****
Guía para programar la autenticacion en la tarjeta ACOS3.
****

Suponemos que la tarjeta está configurada para utilizar 3DES.

* LA SECUENCIA ES LA SIGUIENTE
* TERMINAL------------>TARJETA
*
* START SESSION----->
* <------RNDC
* AUTHENTICATE------>
* GET RESPONSE------>
* <------3DES(RNDT, KS)
* EL TERMINAL VERIFICA QUE 3DES(RNDT,KS) AL DESCIFRARLO COINCIDE CON RNDT
* EL TERMINAL Y LA TARJETA CALCULAN UNA CLAVE COMÚN DE SESION KS
* KS = DES[DES(RNDC, desKC) ORX RNDT, desKT] EN EL CSO DE DES
* KSL = 3DES[3DES (RNDC, desKC), desKT]MITAD IZQUIERDA EN EL CASO DE 3DES
* KSR = 3DES(RNDT, revKT) MITAD DERECHA EN EL CASO DE 3DES
* revKT es la clave del terminal con las mitades derecha e izquierda cambiadas

Observar que después de que el TERMINAL envía la APDU AUTHENTICATE
LA TARJETA NO RESPONDE CON DATOS. Para obtener la respuesta de la tarjeta hay que enviarle una APDU GET RESPONSE a la que la tarjeta responde con DES(RNDT, KS).
Todos los cifrados del proceso de autenticación Mutua se realizan con 3DES modo ECB, pues las longitudes de los datos a cifrar son siempre de 8 bytes.

A continuación una traza de un proceso de autenticación:
_____

T --> C:: 80 84 00 00 08   (APDU START SESSION)
C --> T:: A9 55 20 47 F0 AA 55 87 (Aleatorio de la tarjeta RNDC)

(Aleatorio del Terminal:: RNDT = F9 54 05 97 0F 1B 0B 85)
(Se calcula 3DES(RNDC,KT) = 85 1F AF 31 BA B9 4B 5A y se concatena con RNDT)

T --> C:: 80 82 00 00 85 1F AF 31 BA B9 4B 5A F9 54 05 97 0F 1B 0B 85
(es la APDU authenticate)

T --> C:: 80 C0 00 00 08   (APDU GET RESPONSE)

C --> T:: 14 C8 1E EF 9F DA E2 8D
(Lo que devuelve la tarjeta y 9000 detrás)

Al calcular las claves de sesión, sale:
Clave de sesion L, KSL = 5F A8 6A 8B 02 60 2D EA
Clave de sesion R, KSR = C0 FD BD 4C 01 A7 3E 5E

En el terminal para poder usar esta clave hay que meterla en un objeto clave de sesión, por ejemplo así:

```
      var desKS = new Key();
      desKS.setComponent(Key.DES, KSL.concat(KSR));
```

Al descifrar en el terminal, con la clave KS,
el string: 14 C8 1E EF 9F DA E2 8D
obtiene   F9 54 05 97 0F 1B 0B 85
que coincide con el aleatorio que él generó al principio.

Esto le permite al terminal dar por terminada CON EXITO la autenticación.

**********SUERTE**********