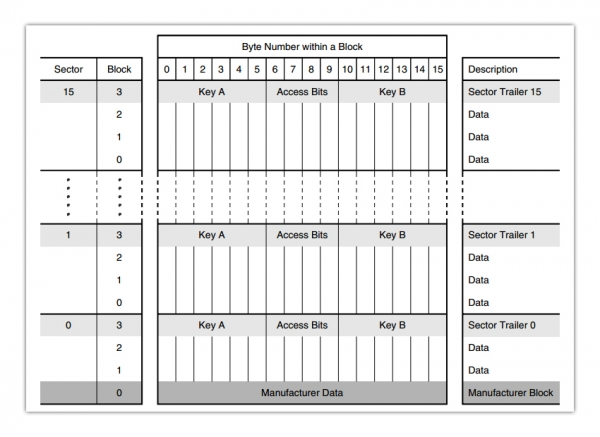
MIFARE

* Chip (lectura / escritura) de proximidad (RFID o radiofrecuencia),
* Funciona a 13,56 MHz (alta frecuencia)
* Cuenta con unas zonas de memoria que permiten almacenar información y que tiene un cierto nivel de seguridad para acceder a dicha información (encriptación)

Almacenamiento de información

* Se almacena en una memoria de tipo EEPROM (algo parecido a la memoria RAM de un PC pero no volátil)
* En las tarjetas de **1K** estos espacios de memoria se dividen en 16 sectores, que a su vez se subdividen en 4 bloques por sector. Cada uno de estos bloques almacena hasta 16 bytes. (16x16x4=1024 bytes)
* El tener varios bloques permite que una unica tarjeta se pueda utilizar para diferente servicios



*\*(Esquema de la memoria de una tarjeta MIFARE Classic 1K)*

El acceso a cada uno de los diferentes bloques es definido por el usuario. Esto significa que cada bloque puede ser:

* público (no necesita clave y puede ser leído por cualquier aplicación)
* privado (necesita clave para poder leer / escribir la información creando zonas seguras).

Esta característica hace que la tarjeta MIFARE sea suficientemente segura para uso como tarjeta monedero (p. ej. la tarjeta del autobús).

MIFARE provee un formato especial llamado 'bloque de valor'; los bloques que tienen información guardada en este formato se comportan de una forma diferente, incluyendo operaciones de descuento e incremento.

Los sectores utilizan dos claves de acceso llamadas 'A' y 'B'. Estas llaves se almacenan en el cuarto bloque junto con los permisos de acceso a cada uno de los tres bloques. Estos permisos pueden ser: lectura, escritura, descuento o incremento (para bloques de valor).

Existe un bloque especial que esta localizado en el bloque de datos 0 del sector 0, que alberga la siguiente información en modo solo lectura:

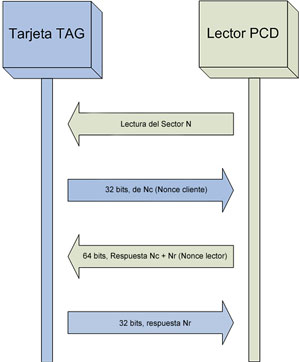
* UID – Identificador único de la tarjeta.
* BCC – bit count check, calculado por la sucesivas XORs de los bytes del UID.
* 11 bytes de datos que identifican al fabricante del tag.

Comunicación cifrada

Una vez que se acerca la tarjeta a un lector, **ésta se activa e inicia un proceso de intercambio con el lector para establecer una comunicación cifrada**. Este proceso es igual con todas las tarjetas y está diseñado para proveer protección contra escucha del canal, y no para autenticar la tarjeta o el lector.

Después de establecer un canal cifrado, la tarjeta envía un código de identificación de conexión, que usualmente es el número de serie de la tarjeta, aunque la norma ISO 14443 dice que este número puede ser aleatorio. Con este número de conexión el lector está en capacidad de realizar cualquier operación en la tarjeta.

Proceso de autenticación



*proceso de handshake.*

1. En primera instancia el lector le comunica a la tarjeta que quiere realizar una operación sobre un sector de datos determinado.
2. La tarjeta en ese momento remite un número aleatorio de 32 bits a modo de desafío, para que sea cifrado con la clave privada compartida previamente.
3. Como respuesta, el lector remite el desafío cifrado y un número aleatorio para que el tag lo cifre con la clave privada, generando una trama de 64 bits.
4. En última instancia la tarjeta le envía al lector su desafío cifrado.
5. En este momento ambos tienen la certeza de que los dispositivos son legítimos.