

ANEXO A - Proceso de personalización de la tarjeta inteligente

En base al manual de referencia de la tarjeta inteligente ACOS2 de la compañía Advanced Card Systems Ltd. (ACS, 2000), se detalla a continuación el procedimiento para llevar a cabo la personalización de estas tarjetas para su aplicación en el sistema de almacenamiento y recuperación de expediente curriculares electrónicos, sistema propuesto en este trabajo.

El ciclo de vida de las tarjetas ACOS2 consta de cuatro etapas, como se muestra en la figura A1. Estas van desde su fabricación hasta la etapa donde el usuario final las utiliza en su operación normal.

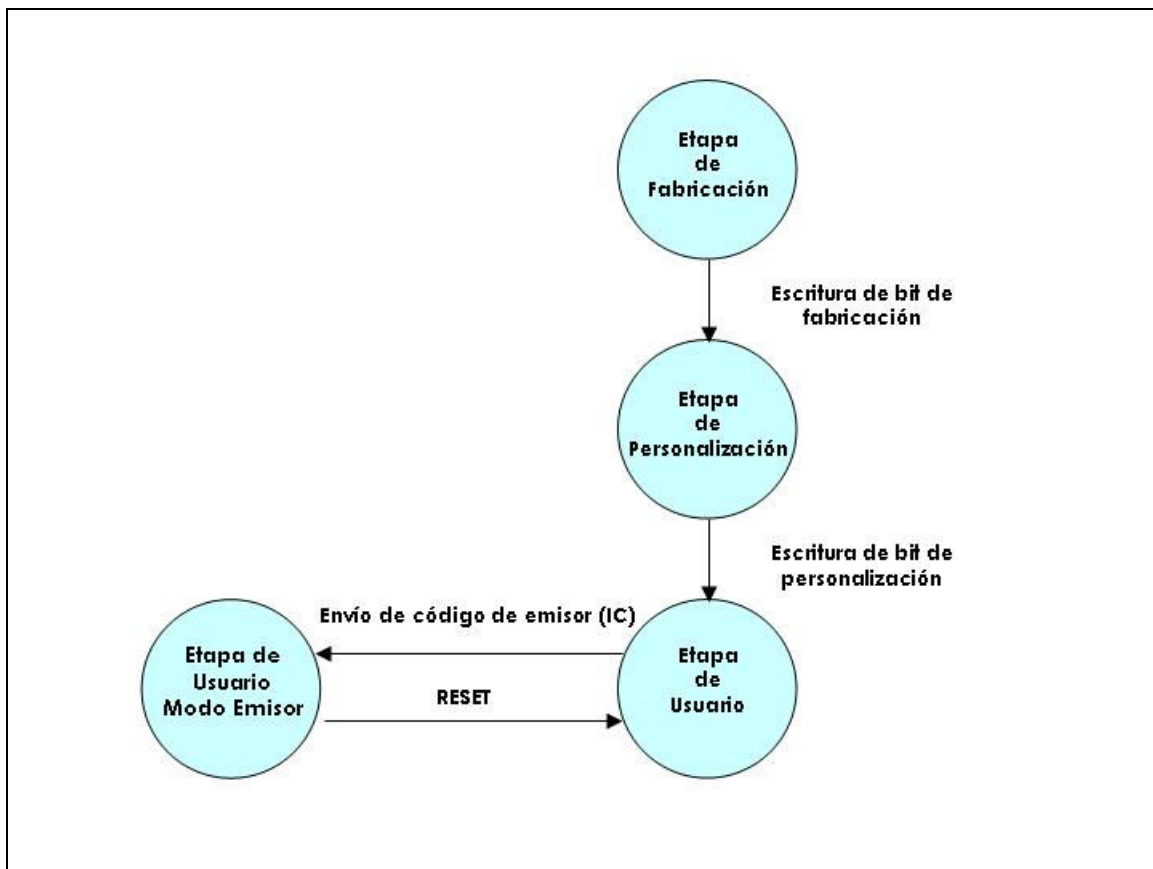


Figura A1 – Etapas del ciclo de vida de la tarjeta inteligente ACOS2

La tarjeta siempre se encuentra en alguna de estas cuatro etapas y su cambio a otra etapa depende de si se escriben ciertos bits en los registros internos de la tarjeta. Las etapas se detallan a continuación:

1. Etapa de fabricación. Esta etapa es efectiva desde el momento de la fabricación del chip de la tarjeta hasta que se realice la escritura de cierto bit de un registro interno de la tarjeta (llamado “fusible de fabricación”), el cual determina el cambio a la siguiente etapa. Durante esta etapa se programa en la tarjeta la siguiente información que quedará almacenada de manera definitiva y que determinará varios aspectos del funcionamiento de la misma:

- a. Identificador del fabricante** – Es un número de 8 bytes que representa información sobre el fabricante así como la versión de la tarjeta.
- b. Número de serie.** Es un número de 8 bytes el cual es único para cada tarjeta.
- c. Código del emisor de la tarjeta (IC code)** - Es un número de 8 bytes proporcionado por el fabricante, el cual se utilizará para tener acceso a personalizar la tarjeta.

