que en caso de tener varios colocados en un edificio o empresa pequeña, cuando desee darse de alta o baja una tarjeta, será necesario repetir el proceso en todos los controladores.

En términos generales pueden encontrarse dos tipos de equipos autónomos, los más básicos y económicos - son un simple «pasa no pasa» que poseen el lector incorporado- y los que incorporan prestaciones de equipos más grandes, como bandas horarias y feriados, almacenamiento de eventos, antipassback, funciones de control básicas, conexiones en red, etc. y que admiten lectores externos.

Estos equipos autónomos "medianos" son muy utilizados en nuestro mercado porque están destinados a clientes pequeños y medianos, de manera de permitirles controlar pocas puertas e ir creciendo a medida de las necesidades. El límite de este perfil de clientes es unas 10 a 20 puertas.

Suelen ser la opción ideal para los instaladores, porque pueden comenzar instalando equipos autónomos dando las altas y bajas con tarjetas de programación y, a medida que la aplicación evoluciona, se agregan más equipos conectándolos entre ellos hasta formar una red limitada de controladores manejada por PC's.

Es muy difícil recomendar equipos, pero sí pueden fijarse algunos parámetros:

1- Deben cumplir un nivel de seguridad mínimo: los equipos autónomos de muy bajo precio están contenidos en una sola pieza, la que debe ser colocada en el exterior porque incluye el lector de proximidad. Estos equipos permiten ser desarmados con mucha facilidad de manera de poder acceder al contacto de cerradura muy simplemente desde el exterior. Ciertamente estos equipos están diseñados para ser utilizados donde se necesite comodidad pero no seguridad.

2- Es conveniente que sean productos adaptados al mercado nacional: todavía hay instalaciones o regiones de nuestro país donde las características de la alimentación no son todo lo estables que algunos equipos importados requieren o, a diferencia de los equipos nacionales, algunos importados tienen prestaciones que no se utilizan en nuestro ambiente.

3- Estos equipos suelen ser el punto de entrada de los instaladores al mundo del control de accesos y es por eso que se recomienda el uso de equipos protegidos eléctricamente contra conexiones equivocadas y con soporte local real.

5.2.2.5. Smartcards

Las Smartcards pueden ser consideradas como la "nueva tecnología" de tarjetas para el control de accesos. Son tarjetas pasivas que cumplen dos condiciones: la posibilidad de almacenar información en forma dinámica y proteger dicha información en condiciones de extrema seguridad.

Continúa en página 176

Viene de página 172

Fueron creadas originalmente para poder ser utilizadas como dinero digital y documentación electrónica, pero con la baja de costos se convirtieron en la opción para reemplazar a la tecnología de proximidad.

Desde el punto de vista del usuario se comportan como tarjetas de proximidad pero desde el punto de vista tecnológico y de seguridad es muy diferente. Además, poseen la característica de almacenar simultáneamente varias aplicaciones, por lo que se puede utilizar la misma tarjeta de control de accesos para comprar café de una expendedora, sacar fotocopias de manera controlada, cargar combustible, etc.

Si bien existen varios tipos de Smarcards (de contacto, sin contacto, microprocesadas, con coprocesadores criptográficos, etc.) describiremos las más utilizadas para el control de acceso: las smartcards sin contacto de memoria sectorizada con llaves o contraseñas. En este grupo las más populares son la Mifare e iCLASS.

Por ejemplo, una tarjeta Mifare de 1Kbyte está organizada como 16 bloques de memoria, 15 de los cuales solo pueden ser "abiertos" conociendo las "contraseñas" que funcionan como llaves y solo uno, denominado MAD (Mifare Address Directory), es de acceso público, es decir que puede leerse sin ninguna clave especial.

Para acceder a la información guardada dentro de uno de los sectores de datos es imprescindible conocer las contraseñas correctas, las cuales son diferentes por cada bloque y según el modelo de chip es necesaria una llave para leer la información y otra para poder modificarla.

Dentro de ese sector público se almacena un número único asignado por el fabricante a cada tarjeta, que en algunos casos será el utilizado por los controles de accesos para identificar las tarjetas entre sí. Este número identificatorio se lo llama "Card Serial Number (CSN)".

