

CyberHack Magazine #4



Indice:

0.- Introducción

1.- Cómo convertir una tarjeta de 1000 Pts en una de 2100 Pts.

2.- Programador de EPROM para PIC. (PIC + Serial ROM programmer).

3.- Tarjetas de crédito. Parámetros

0.- Introducción.

Por fin vamos recibiendo colaboraciones, y en este caso bastante buena sobre como ahorrarte mas de la mitad de pelas llamando con tarjetas de Timofónica.

También he recibido correos pero no como estos de colaboración, sino achacandome que en el numero tres al escanear el ZIP les sale el Virus Terror. Jejejeje ... Estos lamers que se metan el dedo en el culo porque si los he metido son para que contagieis a quien mas rabia os de no para que los borreis... pero bueno después se quieren llamar hackers.....

De todos modos hay bastante gente buena por ahí perdida y que no colaboran ni consigo mismos.

Pero andan sueltos algunos capullos que nada mas saben ciritikar la mag, pues les propongo que hagan una revista... y seguro que aunque la hicieran de lamers no pasaban de dos lineas.

1.- Cómo convertir una tarjeta de 1000 Pts en una de 2100 Pts.

INTRODUCCIÓN

Nosotros, como la gran mayoría de fieles al hacking, y mas concretamente al phreaking, también intentamos llevar a cabo uno de los sueños para cualquier revienta cabinas o TM's (terminales modulares)... pero las repuestas obtenidas para los diferentes esquemas existentes, y me refiero al archiconocido tema de emulación para tarjetas prom, han sido totalmente negativas.

Fue entonces cuando decidimos realizar un estudio a nivel medio del conjunto tarjeta-cabina (nuestros recursos son mínimos), llegando a la conclusión de que no es tan fácil engañar a un TM...

A si que presentamos el fantástico 1000 x 2000; un esquema que nació como parte de nuestros múltiples ensayos para comprobar el funcionamiento del conjunto tarjeta-cabina. Su funcionamiento es extremadamente trivial, ya que lo único que hacemos es engañar al TM haciéndole creer que hemos introducido una tarjeta de 2000 ptas., siendo esta solo de 1000ptas.

Para esto es necesario (esta es la peor parte) poseer (comprar) una tarjeta nueva de 1000ptas y buscar una tarjeta usada de 2000ptas (o mejor de 2100ptas).

FUNCIONAMIENTO

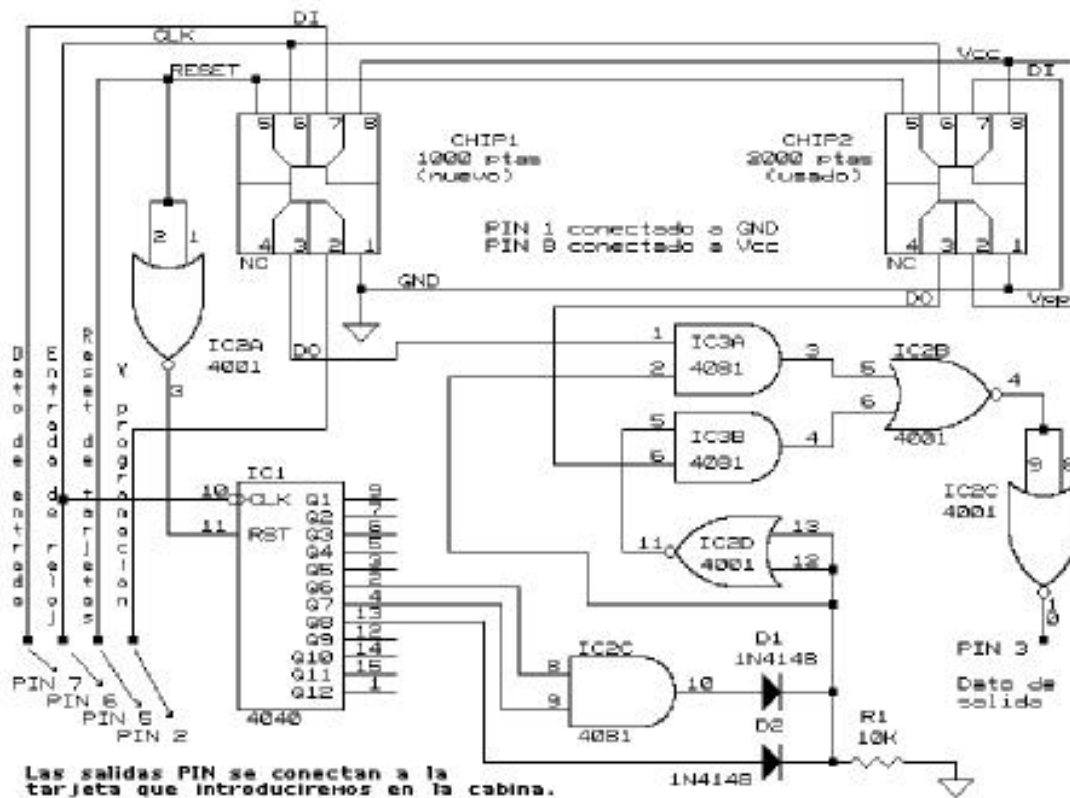
La tecnología utilizada para los circuitos integrados ha sido CMOS ya que el consumo de estos es mínimo (del orden de microamperios).

En un primer plano general podríamos describir el circuito como un selector de datos de una (CHIP1) u otra tarjeta (CHIP2), dependiendo del valor del contador (IC1).

Realmente el conjunto de puertas IC2B-D e IC3A-B se comportan como un multiplexor de dos entradas controlado por la selección de direcciones del contador IC1. De esta forma los primeros 96 bits se leen de la tarjeta CHIP2 (2000ptas) y el resto de la tarjeta CHIP (1000ptas), esto nos permite utilizar una tarjeta de 1000ptas como si fuera de 2000ptas, ya se que lo suyo seria no tener que comprar la tarjeta o que conserváramos el importe total de la misma, pero la pura realidad es que los fusibles de la tarjeta CHIP1 (1000ptas) se irán fundiendo como si pertenecieran a la tarjeta CHIP2 (2000ptas), y tarde o temprano se acabaran... pero la broma nos habrán costado solo la mitad, es decir timofónica nos permite un descuento del 50%.

COMPONENTES

- 4040
- 4081
- 4001
- 2 x 1N4148
- 10K $\frac{1}{4}$ w
- CHIP tarjeta nueva 1000 ptas
- CHIP tarjeta usada 2000 ptas
- tarjeta para introducir en cabina **



**** NOTA**

Necesitaremos construirnos una tarjeta para poder conectar cada uno de los PIN indicados en el esquema. PIN X donde X corresponde a el numero de contacto en el chip de la tarjeta que introduciremos en la cabina.

-- Existen varios métodos en otros docs, para construirse la tarjeta-conector --

Referencias :

- Ingenieros Cabreados. (Comentario de Cy.... Está bien pensado pero es una puta fantasmada de esta gente)
- Emulador de tarjetas PROM.

