

Comandos de la Tarjeta Inteligente C3M2K (1)

Manejo de Claves

INSTRUCCIÓN	CODE	CLA	INS	P1	P2	P3	DATA*
LEER N° SERIE	21	00	54	00	00	08	
PRESENTAR MAESTRA	A1	00	48	CRIP	00	08	00 00 00 00 00 00 00 00
CREAR CLAVE	A1	00	40	MAX	N° CL	08	XX XX XX XX XX XX XX XX
PRESENTAR CLAVE	A1	00	42	CRIP	N° CL	08	XX XX XX XX XX XX XX XX
CAMBIAR CLAVE	A1	00	44	00	N° CL	08	XX XX XX XX XX XX XX XX
ESTADO CLAVE	21	00	C2	N° CL	00	02	
REACTIVAR PIN	A1	00	4C	CRIP	00	08	VALOR CLAVE MAESTRA

Manejo de Ficheros Ordinarios

INSTRUCCIÓN	CODE	CLA	INS	P1	P2	P3	DATA*
CREAR FICHERO	A1	00	E0	NOM	RA1	02	NN LL
SELECCIONAR FICHERO	21	00	E4	NOM	TIPO	00	
ESCRIBIR FICHERO	A1	00	C4	N° RG	OFF	NUM	XX XX . . . XX XX
LEER FICHERO	21	00	C6	N° RG	OFF	NUM	

Interpretación de Códigos

CRIP	La información se envía cifrada (NO --> 00, SI -> 01).
MAX	Número máximo de errores en la presentación de una clave.
N° CL	Número de la clave secreta, comprendido entre 00 y 0F (PIN --> N° CL = 00).
XX	Valor hexadecimal.
NOM	Nombre del fichero.
RA1	Protección de acceso (RA1 = XY --> X protección de lectura , Y protección de escritura). Si X (Y) es igual a Z, y su descomposición en bits es Z = OKPB entonces B bloquea la operación , P requiere el PIN , K requiere maestra , O requiere PIN o maestra. La prioridad de estos bits es B > P > K > O.
NN	Número de registros del fichero.
LL	Tamaño de un registro.
TIPO	Tipo del fichero (Ordinario --> 00, Monedero --> 0F, Protegido --> FF).
N° RG	Número del registro a acceder (N° RG > 00).
OFF	Desplazamiento dentro del registro.
NUM	Número de bytes a leer o escribir (NUM > 00).

Comandos de la Tarjeta Inteligente C3M2K (2)

Manejo de Ficheros Monedero/Protegido

INSTRUCCIÓN	CODE	CLA	INS	P1	P2	P3	DATA *
CREAR MONEDERO	A1	00	E8	NOM	00	08	RA1 RA2 RA3 06 03 SC1_2
CREAR PROTEGIDO	A1	00	E8	NOM	00	08	RA1 RA2 RA3 NN LL SC1_2
SELECCIONAR FICHERO	21	00	E4	NOM	TIPO	00	
ESCRIBIR FICHERO	A1	00	C4	Nº RG	OFF	NUM	XX XX XX XX
LEER FICHERO	21	00	C6	Nº RG	OFF	NUM	
LEER MONEDERO	21	00	30	00	00	06	
CRÉDITO	A1	00	32	00	00	03	CCCCCC
DÉBITO	A1	00	34	00	00	03	CCCCCC
CERTIFICADO CRÉDITO	A1	00	36	00	00	14	CC CC CC NT NT NT CT CT CT
CERTIFICADO DÉBITO	A1	00	38	00	00	14	CC CC CC NT NT NT

Interpretación de Códigos

CRIP	La información se envía cifrada (NO --> 00, SI -> 01).
XX	Valor hexadecimal.
NOM	Nombre del fichero.
RA1	Protección de acceso (RA1 = XY --> X protección de lectura , Y protección de escritura). Si X (Y) es igual a Z, y su descomposición en bits es Z = OKPB entonces B bloquea la operación , P requiere el PIN , K requiere maestra , O requiere PIN o maestra. La prioridad de estos bits es B > P > K > O.
RA2	Como RA1, pero X es igual a O-SC1-SC2-B, donde SC1 y SC2 se refieren a las claves. Además, en los ficheros monedero X protege el crédito e Y protege el débito.
RA3	Reservado su uso en el algoritmo DES.
SC1_2	Identifica el valor de las claves asociadas a SC1 y SC2. Si SC1_2 = XY entonces SC1 se refiere a la clave X y SC2 a la clave Y.
NN	Número de registros del fichero.
LL	Tamaño de un registro.
Nº RG	Número del registro a acceder (Nº RG > 00).
OFF	Desplazamiento dentro del registro.
NUM	Número de bytes a leer o escribir (NUM > 00).
CC	Valor hexadecimal que conforma una cantidad de 3 bytes
NT	Valor hexadecimal que conforma un número de transacción de 3 bytes
CT	Valor hexadecimal que conforma un certificado de 3 bytes