Esquema lógico básico de una Smartcard.

Esta necesidad de "contraseñas" para conocer la información almacenada es la gran ventaja de las Smartcards ante el resto de las tecnologías de tarjetas, ya que las hace no clonables, transformándolas y en elementos de gran seguridad.

Solamente con el espíritu de demostrar la complejidad matemática necesaria para abrir un bloque con las llaves correctas, es que se describe a continuación la secuencia denominada "autenticación". Al compararla con la simpleza que utiliza la tecnología de proximidad para acceder a la información almacenada, podrá tenerse una idea del aumento de seguridad.

Autenticar un bloque de una tarjeta es un proceso por el cual el lector y la tarjeta verifican que ambos conocen la misma clave y por lo tanto son parte de la misma aplicación. Este ejemplo se toma de las tarjetas iCLASS (ISO14443B), que a diferencia de las Mifare (ISO14443A) manejan el concepto de llaves diversificadas.

Un sistema que posee las llaves diversificadas colocará una contraseña diferente en cada tarjeta, que se calcula con un algoritmo de Hash a partir de una información denominada "código semilla" y del CSN, que es diferente para cada tarjeta.

En otras palabras, la "contraseña" del mismo bloque en diferentes tarjetas será diferente porque los CSN de cada tarjeta son diferentes. Sin embargo ambas tarjetas deberán ser autenticadas por el lector para poder ser parte de la misma aplicación.

En forma muy simplificada podemos decir que los algoritmos de Hash son funciones matemáticas que no poseen función inversa por lo que no es posible calcular uno de los miembros por más que se conozca el otro y el resultado.

Siguiendo el esquema de abajo podemos decir que el proceso de autenticación requiere de los siguientes pasos:

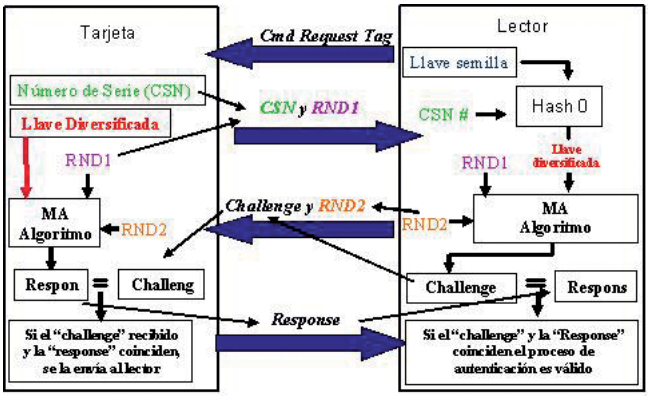
1- La tarjeta es colocada en el campo del lector y a diferencia de proximidad, donde el lector sólo transmite la portadora, aquí el lector modula un comando denominado *Command Request Tag*, perfectamente especificado por la norma.

2- Cuando la tarjeta lo reconoce genera un número aleatorio, que llamaremos *RND1*, y le contesta al lector enviando ese número de su CSN, que como dijimos es público.

3- El lector recibe la información enviada por la tarjeta y utiliza el CSN más la "llave semilla" para calcular una llave diversificada, la que debería coincidir con la que tiene la tarjeta en el caso en que ambas hayan sido calculadas con la misma semilla y el mismo algoritmo de Hash.
Luego genera otro número aleatorio, que llamaremos *RND2*, y con éste la llave diversificada que acaba de calcular y el *RND1* calcula un número al que denominaremos "*challenge*", es decir "desafío". A continuación transmite a la tarjeta ese desafío conjuntamente con el *RND2*.

4- La tarjeta recibe la información del lector y calcula el resultado de la autenticación mutua, utilizando el *RND1*, *RND2* y la llave diversificada del bloque en cuestión, cuyo resultado llamaremos "respuesta", y se la transmite al lector. A continuación compara el desafío recibido con la respuesta calculada y si le dan iguales, la tarjeta queda autenticada. Por lo tanto, hasta tanto no se la retire del campo o se la cierre mediante otro comando, le permitirá al lector acceder a la información de ese bloque.

