

**NUEVAS TECNOLOGÍAS
APLICADAS A LA GESTIÓN (E66)
5º INGENIERÍA EN INFORMÁTICA**

Tema 5.

Estructura Lógica de la Memoria.

- 1.- Introducción.
- 2.- Estructura Lógica según ISO 7816/3.
 - 2.1.- Memoria Volátil.
 - 2.2.- Memoria No Volátil.
- 3.- Estructura Lógica según ISO 7816/4.
 - 3.1.- Jerarquía de Memoria.
 - 3.2.- Estructuras de Ficheros.
 - 3.3.- Tipos de Accesos.
 - 3.4.- Conclusiones.

(Capítulo 5 del Zoreda)

(Capítulo 5 del Rankl)

INTRODUCCIÓN

Planteamiento

- La estructura lógica de la memoria se define a partir de las características de su sistema operativo.
- La evolución de éstos ha variado el modo en el que se gestionan los datos en la memoria.
- Inicialmente se hizo diseñaron una serie de zonas cuya funcionalidad era definida en el estándar 7816/3.
- Por su parte, el tamaño era variable en función del fabricante y tamaño real de la tarjeta.
- La evolución de los sistemas operativos y el aumento de la capacidad de las tarjetas, dio pie a un replanteamiento de esta filosofía.
- En el estándar 7816/4 se definió un sistema de memoria jerárquico similar a los de los sistemas operativos más comunes, DOS y UNIX.
- Este sistema se compone de tres tipos de ficheros diferentes: los ficheros, los directorios y el directorio raíz.
- Cada uno de ellos puede tener una regla de acceso distinta, lo que da a una versatilidad mayor en el control de acceso a los datos.
- Este estándar también permitió definir ficheros de tipos diferentes, que cubrían los distintos modos de manejar los datos en memoria.

ESTRUCTURA EN ESTÁNDAR 7816/3

Memoria Volátil

- La memoria volátil se sitúa físicamente sobre la memoria RAM de la tarjeta.
- Esta memoria contiene datos intermedios y datos que son requeridos por el procesador.
- Esta memoria se suele dividir en las zonas que se mencionan a continuación,
 - Zona de Registros, que emulan los registros de un procesador.
 - Pila del Sistema, similar a la existente en todo sistema informático.
 - Variables Generales, en donde se pueden almacenar los descriptores de los ficheros a acceder y otros tipos de variables.
 - Buffer de Entrada/Salida, utilizado en las operaciones de comunicación, desde y hacia la tarjeta.
 - Zona de Trabajo para Cifrado, en donde se almacenan los resultados intermedios que se obtienen en el cifrado de información.
- En algún caso, el tamaño prefijado para cada una de las zonas puede ser insuficiente, en cuyo caso puede ser necesario habilitar parte de la memoria EEPROM para simular RAM.
- La velocidad de acceso y la limitación en el número de escrituras de la EEPROM aconseja limitar al máximo estas soluciones.

ESTRUCTURA EN ESTÁNDAR 7816/3

Memoria No Volátil

- La memoria no volátil aparece físicamente sobre memoria EPROM y EEPROM, estructurada como sigue,
 - Aparecen varias zonas, cuyo tamaño puede ser variable, según las características de la tarjeta.
 - Cada una de ellas se compone de uno o más ficheros.
 - Los ficheros se dividen en registros.
 - Y los registros son de 1 o más bytes.
- Seguidamente se describe la funcionalidad y tamaño de estas zonas en una tarjeta de 2 Kb.
- Zona del Fabricante (16 bytes), que se suele grabar en el proceso de fabricación.
- La información presente suele ser,
 - Número de Serie de la Tarjeta (8 bytes).
 - Modelo del Circuito y Versión del Sistema Operativo (8 bytes).
- La lectura de esta zona no tiene ningún control de acceso, mientras que su escritura está prohibida.

ESTRUCTURA EN ESTÁNDAR 7816/3

Memoria No Volátil

- Zona Confidencial (72 bytes), en donde se almacena los códigos secretos de la tarjeta
 - Clave del Fabricante.
 - Número de Identificación Personal (PIN).
 - Dos Claves del Usuario.

y los datos necesarios para el cifrado de los datos.

