Definición de un sistema de ficheros de usuario para pruebas de la ACOS3
tiene 32 k de eeprom

PERSONALIZACION FILE (FF02) DE LOS FICHEROS INTERNOS
PERSONALIZATION FILE RECORD 1

HABRIA QUE PONER := 07 14 08 00

BYTE 1: OPTION REGISTER:

00000111 := 07

INQ_AUT=0 (INQ ACCOUNT REQUIRE AUTHENTIFICATION)
TRNS_AUT=0 (ACCOUNT TRANSACTION REQUIRE AUTHENTIFICATION)
REV_DEB=0 (REVOQUE DEB COMAND)
DEB_PIN=0 (PIN SUBMITTED FOR DEBIT COMAND)
DEB_MAC=0 (DEBIT TRANSACTION AUTHENTICATED BY MAC)
PIN_ALT=1 SE PUEDE CAMBIAR EL PIN CON EL COMANDO DE CAMBIO DE PIN)
3DES=1 (SE SE CIFRA SE HACEN CON DES)
ACCOUNT=1 (SE UTILIZA LA CUENTA)

BYTE 2: SECURITY OPTION REGISTER

00010100 := 14

IC_DES=0 (CUANDO SE ENVIE EL IC NO DEBE IR CIFRADO CON DES)
PIN_DES=0 (CUANDO SE ENVIE EL PIN NO DEBE IR CIFRADO CON DES)
AC5_DES=0 (CUANDO SE ENVIE AC5 NO DEBE IR CIFRADO CON DES)
AC4_DES=1 (CUANDO SE ENVIE AC4 DEBE IR CIFRADO CON DES)
AC3_DES=0 (CUANDO SE ENVIE AC3 NO DEBE IR CIFRADO CON DES)
AC2_DES=1 (CUANDO SE ENVIE AC2 DEBE IR CIFRADO CON DES)
AC1_DES=0 (cUANDO SE ENVIE AC1 NO DEBE IR CIFRADO CON DES)
NO IMPORTA=0

BYTE 3: N_OF_FILE

N_OF_FILE := 08 (SE VAN A CREAR OCHO FICHEROS DE USUARIO)

BYTE 4: PERSONALIZATION BYTE: NO SE PONE TOCA := 00 (NO SE ACTIVA EL BIT DE PERSONALIZACION)

PERSONALIZATION FILE RECORD 2: NO SE TOCA.

SECURETY FILE (FF03) DE LOS FICHEROS INTERNOS
SECURETY FILE:

RECORD 00: IC := 41 43 4F 53 54 45 53 54 (ISSUER CODE NO SE MODIFICA: ACOTEST EN ASCII)
RECORD 01: PIN := 30 31 32 33 34 35 36 37 (01234567 EN ASCII)
RECORD 02: Kc := DD DC DF DD DC DF DD DC (CLAVE DES DE LA TARJETA)
RECORD 03: Kt := 00 01 02 03 04 05 06 07 (CLAVE DES DEL TERMINAL)
RECORD 04: RNDc:= AB 8A 7C 6D 2D 88 81 18 (SEMILLA PARA AEATORIOS)
RECORD 05: AC1 := AC 11 AC 11 AC 11 AC 11 (AC1)

RECORD 06:  AC2 := AC 22 AC 22 AC 22 AC 22  (AC2)
RECORD 07:  AC3 := AC 33 AC 33 AC 33 AC 33  (AC3)
RECORD 08:  AC4 := AC 44 AC 44 AC 44 AC 44  (AC4)
RECORD 09:  AC5 := AC 55 AC 55 AC 55 AC 55  (AC5)
RECORD 0A:  NO SE TOCA
RECORD 0B:  NO SE TOCA
RECORD 0C:  Kc(RIGHT HALF):= DD DC DF DD DC DF DD DC  (MITAD DERECHA DE LA CLAVE DE LA TARJETA CUANDO SE USE 3DES)
RECORD 0D:  Kt(RIGHT HALF):= 00 01 02 03 04 05 06 07  (MITAD DERECHA DE LA CLAVE DEL TERMINAL CUANDO SE USE 3DES)