En mi caso construí la tarjeta con un trozo de circuito impreso normal, dibujando los correspondientes contactos (con mucho cuidado y paciencia) con un rotulador (tipo edding 3000) y retocándolos posteriormente mediante un punzón muy afilado. Luego preparamos el cloruro férrico o mezcla de agua fuerte, agua oxigenada y agua normal (proporción 30 cada uno) para grabar las pistas dibujadas; y por ultimo estañamos con decapante (lo usan los fontaneros para soldar tuberías).

Lo mejor es seguir el circuito construido en el documento de emulador de tarjetas prom, por Manuel García.

Por ultimo limar el circuito hasta que su grosor sea el mismo que el de una tarjeta normal y soldar los correspondientes cables al circuito arriba mostrado.

Saludos y feliz phreaking....

Sys Silicon

Gracias a Sys Silicon por este texto que además funciona no como otros cientos que rulan por los Webs españoles...Pues si sabeis que no funciona porque mierda lo poneis..... Habeis visto en este Web esas mierdas de emuladores..... NO!!!! Pues dejad ya de meter mierda a la gente para que vayan a las tiendas de electrónica y hagan ricos a los dependientes comprando todos los componentes menos el 4537, BF320, etc...

2.- Programador de EPROM para PIC. (PIC + Serial ROM programmer).

CARACTERÍSTICAS DEL PROGRAMADOR

MultiMac 1.70 (single-chip)

25 channel single PIC Eurocrypt Emulator, with selectable fileformat and I/O pin. Decodes: Tv3 S/D/N, Filmnet 1/2, Tv1000/Cinema, CNN, Mtv, Discovery, TCC, Eurosport, Canal+, Cinecinema, BBC prime, Tv 2 Nor, DR2, Nickelodeon, VH-1, Supersport, TNT, Cartoon Network, Sci-fi.

MultiMac II (2.11) (double-chip)

27 channel PIC+Eeprom Eurocrypt/VC1 Emulator, with selectable fileformat and I/O pin. Decodes: Tv3 S/D/N, Filmnet 1/2, Tv1000/Cinema, CNN, Mtv, Discovery, TCC, Eurosport, Canal+, Cinecinema, BBC prime, Tv 2 Nor, DR2, Nickelodeon, VH-1, Supersport, TNT, Cartoon Network, Sci-fi and TAC, Eurotica.

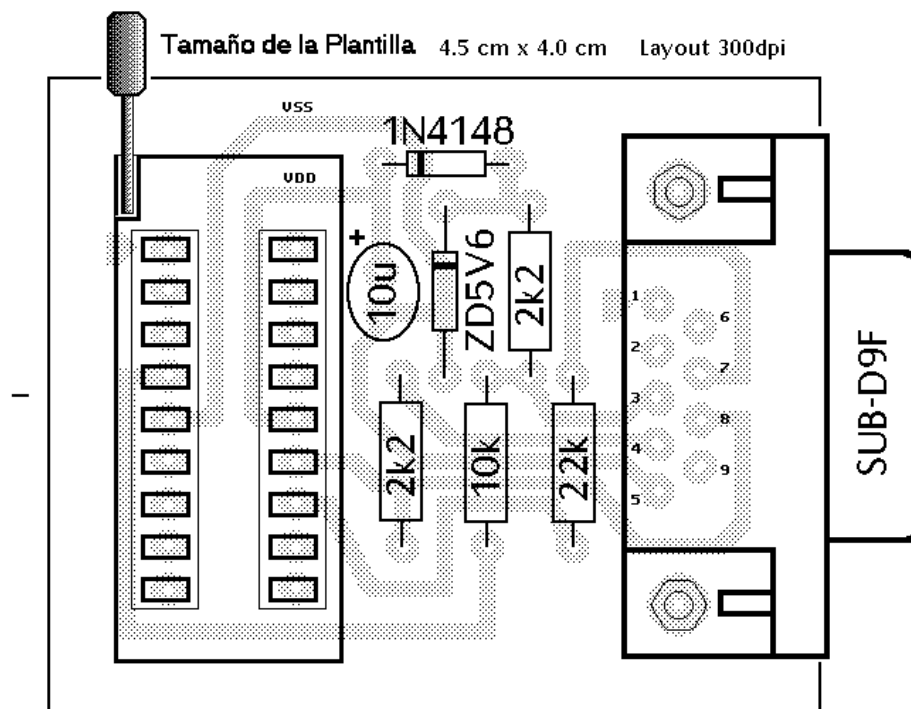
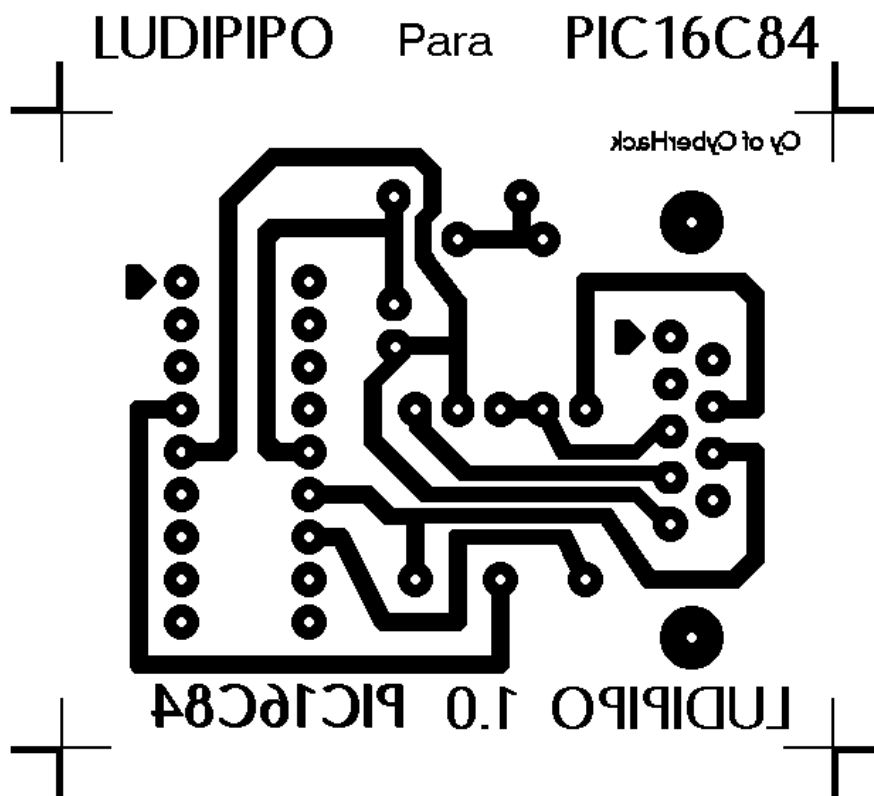
Voyager 1.60

Voyager 1.60. PC Smartcard Emulator for Videocrypt 1 and 2, Eurocrypt M/S2, with plaintext file, so you can add the new key's yourself. bugfixed. (Please mail me if it works)

Ludipipo

Pic + EEprom programmer. Trabaja en todos los puertos de serie sin la necesidad de alimentación adicional.