5- Por último, el lector hace la comparación de la respuesta recibida con el desafío calculado y si le da correcto, sabe que la tarjeta está autenticada.



Se puede notar que nunca una llave "viaja por el aire", lo que hace a este mecanismo extremadamente seguro. Otra cosa notable es que cada vez que se aproxime la tarjeta, todos los números que se transmiten son diferentes a excepción del CSN (público), lo que complica aún más el jaqueo de la seguridad.

Si bien a simple vista parecería que este proceso es lento y que la tarjeta debe dejarse frente al lector por mucho tiempo, la mayor frecuencia de portadora utilizada por las normas ISO14443 A y B y la ISO15693 (de 13,56 Mhz), hace que todo este proceso demore lo mismo que lo que demora una tarjeta de proximidad tradicional de 125 KHz en leer el número almacenado en el chip.

Otra ventaja de las smartcards es que cumplen con normas internacionales y por lo tanto, es posible tener varios oferentes de tarjetas, lectores y aplicaciones que compitan entre sí, permitiéndole al usuario final una enorme variedad de combinaciones.

Con las smartcards aparece la figura de terceras partes que desarrollan aplicaciones que pueden colocarse dentro de las tarjetas. Ahora es posible tener aplicaciones como control de almuerzos en la

Continúa en página 180

Viene de página 176

cantina de una fábrica, control de turnos en una cancha de tenis, limitación de fotocopias a efectuar por mes, manejo de máquinas de gaseosas o café, etc.

5.2.2.5.1. Mifare

Es un chip desarrollado por Philips Semiconductors (hoy llamado NXP), popularizado en los '90, orientado al pago electrónico del transporte público. Si bien se desarrollaron varios miembros de la familia, con diferente capacidad y prestaciones, se sigue fabricando en altos volúmenes debido a la popularidad de su aplicación fundamental. A diferencia del mercado de proximidad tradicional, NXP vende los chips a los fabricantes de tarjetas para que éstos vendan las tarjetas, generando una sensación de competencia en el mercado que termina por bajar los precios.

Con los lectores pasa algo similar ya que NXP no los fabrica directamente sino que existen varios fabricantes en el mercado, generalmente diferentes a los que fabrican tarjetas. El inconveniente está en que estos fabricantes están orientados al mercado de transporte o pago electrónico y sus productos son módulos semiterminados, no necesariamente de forma "potteada", de montaje fácil en marcos de puertas o cajas de luz y con salida Wiegand como lo requiere el mercado de control de accesos.

La norma ISO14443 A se hizo a partir de la tarjeta Mifare por lo tanto puede afirmarse con toda certeza que Mifare cumple el 100% con dicha norma.

5.2.2.5.2. iCLASS

Esta tarjeta fue introducida por HID en el mercado de control de accesos más de 10 años después de las Mifare, por lo que no es justo hacer una comparación directa entre ambas tecnologías. Sólo citar iCLASS como una familia de control de accesos, que genera una aplicación más segura y versátil que la de Mifare, dado que fue pensada para ello y mantiene todo lo referido a los formatos propietarios y de numeración controlada que se describieron para proximidad.Con referencia a las normas, iCLASS cumple con la ISO14443B, que es similar a la versión A con algunas ventajas, y la ISO15693 que, por norma, le permite tener rangos de lectura de hasta 2 metros, mientras que la ISO14443 A y B están limitadas a 10 centímetros máximo.

5.2.2.5.3. Lectores smartcards

Un comentario aparte merecen los lectores de smartcards para control de accesos, debido a que observando las hojas de datos, generalmente se nota que son capaces de leer varias normas. Esto está relacionado con el hecho de que todas las normas trabajan en la misma frecuencia de portadora (13,56 MHz), por lo que los lectores de iCLASS leen también los CSN de las tarjetas Mifare y algunos lectores de Mifare leen los CSN de iCLASS.

Debe tenerse presente que utilizar el número CSN hace que la sofisticada seguridad que describimos no sea utilizada para el control de accesos, porque recordamos que el CSN está guardado en el sector sin contraseñas.