2. Etapa de personalización. Esta etapa comienza en el momento en que se escribe cierto bit durante la etapa de fabricación. Una vez llegada a esta etapa, no se puede volver a la etapa de fabricación. Esta es la etapa que le corresponde programar en la tarjeta a los desarrolladores de la aplicación, ya que es aquí donde se personaliza. Durante esta etapa se escriben los siguientes elementos en la tarjeta:

- a. Códigos de Aplicación (ACs).** Son 5 números de 8 bytes de longitud cada uno, los cuales serán utilizados para proporcionar privilegios de acceso de lectura y escritura de los archivos de usuario de la tarjeta. Las aplicaciones hacen uso de estos códigos para poder leer o escribir en los archivos de la tarjeta. Los códigos pueden ser introducidos por la aplicación en forma

normal o encriptada, dependiendo de la configuración previa en la tarjeta.

- b. Llaves de Encriptación.** Es un par de llaves que se utilizan para el proceso de autenticación mutua, en el cual tanto la tarjeta como la aplicación verifican que su respectiva contraparte sea genuina. Estas llaves pueden tener una longitud de 8 o 16 bytes, dependiendo si utilizan el proceso de encriptación del tipo DES o 3-DES, el cual se especifica durante esta misma etapa.
- c. Clave PIN.** Es una cadena de 8 bytes que se utiliza para controlar los derechos de lectura y escritura de los archivos de usuario de la tarjeta, tal como sucede con los 5 códigos de aplicación (ACs). La diferencia radica en que los ACs no pueden ser modificados una vez programados, en cambio la clave PIN puede ser cambiada por el usuario durante el uso normal de la tarjeta. Esta funciona como un mecanismo de identificación de usuario, en donde el usuario introduce un número que se sabe de memoria, el cual está almacenado en la tarjeta, comprobando de esta manera que es el dueño de la tarjeta. El número es verificado por la tarjeta para proveer privilegios ya sea de lectura o escritura de los archivos.
- d. Bloques de Definición de Archivos.** Son registros que definen la manera en que estarán organizados los archivos de usuario. Cada archivo de usuario se asocia a uno de estos bloques de configuración. Aquí se especifican parámetros como la cantidad de registros por archivo, la longitud de los registros, atributos de lectura, atributos de escritura e identificadores de archivos.
- e. Otros datos** – Se almacenan otros datos específicos a la tarjeta, como velocidad de transmisión, identificador del emisor de tarjetas, tipo de encriptación, etc.

- 3. Etapa de usuario.** Esta etapa designa el modo normal operacional de la tarjeta. Esta etapa es efectiva una vez finalizada la configuración de la etapa de personalización. En esta etapa ya no se puede volver a 2 anteriores, pero si se puede pasar a la etapa del emisor de tarjeta si se introduce el código de emisor (IC), el cual debe estar solamente en manos de este y no del usuario final.

- 4. Etapa de usuario – Modo del Emisor.** Esta etapa es similar a la etapa de usuario, con la única diferencia de que cuenta con privilegios para acceder a ciertas áreas de la memoria que no pueden ser accedidas en la etapa del usuario.

Una vez conocido el ciclo de vida de la tarjeta inteligente ACOS2, podemos determinar como llevar a cabo el proceso de programación y personalización de la tarjeta para la aplicación.

Debido a que cada tarjeta es entregada por el fabricante con un código de emisor (IC), el cual fue almacenado previamente en la etapa de fabricación como se mencionó anteriormente, se deben tomar las medidas necesarias para evitar que estos códigos sean utilizados por personas ajenas al departamento que se encarga de este proceso de personalización. Lo más indicado sería contar con una terminal o consola con privilegios de acceso a la base de datos de la entidad certificadora para acceder a información de los usuarios para el cual se expedirá la tarjeta. Con esta información en mano se puede empezar a realizar la “personalización” de la tarjeta

Basándonos en lo mencionado anteriormente, se puede definir los pasos que se deben seguir en el proceso de personalización. Tal proceso lo llevará a cabo el personal encargado de emitir las tarjetas a los usuarios. Estas personas recibirán las tarjetas en blanco directamente del fabricante o proveedor, con su respectiva clave de emisor (IC) y serán quienes tendrán privilegios de acceso al sistema para realizar tal proceso.

A continuación se presentan una serie de pasos que se han definido para llevar a cabo la personalización de la tarjeta inteligente.