- Cada código secreto se asocia con un fichero de 16 bytes, dividido en dos registros,
 - El primer registro de 8 bytes contiene los parámetros asociado a ese código.
 - Número Máximo de Accesos Permitidos.
 - Número Máximo de Accesos Fallidos Permitidos.
 - Si esta clave puede ser modificada por el usuario.
 - Por su parte, el segundo registro contiene una versión cifrada de la clave.
- Los datos necesarios para el cifrado aparecen en los últimos 8 bytes de la zona.
- Si el algoritmo de cifrado utilizado es DES, este espacio es utilizado para almacenar su clave secreta.

JERARQUÍA EN ESTÁNDAR 7816/4

Tipos de Ficheros

- La jerarquía de memoria que se describe en este estándar es similar a la existente en los sistemas operativos más comunes.
- Aparecen tres tipos de ficheros,
 - Fichero Maestro (MF), que es el directorio raíz del sistema de ficheros.
 - Ficheros Dedicados (DF), cuya función es similar a la de los directorios de un sistema operativo clásico.
 - Ficheros Elementales (EF), que son los ficheros en los que aparece la información.
 - Ficheros Internos (IF), que almacenan datos que son requeridos por el sistema operativo o para la ejecución de una aplicación.
- En el interior del MF y de los DFs, aparecen DFs, EFs y IFs
- Debido a la baja capacidad de las tarjetas, lo más habitual es definir un único nivel en la jerarquía de directorios.
- Si la tarjeta sólo soporta una aplicación, sus EFs pueden situarse bajo el MF o en un DF.
- Para tarjetas multifuncionales, cada aplicación sitúa sus EFs bajo un DF.
- En función del estándar, los IFs pueden tratarse como ficheros invisibles, estándar ISO, o como ficheros normales, en el Instituto de Estándares de Telecomunicación Europeos.

JERARQUÍA EN ESTÁNDAR 7816/4

Nombre de los Ficheros

- En los primeros sistemas operativos. los ficheros se direccionan a través de su posición física dentro de la memoria de la tarjeta.
- En la actualidad, el acceso a los ficheros sigue una metodología orientada a objetos.
- Como consecuencia de ello, los ficheros se deben seleccionar antes de poder accederse a la información que contienen.
- Esto infiere una división de los ficheros en dos partes bien diferenciadas,
 - Cabecera, en donde se describe tanto la estructura del fichero como las condiciones de acceso al fichero.
 - Cuerpo, en donde se almacena realmente la información del fichero.
- Para acceder al cuerpo de un fichero se debe acceder a su cabecera en donde aparece un puntero a la posición de inicio de los datos.
- Normalmente estas dos partes aparecen en zonas de memoria diferentes, que posibilita un mayor nivel de seguridad a nivel física.
- Con ello se consigue que un error de borrado o de escritura en el cuerpo, altere el contenido de la cabecera.

JERARQUÍA EN ESTÁNDAR 7816/4

Nombre de los Ficheros

- Los diferentes elementos definidos en este estándar se pueden seleccionar lógicamente, mediante la utilización de dos conceptos.
- El primero es el Identificador de Fichero (FID), que tiene un tamaño de 2 bytes, que se utiliza para seleccionar un fichero.
- Existe una Versión Reducida del FID que sólo ocupa 5 bits.
- En el estándar ISO se definen dos valores que aparecen reservados,
 - El MF siempre toma el valor 3F00.
 - El valor FFFF se reserva para uso futuro.
- Además, en las aplicaciones GSM se debe cumplir que,
 - Los EFs del MF tienen un FID con valor 2FXX.
 - El FID de los EFs de los DF tienen el valor 6FXX.
- Para evitar la existencia de cualquier conflicto de acceso a un fichero por el uso del FID se resuelve, del modo siguiente,
 - Los EFs dentro de un MF o un DF no pueden tener el mismo FID.
 - Directorios anidados no pueden tener el mismo FID.
 - Un EF no puede tener el mismo FID que el DF o MF que lo contiene, ni el de un DF situado en su nivel.

JERARQUÍA EN ESTÁNDAR 7816/4

Nombre de los Ficheros

- El manejo de 2 bytes puede ser insuficiente para la selección de ficheros.
- Por esta razón, se ha definido el Identificador de Aplicación (AID) asociado a un DF, y que tiene una longitud de 5 a 16 bytes.
- El AID se compone de dos partes,
 - Identificador de Registro (RID) de 5 bytes.
 - Extensión de Identificación de la Aplicación Propietaria (PIX), cuya longitud puede llegar a los 11 bytes.
- El RID es asignado por una oficina nacional o internacional, en la que aparece,
 - Código del País.
 - Categoría de la Aplicación.
 - Número de Identificación del Proveedor.
- Esta secuencia numérica asegura la unicidad del RID.
- La existencia del PIX es opcional, y en el suele aparecer un número de serie o un número de versión.
- El valor del PIX suele ser utilizado con un fin administrativo.