USER FILE MANAGEMENT FILE (FF04) DE LOS FICHEROS INTERNOS

8 RECORDS PUES SE DEFINEN 8 FICHEROS

Se definirá un primer fichero TRANSPARENTE DE  256 bytes  EC01
NO SE PRECISA NADA PARA LEERLO O ESCRIBIR.
ACCESO LIBRE READ AND WRITE. SECURETY ATTRIBUTE:= 00

RECORD 00:  01 00 00 00 EC 01 80  (FILE LENGTH HIGH BYTE := 01, FILE LENGTH LOW BYTE := 00,
READ SECURETY ATTRIBUTE := 00 WRITE SECURETY ATTRIBUTE := 00
FILE IDENTIFIER := EC01, FILE ACCES FLAGS := 80  (BINARIO SIN SECURE MESSAGING)

Se definirá un segundo fichero TRANSPARENTE DE 256 BYTES EC02
PARA LEERLO O ESCRIBIR ES PRECISO PRESENTAR AC2
ACCESO PRESENTAR AC2. SECURETY ATTRIBUTE:= 04

RECORD 01: 01 00 04 04 EC 02 80

Se definirá un tercer fichero transparente de 512 bytes EC03
PARA LEERLO O ESCRIBIRLO ES PRECISO PRESENTAR EL PIN
ACCESO PRESENTAR EL PIN. SECURETY ATTRIBUTE:= 40
SERÁ PRECISO USAR SECURE MESSAGING LEER Y ESCRIBIR. IMPLICA FILE ACCES FLAGS:= E0 (BINARIO CON SECURE MESSAGING)

RECORD 02: 02 00 40 40 EC 03 E0

Se definirá un cuarto fichero transparente de 1024 bytes EC04
PARA LEER O ESCRIBIR ES PRECISO PRESENTAR O AC1 Ó AC3 Ó AC5
ACCESO PRESENTAR AC1 Ó AC3 Ó AC5  SECURETY ATTRIBUTE:= 2A

RECORD 03: 04 00 2A 2A EC 04 80 (BINARIO)

Se definirá un primer fichero tipo RECORD DE 16 records de 8 bytes cada record EC05

NO SE PRECISA NADA PARA LEEOR O ESCRIBIR.
ACCESO LIBRE  SA:= 00

RECORD 04:  08 10 00 00 EC 05 00 (RECORD LENGTH :=08, NUMBER OF RECORDS := 10 (16 EN DECIMAL),
READ SECURETY ATTRIBUE := 00, WRITE SECURETY ATTRIBUTE := 00,
FILE IDENTIFIER := EC 05, FILE ACCES FLAGS := 00 (RECORD)

Se definirá un segundo fichero tipo RECORD de  16 records de 16 bytes cada record EC06
PARA LEERLO O ESCRIBIRLO ES PRECISO PRESENTAR EL PIN
ACCESO PRESENTAR EL PIN. SECURETY ATTRIBUTE:= 40
SERÁ PRECISO USAR SECURE MESSAGING LEER Y ESCRIBIR. IMPLICA FILE ACCES FLAGS:= 60 (RECORD CON SECURE MESSAGING)

RECORD 05:  10 10 40 40 EC 06 60

Se definirá un tercer fichero tipo RECORD de 255 records de 16 bytes cada record EC07

PARA LEERLO O ESCRIBIR ES PRECISO PRESENTAR AC4
ACCESO PRESENTAR AC4. SECURETY ATTRIBUTE:= 10

RECORD 06: 10 FF 10 10 EC 07 00

Se definirá un cuarto fichero tipo record de 255 records de 32 bytes cada record EC08

PARA LEERLO O ESCRIBIRLO ES PRECISO PRESENTAR EL PIN
ACCESO PRESENTAR EL PIN. SECURETY ATTRIBUTE:= 40
SERÁ PRECISO USAR SECURE MESSAGING LEER Y ESCRIBIR. IMPLICA FILE ACCES FLAGS:= 60 (RECORD CON SECURE MESSAGING)

RECORD 07: 20 FF 40 40 EC 08 60