Veamos el esquema que tendríamos que montar:

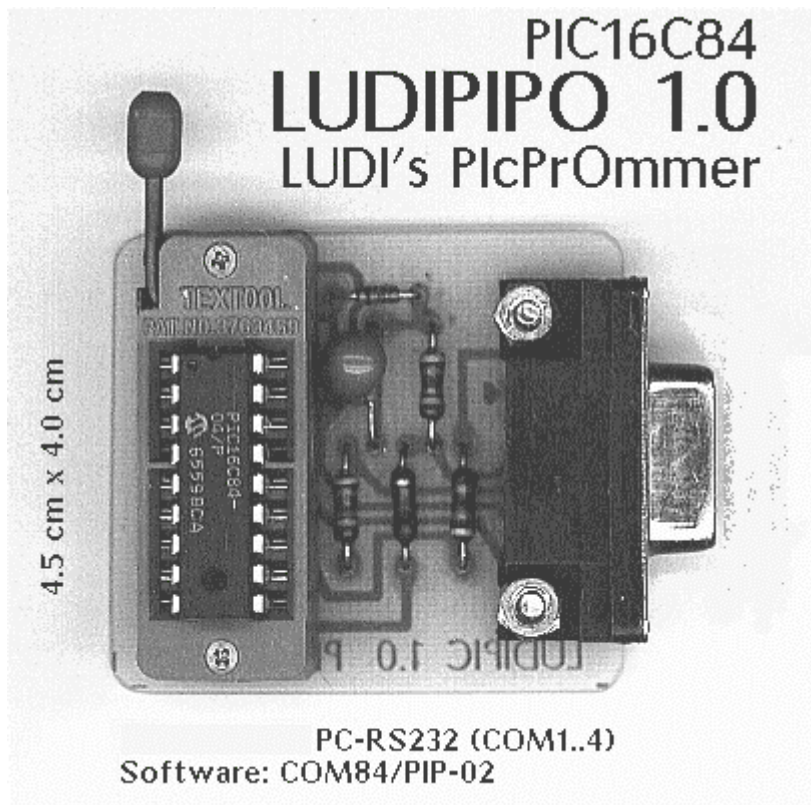


Material Necesario: Placa fotosensible, Zócalo ZIF 18 PINES, Conector SUB-D9F, Condensador tantalio 10u/16V
 Diodo 1N4148, Diodo Zener 5V6, Resistencias 2k2, 2k2,10k, 22k
 SoftWare: COM84 (Para el puerto de serie (TSR)), PIP-02

De todos modos en el archivo pack, incluyo el dibujo para que pueda ser visto e impreso mejor.

Este programador vale también para el chip de la PSX, pero hay que saber como hacerlo y para eso hacen falta profesionales (Fre... y Wil....) que son expertos en ello.

El invento final quedaría tal que así.



Bueno pues como veis no es nada difícil de construir y los programas ya van incluidos en el paquete de la revista.

3.- Tarjetas de crédito. Parámetros.

Utilizada por lo general para identificar las partes que intervienen en una transacción financiera y para facilitar información de entrada para una transacción. Por consiguiente, es semejante a la definición de tarjeta para transacciones financieras.

Periodo (ciclo): Lapso de tiempo fijo o predeterminado que determina la validez de ciertas transacciones.

PAN (número de cuenta primario, del inglés “ primary account number “). Número asignado que identifica al emisor de la tarjeta y a su poseedor. Se

compone de una identificación del emisor, una identificación de una cuenta individual y de un dígito de comprobación que lo acompaña, tal como se especifica en la norma ISO 2894 (hoy en la 7812:1987), donde podrá encontrarse la estructura del PAN y las variaciones que la norma 4909 que comentamos determina para las tarjetas bancarias.

SAN-1 (de “ subsidiary account number “). Identificación de una primera cuenta subsidiaria opcional complementaria del PAN.

SAN-2 .Identificación de una segunda cuenta subsidiaria opcional complementaria del PAN y del SAN-1.

PIN (número de identificación personal): Código secreto usado por un poseedor de tarjeta para acreditar la propiedad de la misma.

La siguiente tabla muestra la disposición de la información en pista 3:

N.	CONTENIDO (A)	(B)	(C)	(D)	(E)
1	Cácter de comienzo	0	E	F	1
2	Código de formato	0	E	F	2
3	Numero de cuenta primario PAN	(3)	E	V	(3)
4	Separador de campos	0	E	F	1
5	Codigo del pais	0(5)	E	F	3
6	Moneda	0	E	F	3
7	Exponente de la moneda	0	E	F	1
8	Importe autorizado por ciclo	0	E	F	4
9	Importe disponible en el ciclo en curso	0	D	F	4
10	Principio del ciclo	0	D	F	4
11	Duracion del Ciclo	0	E	F	2
12	Numero de intentos	0	D	F	1
13	PINPARM	0(13)	E	F	6
14	Control de intercambio entre instituciones bancarias	0	E	F	1
15	Tipo de cuenta (TA) y restricciones de servicio (SR)(PAN)	0	E	F	2
16	TA y SR (SAN 1)	0	E	F	2
17	TA y SR (SAN 2)	0	E	F	2
18	Fecha de Caducidad	0(18)	E	F	4
19	Núm. De Secuencia de tarjeta	0	E	F	1
20	Núm. Seguridad tarjeta	0(20)	D	F	9
21	SAN-1	F	E	V	(21)
22	Separador de campo	0	E	F	1
23	SAN-2	F	E	V	(23)
24	Separador de campo	0	E	F	1
25	Indicador de transmision de informacion discrecional	0	E	F	1
26	Dígitos de comprobacion de criptografia (CDD)	0(26)	D	F	6
27	Informacion discrecional del emisor	F	D	V	(27)

28	Centinela final	0	E	F	1
29	Comprobacion de redundancia (LCR)	0	D	F	1

Notas generales sobre las columnas del cuadro anterior de la pista 3:

(N) Número de orden de cada campo.

(A) Los caracteres que se especifican en las observaciones que siguen referidas a cada campo corresponden al juego para las pistas 2 y 3.

(B) Los campos pueden ser O= Obligatorio; F= Facultativo (cuando en un campo facultativo no esté presente un separador FS= carácter línea 13, irá en su lugar).

(C) Los campos D= Dinámicos, serán actualizados, cuando corresponda, por los participantes en el sistema de intercambio bancario, mientras que los campos E= Estáticos, serán modificados únicamente por el emisor.

(D) Formato: F= Fijo; V= Variable.

(E) Longitud de cada campo en número de caracteres. El número de caracteres en esta pista 3 no excederá de 107.