JERARQUÍA EN ESTÁNDAR 7816/4

Direccionamiento de los Ficheros

- Como se ha comentado con anterioridad, el FID no es único dentro de la jerarquía, aunque si es necesario cumplir ciertas reglas.
- Por lo tanto no es posible direccionar de un modo directo un fichero.
- Los MF y los DF si pueden ser seleccionados directamente del modo siguiente,
 - Dado que el MF posee un FID que es único, éste puede ser utilizado para seleccionarlo.
 - Los DF se pueden seleccionar mediante su AID que también es único.
- El uso del FID se puede utilizar para seleccionar los DFs y los EFs.
- Existen dos posibilidades,
 - Uso de la versión de 2 bytes, que permite la selección de un fichero dentro de un ámbito.
 - La utilización de la versión reducida que sólo permite seleccionar un EF en un DF o MF.
- El segundo permite utilizar una única instrucción para seleccionar y acceder a un EF.
- En el primer caso se puede indicar el camino desde el MF o desde la posición actual.
- Para evitar la ambigüedad, desde la posición actual, sólo se permite el acceso a ciertas zonas.

ESTRUCTURAS DE FICHEROS EN 7816/4

Ficheros Elementales

- Los ficheros de un sistema operativo suelen tener una única estructura.
- En las tarjetas inteligente este planteamiento varía, definiéndose diferentes tipos de ficheros, en función de la estructura interna que poseen.
- De este modo se facilita el manejo del usuario, ya que permite la definición de estructuras de datos que puedan ser accedidos de un modo rápido y sencillo.
- Pero el tamaño de los programas de gestión de estos ficheros es mayor.
- Es por ello, que sólo se definen las estructuras de ficheros más utilizadas.
- Seguidamente se describen las estructuras de ficheros siguientes,
 - Ficheros Transparentes.
 - Ficheros Lineales de Tamaño Fijo.
 - Ficheros Lineales de Tamaño Variable.
 - Ficheros Cíclicos.
 - Ficheros Ejecutables.

ESTRUCTURAS DE FICHEROS EN 7816/4

Ficheros Transparentes

- Estos ficheros también se denominan como ficheros binarios o ficheros con estructura amorfa.
- Estos ficheros no poseen una estructura interna definida.
- Dado que no poseen una estructura definida, las operaciones de lectura y escritura se basan en dos parámetros,
 - Desplazamiento, que define la distancia desde el principio del fichero en donde se va a realizar la operación.
 - Tamaño, en el que se indica el número de bytes a leer o escribir.
- Las instrucciones asociadas utilizan 1 byte para el desplazamiento y 2 bytes para el tamaño.
- Este tipo de ficheros se utilizan para almacenar datos muy cortos, que pueden ser de 1 byte, y sin estructura, como una foto digitalizada.
- También se pueden utilizar para almacenar datos estructurados cuya estructura aparece descrita en el propio fichero.
- Pero en este caso, se complica el acceso a los datos por parte del terminal, ya que ésta se define a partir de la información que aparece en el fichero.

ESTRUCTURAS DE FICHEROS EN 7816/4

Ficheros Lineales de Longitud Fija

- Estos ficheros están compuestos de registros de tamaño fijo.
- El rango de tamaños válidos es 1-254 bytes.
- El número de registros en un fichero varía de 1 a 254, que se nombran en formato hexadecimal.
- En ambos casos, el tamaño 255 se reserva para uso futuro.
- Sobre estos ficheros se realizan operaciones sobre registros completos, siendo imposible la selección de una parte de un registro.
- Por lo tanto, las operaciones deben indicar sobre que registro van a operar, o también un desplazamiento de registros en el fichero.

Ficheros Lineales de Longitud Variable

- El manejo del fichero, así como los rangos en el tamaño y número de registros, coinciden con los ficheros lineales de longitud fija.
- Pero en este caso, no todos los registros tienen el mismo tamaño.
- De este modo, se ajusta el tamaño del registro al tamaño de los datos, pudiendo reducir el espacio ocupado en memoria.
- Pero cada registro debe contener un campo adicional en el que se almacene el número de bytes del registro.