A partir de entender los mecanismos de seguridad, la ventaja de estar normadas y sabiendo que los costos de una smartcard son similares -y hasta menores que los de proximidad- y que mantienen los conceptos de formatos y numeración, es fácil de ver porque esta tecnología está reemplazando a la de proximidad, aunque no con la velocidad esperada.

5.2.2.5.4. Aplicaciones

Como ya se mencionó, las smartcards admiten varias aplicaciones simultáneamente debido a que poseen varios bloques/sectores de memoria aislables entre sí.

No es necesario que todas las aplicaciones estén cargadas en la tarjeta al momento de entregarlas. O sea que se puede vender una aplicación de control de accesos y cuando el usuario necesite otra aplicación, por ejemplo control de comedor de fábrica, mediante un proceso de software se habilitará esta nueva aplicación. Este proceso podrá repetirse tantas veces como se desee en tanto haya lugar disponible en la tarjeta y se conozca la información de las llaves. Esto es necesario aclararlo, ya que algunos fabricantes de aplicaciones se reservan el resto de la tarjeta disponible (esto se hace cambiando las llaves de transporte por llaves privadas).

Para entender el funcionamiento y la interacción de las tareas entre sí, describiremos el proceso de una manera más detallada, utilizando como ejemplo a una tarjeta iCLASS de 2Kbytes con 16 bloques/sectores, de forma tal de tener en una primera etapa sólo la aplicación de control de accesos y luego agregar una aplicación de comedor:

1- Al momento de comprar una tarjeta iCLASS preparada para control de accesos se recibe una tarjeta configurada de la siguiente forma:

a. 1 sector público que no tiene llaves y donde se encuentra el CSN (Card Serial Number).

b. 1 sector que HID utiliza para almacenar la "aplicación de control de accesos". Sólo HID conoce las llaves de este sector/aplicación y es ahí donde se almacena, con toda seguridad, el número con formato que será leído por el lector HID (que conoce las llaves de ese sector) y enviado al controlador según el formato indicado, por ejemplo Wiegand 35 bits.

c. 13 sectores libres con las denominadas "llaves de transporte", es decir llaves semipúblicas y conocidas por el usuario

2- En estas condiciones el conjunto de tarjetas y lectores funcionan correctamente en la aplicación de control de accesos. Vale mencionar que los lectores utilizados para esta aplicación son los denominados "read only", es decir, lectores HID de lectura solamente, que lo único que hacen es autenticar las tarjetas iCLASS con las llaves de HID, leer la información almacenada en el sector/aplicación de control de acceso y transmitir ese código por la salida Wiegand.

3- Supongamos que un tiempo después, el cliente final, por ejemplo una empresa automotriz, desea tener una aplicación para ser utilizada por los obreros en su comedor. La misma prevé que todos los lunes se cargará en cada tarjeta una cantidad de comidas, dependiendo de los turnos que deba cumplir (por ejemplo 7). Para poder implementar esto será necesario adicionar el siguiente equipamiento:

a. Un equipo en cada comedor, generalmente PC's con lectoras iCLASS de lectura y escritura, corriendo la aplicación del comedor. Esta aplicación deberá leer el sector que posee la cantidad de comidas permitidas y descontar una cada vez que el empleado se presenta en el comedor, permitiéndole el acceso si todavía "tiene crédito de comidas".

b. La aplicación, todos los lunes o el primer día de la semana que el empleado se presente, deberá adicionar 7 o el número que corresponda a este contador de comidas habilitadas.

4- Para que esto funcione correctamente y en forma segura, las tarjetas deberán ser inicializadas con la información inicial necesaria por la aplicación, proceso que puede ser implementado en forma transparente en las mismas lectoras del comedor la primera vez que el empleado presente su tarjeta en alguna de ellas o si el departamento de recursos humanos así lo decide, podrá colocarse un puesto adicional exclusivo para este fin. En qué consiste técnicamente esta inicialización: en cambiar las llaves del sector elegido para esta aplicación por llaves privadas e inicializar la información del sector con por ejemplo 0 comidas. Si no se cambian las llaves de la aplicación, cualquier persona capacitada podrá acceder a este sector/aplicación y modificarla a voluntad, dado que estará con las llaves de transporte, que es semipública. ■