Información adicional sobre cada uno de los campos .(Se indica delante el número del campo):

- 1) Contenido carácter línea 11.
- 2) Formato de los dígitos con el siguiente contenido: 00 = no válido para intercambio internacional; 02 a 19 = reservado para futuras asignaciones por el subcomité ISO/TC 68; 20 a 89 = reservado para futuras asignaciones del subcomité ISO/TC 95 S/C 17; 90 a 99 = disponibles para uso particular de los emisores de tarjetas, pero no para intercambio internacional. (Los emisores que deseen usar códigos comprendidos entre 02 y 89 y se dirigirán a través de su organismo nacional de normalización, al comité correspondiente de ISO).
- 3) Identifica al emisor de la tarjeta al cual debe ser enviada la transacción y al titular o poseedor de la misma.

Véase su composición en el apartado anterior, como ya dijimos. La identificación del emisor es de longitud variable entre 3 y 11 caracteres y la de cuenta individual pueda tener una longitud hasta de 23 caracteres. Sigue un dígito de comprobación de un carácter.

Cuando se utilizan dos pistas, si el PAN va codificado en la pista 2 la codificación en el PAN en la pista 3 es opcional. Cuando el PAN sea codificado en la pista 3 figurarán todos los componentes.

- 4) Tiene por objeto indicar final del PAN o ausencia del mismo.

Carácter línea 13.

- 5) Identifica el país al que debe ser encaminada la información de la transacción generada por la tarjeta, cuando se ha usado el identificador 59 de actividad económica. Formato:3 dígitos (CCC) de acuerdo con asignación de ISO 3166 (para España el 724).

- 6) Indica el tipo de moneda que debe emplearse en el cálculo para la actualización. Formato 3 dígitos con arreglos a códigos de moneda de la norma ISO 4217 (para España 724). Si se rellena con tres ceros significa que la tarjeta no es válida para intercambio internacional.
- 7) Su objeto es determinar el valor base de los campos “ importe autorizado” e “ importe disponible” , mediante un dígito que indica la potencia de 10 por la que hay que multiplicar los citados campos para expresarlo en la unidad principal de la moneda que se especifica en el campo 6. Los exponentes autorizados son 0 para unos países, 0 y 1 para otros y 0 a 2 para un tercer grupo. Como los campos citados tienen cuatro cifras, los valores máximos resultantes serán: 0=9.999; 1= 9.990; 2= 999.990. Recomienda la norma que todas las tarjetas , cualquiera que se sea su fecha de emisión, contengan el mismo exponente de la moneda y que exceda de los asignados en la tabla que acompaña a la norma. No obstante, los fenómenos de inflación obligan a revisar esta asignación.
- 8) El valor numérico de este campo se utiliza para actualizar el importe disponible en el ciclo de actualización del campo siguiente. Se codifica cuatro ceros si no se permite operaciones de cargo.
- 9) Indica el saldo disponible del importe autorizado en el ciclo en curso. Se redondea a la unidad más próxima, en la moneda utilizada en el campo anterior. En la primera utilización después del principio de cada nuevo ciclo, este se repondrá con el valor del importe autorizado por ciclo. Después, contendrá el importe disponible en este ciclo.
- 10) Indica la fecha en la cual comienza un nuevo ciclo. También puede utilizarse para definir la primera fecha de validez de la tarjeta. El formato es YDDD, donde Y es el último dígito significativo del año y DDD es el número secuencial del día dentro del año en la escala 001 a 366. Debe ser actualizado con fecha actual cuando el valor de este campo más el valor del campo “ duración del ciclo “sea menor o igual a la fecha actual, salvo que el valor del campo “ duración del ciclo “ esté comprendido entre 80 y 99, ambos inclusive.
- 11) Indica el periodo de tiempo durante el cual la suma acumulada de todas las transacciones no debe exceder del importe autorizado. Su contenido, en dos dígitos, tiene el siguiente significado: 00= igual “ importe disponible en el ciclo tendrá una duración de 7 días, y el campo “ principio del ciclo “(en lo sucesivo PC) se actualizará solamente por adiciones de periodos múltiplos de 7; 81 = el ciclo de una duración de 14 días y el campo “ PC” se actualizará solamente por adiciones de periodos múltiplos de 14; 82 =el ciclo empezará solo en los días primero o decimoquinto de un mes cualquiera; 83= el ciclo empezará en la misma fecha de cada mes de calendario, comenzando en la fecha representada por el campo “ PC” que fue grabado en la emisión de la tarjeta; 84= el ciclo empezará en la misma fecha de cada tercer mes del

calendario, comenzando en la fecha representada por el campo “PC” que fue grabado en la emisión de la tarjeta; 85= el ciclo empezará en la misma fecha representada en el campo “ PC” que fue grabado en la emisión de la tarjeta; 86= el ciclo empezará en el aniversario de la fecha representando en el campo “ PC” que fue grabado en la emisión de la tarjeta.

- 12) Sirve para registrar el número de intentos fallidos de que se dispone para introducir el número de identificación personal (PIN) asociado a la tarjeta. Formato de un dígito que en el intercambio entre instituciones bancarias será 3, que se grabará al emitir la tarjeta y posteriormente se repondrá después de cada introducción correcta del PIN .Se restará uno por cada entrada incorrecta del PIN. La tarjeta será inválida para todo propósito del intercambio si el contenido de este campo es 0.
- 13) El PINPRAM contiene parámetros de control para el número de identificación personal con objeto de facilitar una medida de seguridad opcional en forma de un código de algoritmo y un valor complementario, estando constituido por seis dígitos en la forma AA0000, en donde AA: es la identificación del algoritmo y 0000 es el valor complementario que cuando se calcule el algoritmo servirá para validar el número de identificación personal. Si no se utiliza el PINPRAM en este campo se incluirá un separador de campo. También si el valor de AA = 00 indica que no se emplea algoritmo, los valores 01 a 99 serán definidos por ISO.
- 14) Indica si la tarjeta está autorizada para el intercambio entre instituciones bancarias, y está formado por un dígito con el siguiente significado: 0= sin restricción; 1= no disponible para intercambio internacional; 2 a 9 intercambio limitado, en cuyo caso la tarjeta está restringida a usarse en un ámbito local, ciudad o país, y no debe ser aceptada sin acuerdo previo con el emisor de la tarjeta. En España el código 2 indica “ no disponible para intercambio nacional “.
- 15) Define mediante 2 dígitos el tipo de cuenta (TA) y las posibles restricciones de servicio (SR) para la cuenta registrada en la identificación de cuenta individual en el campo PAN. El primer dígito define el tipo de cuenta con el siguiente contenido: 0 = número de cuenta del primario no codificado en pista 3; 1 cuenta de ahorro; 2= cuenta corriente o de cheques; 3 cuentas de tarjetas de crédito; 4= número común aplicable a más de un tipo de cuenta, por ejemplo; Número cuenta universal, 5 a 8 = reservado para asignaciones ISO; 9= disponible para uso interno del emisor y no para intercambio entre instituciones bancarias. El segundo dígito define las restricciones de servicio con los siguientes contenidos: 0= sin restricciones; 1= prohibido cargos; 2= prohibido abonos; 3= sólo permitidas transacciones de abonos; 4 a 7= reservado para asignaciones de ISO; 8 y