ESTRUCTURAS DE FICHEROS EN 7816/4

Ficheros Cíclicos

- Estos ficheros también están compuestos de registros de tamaño fijo.
- La principal diferencia con los ficheros de longitud fija reside en el modo de nombrar a sus registros,
 - El último registro escrito es el registro 1.
 - El siguiente registro es el registro 2.
 - El registro anterior al registro 1 es el último registro del fichero.
- Por lo que respecta al manejo del fichero, sus operaciones también se realizan a nivel de registros.
- Una posible aplicación es como ficheros de protocolo en tarjetas inteligentes, de modo que la última entrada borre la más antigua.

Ficheros Ejecutables

- Realmente, este tipo de ficheros se pueden definir como un subconjunto de los ficheros transparentes.
- Su única diferencia estriba en su contenido, ya que en este caso contiene código que puede ser ejecutado por el procesador de la tarjeta.
- Su uso se debe realizar de modo controlado, ya que es posible introducir un código que sea un "caballo de Troya" en el que se accedan a zonas reservadas de la tarjeta.

ESTRUCTURAS DE FICHEROS EN 7816/4

Atributos de los Ficheros

- Además de la estructura de fichero, también es posible definir una serie de atributos que modifican el manejo de los EF.
- La mayoría de estos atributos explotan las características de la EEPROM.
- El primer atributo se conoce como WORM (Write Once Read Many), implementado vía hardware o vía software.
- Mediante este atributo se intenta proteger aquellos datos que no deben ser modificados, como el número de serie de la tarjeta.
- También es posible definir los Ficheros de Múltiples Escritura, en donde es posible aumentar el número de escritura en la EEPROM.
- Se puede desarrollar de dos modos diferentes,
 - Escribiendo los datos en más de un fichero.
 - Escribiendo de modo alternativo en ficheros diferentes.
- Para proteger los ficheros ante la aparición de errores se pueden introducir Técnicas de Corrección y Detección de Errores.
- Estos errores tienen gran importancia en los ficheros monedero.
- También es posible incluir un mecanismo de Recuperación de Errores, que permite eliminar la existencia de datos erróneos en el fichero.

TIPOS DE ACCESO EN 7816/4

Planteamiento

- El tipo de acceso permitido para un fichero se define cuando éste es creado, y se almacena en su cabecera.
- El control de acceso a aplicar es diferente para los diferentes tipos de ficheros.
- El control en el MF y los DF se refiere al manejo de la jerarquía de ficheros, es decir, el borrado y la creación de ficheros.
- Por su parte, el control en los EF se refiere a los datos que aparecen en ellos, es decir, se centra en la lectura y escritura de información.
- El tipo de control de acceso difiere entre los diferentes sistemas operativos, pudiéndose definir dos tipos diferentes,
 - Control por Niveles de Prioridad.
 - Control sobre las Instrucciones.
- En el primer caso, un usuario puede realizar una operación sobre un fichero, si se encuentra en el nivel o niveles de prioridad autorizados.
- Dichos niveles son definidos dentro del sistema operativo.
- Para el segundo caso, se deben de definir las instrucciones que deben ser ejecutadas antes de posibilitar la realización de una operación en un fichero.
- Las instrucciones más comunes son las relativas a la comprobación de una o más claves.

ESTANDAR ISO 7816/4

Conclusiones

- Por todo lo dicho, cuando se crea un fichero resulta necesario especificar las siguientes informaciones,
 - Nombre del Fichero. El FID del fichero, más el AID si el fichero es DF.
 - Tipo del Fichero, que puede ser MF, DF, EF.
 - Estructura del Fichero.
 - Atributos del Fichero.
 - Tamaño del Fichero. Para ficheros lineales de tamaño fijo se debe indicar el tamaño y número de los registros.
 - Condiciones de Acceso.
 - Conexión en la Jerarquía de Fichero. Indica el directorio donde se sitúa el fichero.
- Todas estas informaciones aparecen en la cabecera del fichero.
- En la mayoría de tarjetas, la creación de los ficheros sólo es posible cuando se personaliza la tarjeta.
- Posteriormente el usuario no puede crear o borrar ficheros.
- De este modo se reduce la complejidad del gestor de ficheros, ya que no debe realizar una gestión de la memoria liberada.