Guía para programar la escritura en un fichero en la tarjeta ACOS3 UTILIZANDO SECURE MESSAGING, es decir: cifrando el envío desde el terminal a la tarjeta.
****

Esto es lo que el manual de la tarjeta se denomina:
ISO-IN (pág 36 del manual de la ACOS3)

****

Pista o truco:
Se puede escribir o leer con Secure Messaging en un fichero, incluso si no tiene puesto los correspondientes flags en su record de definición. Los flags; si se ponen, obligan a usar Secure Messaging, pero si no se ponen no lo impiden.
Por tanto para probar será conveniente hacerlo en un fichero que no tenga ninguna restricción de acceso.
Escribiremos en él con Secure Messaging y podremos leer de él libremente(sin Secure Messaging) para comprobar que la escritura ha funcionado.
Si esto fuese un desarrollo real, por supuesto que habría que poner los flags de Secure Messaging para impedir que se leyera o se escribiera de otra forma.
****

Se trata de escribir en un fichero de la tarjeta un mensaje de longitud menor o igual a 240 bytes.

Suponemos que la tarjeta está configurada para utilizar 3DES.

Hay que realizar la Autenticacion Mutua con éxito, calcular la clave de sesión KS.
Poner la clave de sesión en un objeto para poder utilizarla.

A la tarjeta hay que enviarle una APDU como la siguiente:

CLA*	INS	P1	P2	P3*	87H	L87	Pi	Encripted data	8EH	04H	MAC

CLA* = 8C, el CLA de la apdu de escritura es 80 modificado para secure messaging es 80H ORX 0CH = 8CH.

INS es D0, es la instrucción para escribir en un fichero binario. Si fuese escribir en un fichero de records la instrucción sería D2.

P1, P2 son los bytes de la posición del fichero donde se va a escribir, parte High y Low respectivamente es decir si vamos a escribir desde la posición 0000H del fichero P1=00 y P2=00. Si fueramos a escribir a partir de la posición 0129H P1=01H y P2=20H.

P3* Es igual a 3 + n* +2 +4 donde n* es igual a: la longitud de datos a escribir en el fichero incluyendo el

relleno hasta múltiplo de ocho. Al utilizar sendApdu con el eclipse, este parámetro (P3*) se calcula solo.

El string | 87H | L87 | Pi | Encripted data | es una TLV donde 87H significa indicador de padding seguido de datos cifrados, L87 es la longitud de datos que es la longitud de Encripted data más uno (la longitud de Pi).
Encripted data es el mensaje cifrado con CBC, con vector de inicialización IV.
IV se calcula haciéndole un AND lógico bit a bit al RNDC (el aleatorio de la tarjeta) con el byteString: 00 00 00 00 00 00 FF FF. Al resultante se le incrementa en uno para obtener IV.
Pi es el número de bytes de relleno al cifrar el mensaje a escribir en el fichero. Hay que calcularlo y ponerlo aquí.

El string | 8EH | 04H | MAC| es otra TLV donde 8EH significa Cryptographic Checksum o MAC que es lo mismo.

Para calcular el MAC hay que efectuar las siguientes operaciones:

Se generan las siguientes TLV's concatenadas:

| 89H | 04H | CLA* | INS | P1 | P2 | 87H | L87 | Pi| Encripted data (con padding)|

La primera TLV (| 89H | 04H | CLA* | INS | P1 | P2 |) tiene de etiqueta 89H, que significa command header.

La segunda TLV (| 87H | L87 | Pi| Encripted data(con el padding incorporado)|) ya se cálculo y explicó antes para la APDU.

Ahora hay que cifrar estas dos TLV's concatenadas (rellenando con padding), con 3DES y con el modo CBC, con la clave de sesión KS, y con el mismo IV descrito antes.

El resultado de este cifrado será un string de gran longitud. Nos fijaremos en el último octeto de ese string.
Si a ese string lo llamamos "todocifrado": El último octeto se obtiene, en eclipse, con la instrucción: octetoparamac = todocifrado.right(8); Supongamos que es: F9 54 05 97 0F 1B 0B 85 El MAC que buscamos son los 4 bytes más a la izquierda de estos 8 bytes. Sería: F9 54 05 97 se puede obtener, en eclipse, con la intrucción: MAC = octetoparamac.left(4);

Estos 4 bytes son el MAC que hay que enviarle a la tarjeta en la APDU de envío con secure messaging.

****
*
*
**Resumiendo y escribiendo la secuencia de pasos quedaría así: *
*
*
****

Paso 1) Realizar la AUTENTICACIÓN MUTUA con éxito para obtener una clave de sesión KS.
Paso 2) Cifrar el mensaje a enviar con padding (relleno): pad(Crypto.ISO9797_METHOD_2, true).
Paso 3) Calcular cuantos bytes de relleno se han producido, porque lo necesitamos despues (Pi).
Paso 4) Calcular el vector de inicialización a partir del random de la card.
Paso 5) Formar las TLV's concatenadas y rellenar para calcular el MAC.
Recomiendo formar las TLV's por concatenación de variables. No usar las instruccuiones de TLV que proporciona el pluging del eclipse pues están normalizadas para tarjetas bancarias y difieren ligeramente de éstas.
Paso 6) Calcular el MAC.
Paso 7) Formar la APDU a enviar a la tarjeta.
Paso 8) Con la apdu SELECT FILE apuntar al fichero al que queremos escribir.
Paso 9) Enviar la APDU

Si todo ha ido bien la tarjeta devolverá 9000H.
Si devuelve 6882H ("SECURE MESSAGING NOT ALLOWED") mirar en el fichero a ver si ha escrito. En mi caso una vez me salió ese mensaje y todo funcionaba perfectamente y escribió en el fichero.

Paso 9) Pedirle a la tarjeta GET RESPONSE con longitud 0CH, con la APDU: 80 C0 00 00 0C.
La apdu GET RESPONSE debe ir obligatoriamente inmediatamente después (no se puede enviar ninguna apdu entremedias) del envío de la apdu donde se envían los datos cifrados.

La tarjeta responderá con:

99H	02H	Sw1Sw2	8EH	04H	MAC	9000H

Son dos TLV's concatenadas:

La primera TLV: 99H es la etiqueta de la respuesta del comando (en este caso la respuesta de la escritura en disco).

02H es la longitud

Sw1Sw2 es la respuesta del comando de escritura en disco = 9000H si todo ha ido bien.

La segunda TLV: 8EH es la etiqueta de crytographic checksum, 04H es la longitud, MAC es el checksum calculado por la tarjeta y 9000H significa todo OK.

El programador del terminal debería verificar este checksum (el MAC) que envía la tarjeta.

Este MAC se ha obtenido cifrando dos TLV's concatenadas.

89H	04H	CLA*	INS	P1	P2	99	02	SW1	SW2

La tarjeta ha hecho padding para llegar a 16 bytes.

Se ha cifrado con CBC, con la clave de sesión (KS) y con vector de inicialización IV+1.

Los cuatro octetos más a la izquierda del resultado del cifrado es el MAC devuelto.

Ver página 37 del manual.

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