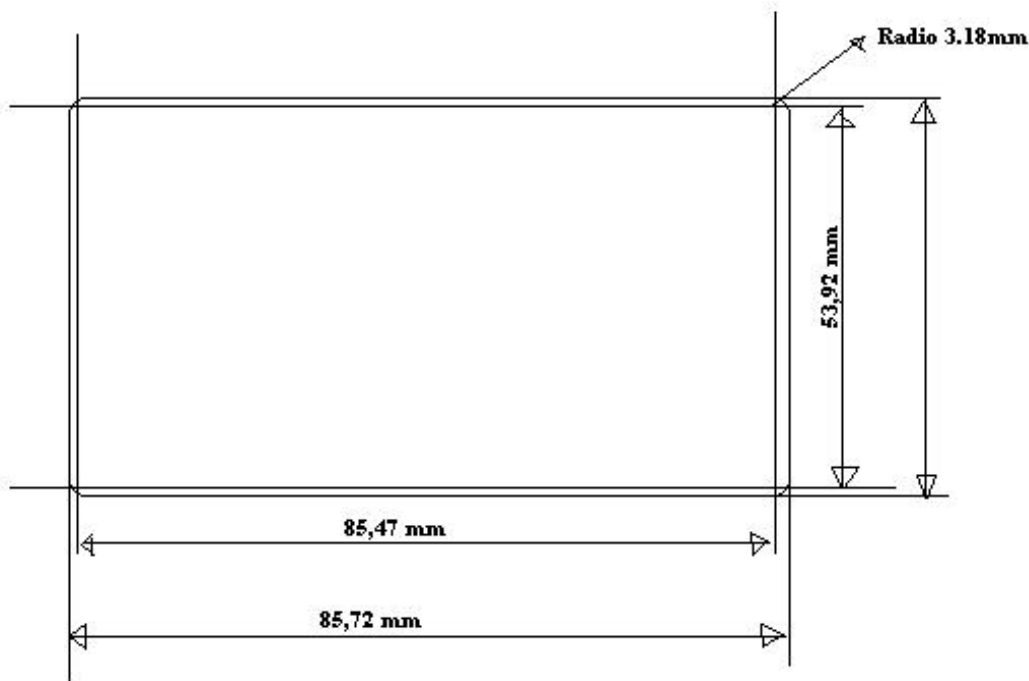
- 9 = disponible para uso externo de los emisores, en cuyo caso el uso de la tarjeta está limitado a un ámbito local, ciudad o país, y no debe ser aceptado sin previo acuerdo con el emisor de la tarjeta.
- 16) Tipo de cuenta y restricciones de servicio referidas al número de cuenta contenido en el campo SAN-1 (21). El significado de los códigos será el mismo que en el campo 15, excepto que el tipo de cuenta = 0 indica que SAN-1 no está codificado en la pista 3.
 - 17) Los mismos que en el campo anterior, pero referido al número de cuenta SAN-2 contenido en el campo 23. Si el tipo de cuenta es =0 indica que SAN-2 no está codificado en la pista 3.
 - 18) Indica la fecha después de la cual la tarjeta pierde su validez. Se expresa con 4 dígitos en la forma YYMM, cuando existían, siendo YY últimos dígitos del año de caducidad. La validez de la tarjeta cesa después del último día del mes especificado. Si no se especifica fecha de caducidad se sustituirá por un separador.
 - 19) Permite distinguir entre distintas tarjetas (emitidas concurrentes o secuencialmente) que tengan el mismo PAN. El contenido es un dígito a discreción del emisor y será grabado en la emisión original de la tarjeta o renovación siguiente a la caducidad. Debe ser incrementado en una unidad cada vez que una tarjeta sea emitida con carácter adicional o por sustitución de la original.
 - 20) Permite relacionar la información contenida en la banda magnética con la tarjeta física. Está constituido por 9 dígitos en la forma MCCCCCCCC, en donde M = identificador del método de seguridad y CCCCCCCC, es el código capaz de establecer la relación entre la información y la tarjeta. Si no se utiliza incluirá un separador de campo.
 - 21) Número de la primera cuenta subsidiaria SAN-1 que es opcional, siendo el contenido cualquier valor numérico de longitud variable si existe la cuenta.
 - 22) Este separador de campo tiene por objeto terminar o indicar la ausencia de SAN-1.
 - 23) Número de la segunda cuenta subsidiaria SAN-2 opcional, mediante un valor numérico de longitud variable.
 - 24) Este separador de campo tiene por objeto terminar o indicar la ausencia de SAN-2.
 - 25) El objeto de este campo es facilitar la reducción de la longitud de los mensajes intercambiados entre los centros informáticos de los bancos. Este indicador muestra si el mensaje que se intercambia debe o no incluir los contenidos del campo de información discrecional (27). Su contenido será un dígito con el siguiente significado 0 = incluir toda la información discrecional; 1 = no incluir la información discrecional; 2 a 9 = inválidos.

- 26) Tiene como finalidad proporcionar un medio de verificar la integridad de los elementos de la información en la pista 3, a través de la aplicación de una fórmula criptográfica. El formato es de seis dígitos a ser definidos por ISO. Si se utiliza se incluirá en este campo de separador.
- 27) Su objeto es incluir información válida para el emisor de la tarjeta. Los contenidos de este campo se incluirá en el mensaje de intercambio que pasa entre el dispositivo lector de la pista 3 y el emisor de la tarjeta si el indicador de transmisión discrecional puede incluir cualquier valor numérico.
- 28) Indica la terminación de la información válida en la pista 3. El carácter es el correspondiente a la línea 15 del juego de caracteres.”
- v. sistema de numeración y procedimiento de registro para los identificadores del emisor de tarjetas de transacciones financieras; tarjetas de identificación destinadas a “ transacciones financieras”. Normalización. Estructuras pistas 1 y 2.*

Tarjetas de identificación destinadas a “ transacciones financieras “. Normalización. Estructuras de las pistas 1 y 2.

No es hasta 1985 cuando se establece una distinción específica, dentro de las tarjetas de identificación, de aquellas destinadas a las transacciones financieras, momento en el que se publica la ISO 7813, de la que se produce una segunda edición recogiendo revisiones técnicas posteriores en 1 de junio 1987. El objetivo de esta norma es especificar directamente o por referencia a otras normas las condiciones que deben cumplir las tarjetas utilizadas en las transacciones financieras, teniendo en cuenta aspectos humanos y de máquinas o equipos. Abarca las características físicas, la presentación, las técnicas de registro, el sistema de enumeración, los procedimientos de registro, pero no contiene especificaciones concernientes a la seguridad. La definición de la tarjeta que da esta norma así como sus características físicas deben ser las estipuladas por la norma ISO 7810, con las precisiones que realiza la norma 7813. Las dimensiones son las que aparece en la figura, admitiendo una tolerancia para el grueso de 0.08 mm (0.003 in), debiendo ser las esquinas redondeadas con un radio de 3.18 mm (0.125 in), evitando que presenten defectos de alineamiento con referencia a los bordes rectilíneos de la tarjeta.

