**Logo**

* **Código de Comando (ocupa 2 bytes e índica que se quiere hacer, en este caso el valor KQ indica que se quiere validar el ARQC o generar él ARPC):** KQ
* **Modo (ocupa 1 byte)**: Tiene 3 valores posibles:

0: Sólo validar ARQC

1: Válidar ARQC y generar ARPC

2: Sólo generar ARPC

* **Identificador del esquema EMV (ocupa 2 bytes):** Tiene 3 valores posibles:

0: VISA

1: MASTERCARD

2: AMERICAN EXPRESS

* **MK-AC**: Es el criptograma que se usa para el cálculo del ARPC, a nosotros el banco nos ha suministrado el siguiente para Mastercard:

UBF00ACCCC75A445F4E4676347537973D

* **PAN/PAN Sequence No:** Este campo es de 8 byte, y está formado por el número de tarjeta empaquetada excluyendo la primeras posición + 1 byte del PSN (campo 23 de la red)

EJEMPLO = 1309151253750800

* **ATC**. **Application Transaction Number**

Ocupa 2 BYTE, y corresponde con el TAG 9F36 del chip (campo DE055 de la red)

* **UN. Unpredictable Number**

Ocupa 4 BYTE Es el Unpredictable Number, para Visa se informara con ceros binarios (00000000), para Mastercard es el tag 9F37 del campo DE055 .

Ejemplo = CEB4FBA6

* **Transaction Data Length**

Es la longitud del mensaje que se va a utilizar, se expresa en hexadecimal. Por ejemplo si el mensaje tiene 40 bytes de longitud, el valor en este campo sería 28

* **Transaction Data**

Es el mensaje que se va a utilizar para cifrar, está compuesto por algunos de los TAG del campo 55 que envía la red.

Ejemplo = 0000000050000000000000000724000000C000084011052300CEB4FBA67C00010003A0A002000000

Se detalla los campos que componen el mensaje:

TAG 9F02 (Amount Authorized)            000000005000

TAG 9F03 (Amount other)    000000000000

TAG 9F1A (Terminal Country Code)         0724

TAG 95 (Terminal Verification Result) 000000C000

TAG 5F2A (Transaction Currency Code)   0840

TAG 9A (Transaction Date)                   110523

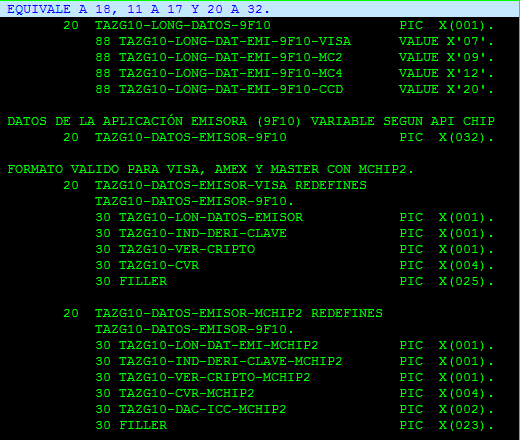
TAG 9C Transaction Type   00

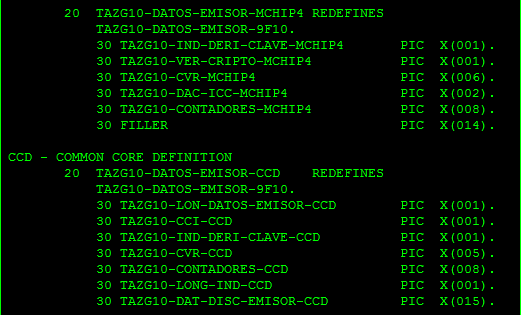
TAG 9F37 (Unpredictable Number)   CEB4FBA6

TAG 82(Application Interchange Profile) 7C00

TAG 9F36 (Application Transaction Counter)  0100

CVR (Card Verification Result). Es uno de los subcampos del TAG 9F10, este campo en función de la versión del chip puede ocupar más o menos bytes y empezar en una u otra posición, depende de la longitud del tag 9F10, a continuación se listan las posibles longitudes que pueden venir en el TAG 9F10 y los diferentes formatos del TAG 9F10 y donde está el CVR:





COUNTERS: Se informara con el campo subcampo COUNTERS del TAG 9F10 .Solo se informara si el CVN es ’11’ o ‘15’. El CVN es el subcampo del TAG 9F10 que va antes del CVR.

Padeo: En el caso que la longitud del mensaje no sea múltiple de 8, se debe padear a la derecha hasta que su longitud múltiple de 8, por ejemplo si el mensaje ocupa 42 bytes se deberá padear hasta que ocupe 48 posiciones, el padeo se realizará de la siguiente forma:

-VISA = Se padeará con ceros binarios

-Mastercard: El primer byte será 80 y el resto ceros binarios

* **Delimiter:** Valor fijo ‘;’
* **ARQC:**TAG 9F26 del campo 55 de la red
* **ARC Es el código de respuesta generado utilizado para calcular el ARPC, ocupa 2 bytes y solo se debe informar cuando se quiera generar el ARPC, sus valores son los siguientes**
  + MCHIP/4:
    - Si la operación está autorizada se informará con el valor hexadecimal ‘0012’
    - Si la operación está denegada se informará con el valor hexadecimal ‘0000’
  + Si no es MCHIP/4:
    - Si la operación está autorizada se informará con el valor hexadecimal ‘3030’
    - Si la operación está denegada se informará con el valor hexadecimal ‘3035’
* ARPC: En el caso en el que se haya solicitado generar el ARPC el comando criptográfico nos devolverá el ARPC que ocupa 8 posiciones, y que debe informarse en la respuesta a las franquicias (VISA, MASTERCARD, CREDICARD) en el TAG 91 del campo DE055