1. El usuario emisor de tarjetas (aquel que se encarga de programarlas) se autentica en el sistema para obtener privilegios de acceso a la información de los usuarios, así como para programar las tarjetas. Este paso es crítico y se debe contar con un buen esquema de seguridad, ya que si alguna otra persona logra tener acceso a estas opciones del sistema, pudiera programar nuevas tarjetas poniendo en riesgo la seguridad del sistema en general. Lo recomendable para realizar este proceso en forma segura, es contar con una aplicación cliente que se encuentre en la misma red local del servidor de aplicaciones de la entidad certificadora.
2. El usuario emisor extrae del sistema una relación de usuarios nuevos que acaban de registrarse para obtener su tarjeta. Entre esta lista de usuarios también pueden encontrarse aquellos que perdieron su tarjeta y la reportaron o que tuvieron algún otro problema que implicó darle de baja la tarjeta actual. Esta relación de usuarios se puede utilizar para realizar el proceso de impresión que incluye el logotipo del sistema, su profesión, nombre completo, fecha de emisión, e información adicional que se requiera tener impresa en ella.
3. Una vez que las tarjetas estén impresas, el usuario emisor hace una búsqueda del usuario final en la base de datos y selecciona la opción de programar una nueva tarjeta. Esto lo hará con cada nueva tarjeta. El sistema debe estar validado para comprobar que no se ha expedido previamente otra tarjeta para el mismo usuario. Esto con la finalidad de asegurarse de que no existan tarjetas duplicadas. De lo contrario, dos o más personas pudieran identificarse con tarjetas idénticas. Este punto crítico se puede comparar a la problemática que surgiría en un banco si se expedieran tarjetas duplicadas. El usuario pudiera de alguna manera conseguir la clave PIN de la persona y lograr extraer dinero de los cajeros o realizar otras transacciones. De manera similar, si se duplica una tarjeta curricular, otra persona pudiera identificarse en establecimientos afiliados, y en el peor de los casos, al adivinar o robar la clave PIN, pudiera otorgar acceso al expediente curricular o realizar cambios en el mismo.

4. Una vez seleccionado al usuario de la tarjeta, se procede a seleccionar la opción de programar la tarjeta. Durante este proceso, la aplicación del sistema genera en forma aleatoria las llaves de autenticación mutua y los códigos de aplicación (AC) que se almacenarán en la tarjeta y en el sistema. Este proceso de almacenamiento de llaves y códigos se realiza en forma automática sin que ni siquiera el usuario emisor tenga acceso a ellas. A su vez, se genera en forma aleatoria el número de identificación personal (PIN) el cual podrá ser cambiado posteriormente por el usuario final. Este número no se almacena en el sistema, solamente en la tarjeta, ya que funciona como mecanismo para identificar al usuario portador de la tarjeta. Posterior a esto, la aplicación procede a programar la tarjeta para que esta pase a la etapa de usuario final y no se pueda volver a personalizar. A partir de este paso, tanto las llaves de autenticación mutua, como los códigos de aplicación de esta tarjeta en específico, no deben volver a transferirse, sino solamente quedar almacenados en ella y en la base de datos del servidor de la unidad certificadora. Como se verá más adelante, para el proceso de autenticación mutua, las llaves almacenadas nunca salen de la tarjeta, sino que se emplea un mecanismo de comprobación de llaves por medio de envío de mensajes aleatorios. Los códigos de aplicación (ACs) tampoco se expondrán durante la operación normal de la tarjeta (por ejemplo, al realizar una consulta del expediente curricular) debido a que estos códigos viajarán en forma cifrada utilizando llaves de encriptación distintas para cada sesión.

5. En este momento la tarjeta ya está relacionada con el usuario en específico. El siguiente paso consiste en almacenarle los datos personales, lo cual lo realiza la misma persona. Esto lo hace autenticándose al sistema usando la tarjeta inteligente e introduciendo la clave PIN. Este proceso le sirve también para comprobar si la tarjeta quedó programada correctamente. Una vez que el sistema identifica al usuario, el emisor selecciona la opción de actualizar los datos personales y estos se almacenan en la tarjeta.

6. Una vez personalizada la tarjeta, esta debe entregársele al usuario final junto con la clave PIN en un sobre a prueba de alteraciones, tal como lo realizan los bancos cuando entregan tarjetas de crédito a sus cuenta habientes. De esta manera se puede comprobar si el PIN fue leído por otra persona, y tomar las medidas necesarias en caso de que esto ocurra (por ejemplo, cancelar la tarjeta y entregarle otra). El portador de la tarjeta (usuario final) debe acudir a una oficina de la entidad certificadora para que por medio de la tarjeta inteligente le almacenen en el sistema sus documentos probatorios, los cuales forman parte de su expediente curricular.