Dimensiones de la tarjetas



Las posibles rebabas de los bordes, perpendiculares a la tarjeta, no pueden rebasar 0.08 mm (0.003 in). En cuanto a la presentación, remite en lo referente a la zona de la estampación que debe situarse sobre el anverso de la tarjeta a las especificaciones de ISO 7811/3, en el que tomamos en cuenta las variaciones de la norma 7813 para las transacciones financieras no estampadas, en tanto que para la zona de la banda magnética, que debe estar situada en el reverso de la tarjeta, adyacente a su borde superior, deben observarse las especificaciones de las normas ISO 7811/4 e ISO 7811/4. El proceso de estampación debe seguir las especificaciones de ISO 7811/1 y 7811/3. Las características de la banda se contienen en las normas ISO 7811/2, 7811/4 y 7811/5.

El sistema de numeración para identificadores del emisor está descrito en la norma ISO 7812. Por consiguiente, las normas son las mismas que las establecidas para las tarjetas de crédito, con las precisiones que hemos hecho hasta ahora. Sin embargo, para la estructura de las pistas 1 y 2 se dan las siguientes normas específicas para las tarjetas de identificación de transacciones financieras, remitiendo en lo diferente a la pista 3 a la norma ISO 4909. Veamos ahora la normalización de las pistas 1 y 2 de la tarjeta que nos ocupa:

Estructura de la pista 1. Admite dos estructuras para esta pista. La que denomina “A” no se define, indicando que queda reservada al uso privado del emisor de las tarjetas, quien, por tanto, puede darle la estructura que satisfaga sus requisitos de proceso y control. La estructura que denomina “B” tiene las siguientes especificaciones:

STX Carácter de comienzo (posición 0/5 = %).

FC Código de formato (posición de formato 2/2=B).

PAN Número de identificación (hasta 19 cifras).

FS Separador (posición 3/14= ^).

CC Código de país (definidos en ISO 3166)(3 cifras). Puesto que el número de identificación (PAN) comienza por el identificador de la actividad económica “5” seguido de la cifra “9”, es obligado de codificar el código numérico de país ISO 3166. En los restantes casos el nombre debe seguir inmediatamente al separador situado al final del número de identificación (PAN).

NM Nombre (2 a 6 caracteres, como mínimo un carácter alfabético correspondiente al nombre y el separador del nombre). El orden de este campo es: 1) nombre; 2) separador del nombre(0/5=/); 3) primer apellido seguido de espacio (0/00), 4) segundo apellido o inicial y un punto (0/14=.) Si sigue un título; 5) título si se usa.

En el caso de que sólo se utilice el nombre, el separador del nombre seguirá un espacio. El juego de caracteres y las posiciones binarias se especifica en ISO 7811/2.

FS Separador (posición 3/14=^).

ED Fecha de expiración de validez en formato AAMM (cuatro cifras o en su ausencia posición 3/14=^).

ID Indicación de intercambio (una cifra) o posición 3/14. Este código es atribuido por el comité ISO responsable de esta normalización. Los códigos ya atribuidos son los siguientes: 1= disponible para intercambio internacional; 5= disponible para intercambio únicamente en el país de emisión 7= no disponible para un intercambio general (son posibles, acuerdos bilaterales particulares entre emisores); 9= tarjeta de prueba.

SC Código de servicio (dos cifras) o posición 3/14 (separador). Los códigos de servicios comprendidos entre el 00 y el 99 son atribuidos con el siguiente significado por tramos: De 00 a 49, códigos atribuidos y publicados por el comité ISO responsable de esta normalización; 50 a 59, códigos atribuidos y publicados por las instituciones nacionales de normalización; 60 a 99, códigos disponibles para ser asignados en relaciones privadas. En los códigos 00 a 49 se incluyen los que determinan restricciones de servicio o servicios que prestarse a existencia de autorización, presencia de un circuito integrado con o sin restricciones.

DD Datos libres (restos de los caracteres).

EXT Carácter de fin (1/15=?).

LRC Carácter de control de redundancia longitudinal.

El total de caracteres es como máximo de 79.

Estructura de la pista 2. Su contenido normalizado es el siguiente:

STX Carácter de comienzo (BCD11).

PAN Número de identificación (hasta 19 cifras).

FS Separador (BCD 11).

CC Código de país (3 cifras, con iguales requisitos que los vistos para la pista 1).

ED Fecha de caducidad o expiración, en formato AAMM (cuatro cifras o BCD 13).

ID Indicador de intercambio, con las mismas características que se han visto para la pista 1.

SC Código de servicio con las mismas características y significación de códigos que en la pista 1, para los asignados por el Comité ISO.

DD Datos libres (restos de cifras disponibles).

ETX Carácter de fin (BCD15).

LRC Carácter de control de redundancia longitudinal (una cifra).

La longitud máxima de registro será de 40 caracteres.

v. tarjetas bancarias. Zona magnética. Contenido en datos de la pista 3.

Técnicas de registro de las tarjetas, estampación y posición de los caracteres.

La estampación e caracteres destinados a la transferencia de datos a diversos soportes, bien por medio de máquinas de imprimir, bien por la lectura visual o por máquina, está normalizada en la ISO 7811/1, resumiendo a continuación esta norma aplicable, advirtiéndose que las para las tarjetas de identificación financiera es también aplicable en tanto no se produzca norma específica, cuando tales tarjetas lleven caracteres estampados:

-Caracteres legibles visualmente o por máquina: Pueden ser utilizados los juegos de caracteres ópticos OCRA (ISO 1073/1) dimensiones I y IV, y el tipo de caracteres 7B, que son los que se muestran en la figura, con la normalidad de que pueden ser leídos visualmente y/o por máquinas, sea directamente por la tarjeta, sea a partir de impresiones obtenidas sobre otro soporte directamente de la tarjeta por cal entre caracteres deben ser de 3.63 mm (0.143 in) nominal y mínimo entre dos caracteres consecutivos de 3.48 mm (0.137 in) en tanto que la lectura de los caracteres estampados sobre la superficie de la tarjeta debe ser de 0.48 mm (0.019 in) con tolerancia por defecto de 0.05 mm (0.002 in).

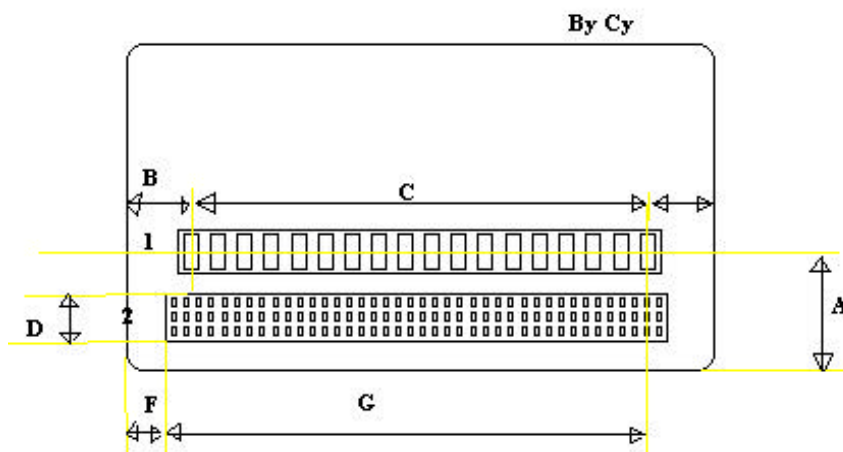
Los tipos de letras empleados son: OCR-A, OCR-B y Farrington 7 B que se pueden encontrar en cualquier sitio de Internet dedicado a FONTS... jejeje

- Caracteres legibles visualmente: Son los que no están destinados a ser legibles para una máquina.

Se utilizará para la estampación de estos caracteres el subconjunto de caracteres de mayúsculas alfanuméricas que figuran en el juego OCR-B (ISO 1073/2) dimensión I, siendo legibles directamente sobre la tarjeta o sobre un soporte impreso a partir de la tarjeta. El espaciamiento de caracteres de este caso es de 2.45 mm (0.100 in) nominal y mínimo entre

dos caracteres consecutivos 2.46 80.097 in), en tanto que la altura de relieve sobre la superficie de la tarjeta debe ser 0.46 mm (0.018 in) con una tolerancia por defecto de 0.05 mm (0.002 in).

Del posicionamiento de los caracteres estampados sobre las tarjetas ID-I se ocupa la norma 7811/3, a la que son aplicables las definiciones de la norma 7810 y de las restantes normas que le afecten. Cuando en ésta norma se refiere al “ número de identificación” debe entenderse que es el que identifica al portador o titular de la tarjeta. Las principales especificaciones son:



- Zonas atribuidas: Se destinan dos zonas (véase figura):
 - Zona 1.- reservada para el número que identifica al mismo tiempo al emisor y al portador de la tarjeta. Se denomina “ línea de número de identificación”. Los caracteres situados en esta zona y las impresiones obtenidas de los mismos deben ser válidos a la vez para la lectura humana y para el reconocimiento óptico de caracteres por la máquina.
 - Zona 2.- Prevista para datos concernientes a la identificación del portador de la tarjeta, tales como nombre, dirección y otras informaciones que puedan ser necesarias. Se denomina “zona de nombre y dirección”. Los datos que figuran en esta zona de la tarjeta u obtenidos por impresiones a partir de la misma mediante calco o copia son normalmente destinados a la lectura humana solamente.

Línea de “ número de identificación”: Debe disponerse en una sola línea de espacio necesario para incluir caracteres el tipo especificado en ISO 7811/1, comprendido en número máximo de 19 posiciones de caracteres con un espaciado nominal de 7 por pulgada, dependiendo del número de posiciones utilizadas (estampadas) de las condiciones de aplicación.

Advierte la norma que cuando se prevea un nuevo sistema es aconsejable la mayor flexibilidad posible en el empleo de esta línea, como por ejemplo justificar el número de identificación estampado a la izquierda; dejar espacio para un número de identificación de longitud máxima; si una posición está disponible, se recomienda insertar un espacio entre la

identificación del emisor y el identificador de la cuenta individual del número de identificación. Si no se tiene en cuenta estas condiciones, puede ser necesario ponerse de acuerdo sobre ciertas limitaciones para que el intercambio de tarjetas y de datos entre diferentes sistemas pueda efectivamente tener lugar.

Las especificaciones referentes a las posiciones en la tarjeta pueden verse en la figura reproducida teniendo en cuenta que la distancia (A) será $21.42 + 0.12 \text{ mm}$ ($0.843 + 0.005 \text{ in}$); la distancia (B), $(10.18 + 0.25 \text{ mm})$ ($0.401 + 0.010 \text{ in}$); la tolerancia entre las líneas medianas del primero y último carácter de la línea es $+0.08 \text{ mm}$ ($+0.003 \text{ in}$).

- Zona de nombre y dirección: Dispone el espacio necesario para cuatro líneas de 27 caracteres cada una con espaciado nominal de 10 por pulgada el tipo especificado en ISO 7811/1. Todas las informaciones estampadas en la zona del nombre y de la dirección debe estar siempre lo más lejos posible del número de identificación. Advierte a los emisores de tarjetas que tengan necesidad de estampar las cuatro líneas del nombre y dirección que deben saber que los documentos obtenidos por máquinas de impresión y producidos con sus tarjetas pueden no ser aceptables en las condiciones de intercambio en razón de la exigencia de una zona en blanco OCR sobre ciertos tipos de aparatos de lectura OCR. Las especificaciones de posición (véase figura) son para la altura máxima (D) 14.53 mm (0.572 in), referida la superficie a imprimir sin incluir tolerancias; el margen inferior (E) estará a 2.41 mm min., y 3.30 mm máx. (0.095 y 0.130 in), debiendo tener en cuenta que cuando exista banda magnética en la tarjeta, el margen mínimo deberá ser de 2.54 mm (0.110 in). La distancia (F) será de $7.65 + 0.25 \text{ mm}$ ($0.301 + 0.010 \text{ in}$). El primer carácter en la zona de nombre y dirección es necesario que esté justificado a la izquierda.

No obstante, el empleo de 27 posiciones de caracteres está basado sobre una distancia de 7.65 mm al borde como se ha indicado.

Finalmente la tolerancia (g) acumulativa máxima entre las líneas medianas del primero y del último carácter de cada línea será de $+0.08 \text{ mm}$ ($+0.003 \text{ in}$).

v. Sistema de numeración y procedimiento de registro para los identificadores del emisor de tarjetas de transacciones financieras; tarjetas de crédito y de identificación para transacciones financieras, evolución de las características físicas y normalización; técnicas de registro magnético en tarjetas de identificación para transacciones financieras.

Técnicas de registro magnético en tarjetas de identificación para transacciones financieras.

Están también normalizadas las características de la banda magnética sobre las tarjetas de identificación, así como las técnicas de codificación

y los juegos de caracteres codificados, cuyo registro magnético está destinado a su lectura por máquinas, encontrándose estas especificaciones en la norma ISO 7811/2:1985, que examinamos a continuación en los aspectos esenciales:

Definiciones aplicables: La norma establece que a efectos de la misma la definición de “tarjeta de identificación” es aplicable la dada en ISO 7810.

Establece como “referencia de amplitud para ordenador” guardado en depósitos en la Oficina Nacional de normas de los Estados Unidos (NBS). La relación entre el patrón primario y la banda de referencia SRM 3200 es dada por el certificado producido por la NBS con la banda. También define como “tarjeta de referencia”, que considera como una referencia secundaria una tarjeta de identificación con una pista magnética de la referencia secundaria (referencia de amplitud para ordenador) SRM, indicando que estas tarjetas pueden ser solicitadas a Physikalisch - Technische Bundesanstalt, lab.1.41 – Bundesallee 100, D-3.300 Braunschweig, Allemagne, R.F., en cuanto existan disponibles.

Contiene también las siguientes definiciones que delimitan las características técnicas del registro magnético: “transición de flujo”: posición del máximo de amplitud de la componente magnética; “corriente de referencia/R,” amplitud mínima de la corriente de registro (onda cuadrada) que provoca, en las condiciones de ensayo dadas una amplitud de tensión de relectura sobre la tarjeta de referencia igual al 80% de la amplitud máxima, a la densidad de 8 ftpmm (transacciones de flujo por milímetros) (200 ftpi, esto es, transiciones de flujo por pulgada); “corrientes de registro de ensayo”; dos corrientes de ensayo (onda cuadrada) al 350% y 500% de la corriente de referencia (/R) deben utilizarse; “amplitud media de la señal : tensión de relectura medida de cresta a cresta, de la que se ha tomado la media sobre la zona de registro de una tarjeta, cuando se la registra con la corriente de registro de ensayo a la densidad especificada; “amplitud de la señal de referencia”, amplitud máxima de la señal de la tarjeta de referencia corregida por comparación con el patrón primario; “amplitud de señal individual” amplitud cresta a cresta de una sola señal de tensión de relectura; “densidad de ensayo”: densidades de ensayo 8 ftpmm (200 ftpi) y 20 ftpmm (500 ftpi) pueden utilizar para los ensayos.

Características físicas de las tarjetas. Son especificadas en la norma 7810.

Características físicas del material magnético. La “altura” (o espesor) de la superficie de lectura sobre la superficie posterior de la tarjeta, al ser perfilada con un estilete en un radio de 0.38 mm (0.015 in) y 2.54 (0.100 in) será de 0 mm como mínimo y de 0.038 mm (0.0015 in) como máximo; “rugosidad de la superficie”: la irregularidad media del nivel

de la superficie de la lectura no debe exceder de 0.404 mm (15.9 in) la media de la línea central(CLA) tanto en sentido longitudinal como transversal, utilizando una longitud de onda crítica de 0.25 mm (80.01 in) máximo de radio; el “perfil de la superficie” de la banda magnética, cuando es el medio paralelamente al ancho de la tarjeta con una sonda de un radio de 0.38 mm (0.015 in) a 2.54 mm (0.100 in) no debe mostrar una desviación vertical por comparación con una línea derecha de un lado a otro de la anchura mínima de la banda, que sobrepase 3.8 mm (150 in) para cada porción de banda de 2.54 mm (0.100 in) de ancho.

Características de funcionamiento del material magnético para las tarjetas de identificación recientemente fabricadas. Para pistas 1,2,3, las medidas que siguen deben ser hechas utilizando el mismo dispositivo y las condiciones: “amplitud de la señal”: cuando el material magnético provisto de su revestimiento protector es registrado con las corrientes de registro de ensayo, vistas anteriormente, la amplitud de la señal debe estar situada entre el 80% y el 130% de la amplitud de la señal de referencia y se añaden otras precisiones y resultados de estos ensayos; el “borrado” del material magnético debe poder realizarse con una corriente continua de escritura igual al 350% de/R con un nivel de 3% o menos de la amplitud de la señal de referencia; otras especificaciones son el ambiente en el que se realizan ensayos y las características de la cabeza de la lectura que deben tener un entrehierro de 0.025 mm (0.001 in) o menos.

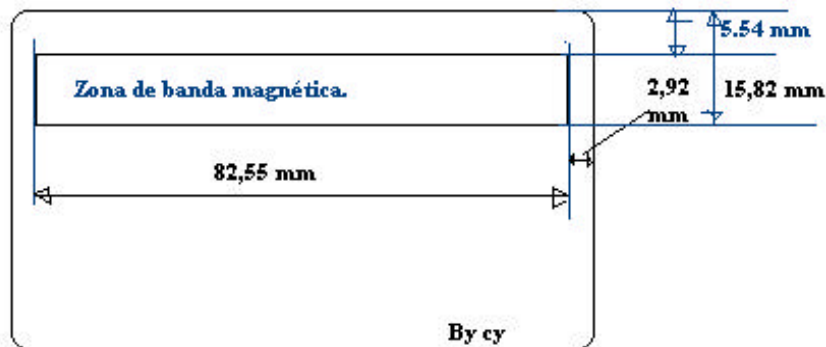
Técnica de codificación magnética. Es conocida bajo el nombre de grabación de fase coherente, a dos frecuencias. Este método permite la grabación en serie de datos autosincronizados en cada pista (véase la figura). El conjunto de las informaciones comprenden a la vez los datos y las señales del reloj (para la sincronización). Una transición de flujo entre dos señales consecutivas de reloj significan un “uno”, mientras que la ausencia de la transición de flujo magnético significa 0. Los datos han de ser registrados como una secuencia sincronizada de caracteres, sin espacios intermedios.

Especificaciones de la codificación. Se especifica un “ángulo de grabación”, indicando que el ángulo de registro debe de ser perpendicular al borde mas proximo de la tarjeta, paralelo a la banda magnética, con las siguientes tolerancias: siendo b/mm = bits por milímetro y b/p = bits por pulgada, para pista de lectura con 3 b/mm (75 b/p)(Pista 2).

Especificaciones de codificación de la pista alfanumérica de solo lectura, pista 1. La “densidad de elementos binarios” nominal de señales registrada debe de ser 8,3 elementos binarios por milímetro (210 elementos binarios por pulgada) +5%, en el caso de una medida afectada a lo largo de una línea paralela a la línea de medida

longitudinal de la pista. El espacio entre des transiciones de flujo adyacentes debe de ser de $0,121 + 0,006$ mm ($4762 + 238$ in) +5% para un “cero” y de $0,06 + 0,004$ mm ($2381 + 167$ in) + 7% para “uno”.

Aquí llevais las posiciones de la banda magnetica en las Credit de tipo ID-1 para las pistas 1,2 y 3.



Bueno con esta información creo que hay suficiente de todos modos si a alguien le falta algo mas que me mande un mail pidiendo datos..... que quede claro que ha sido tecleado integramente por Cy y NaT de CyberHack e integramente investigado por Cy... así que despues nadie se marque el moco.....

Si quieres mas info: Cyberhackcy@geocities.com

Bueno que quede claro que esto es con propositos educacionales y en ningun momento con fines delictivos. La pusta en marcha de algunos de estos conocimientos puede ser hecho constitutivo de delito. Y Cy no se responsabiliza de nada de esto ☺ Cy ☺

Bueno espero que haya mas colaboración en los proximos numeros... porque a mi no me cuesta trabajo mandarlo todo a tomar por el puto culo, porque yo seguiré teniendo la info, y si colaborais vosotros no la tendreis porque no habrá puta revista así que menos coña a los mierdas que solo critican...

Bueno pues nos vemos en el nº 5.

Un saludo:

Cy of CyberHack



Saludos a: Freezer, Angelipas, Daemon, Raptor, Wildraf, Alvarito, AJMS, EMF, WAREZZMAN, Islatortuga, eljaker, Marietta, NaT, Makinero, Binaria, y a todos los que siempre se olvidan pero están ahí....