

QONTINUUM

BOLETIN TECNICO DE PRODUCTO

Código: BTP021
Título: CONACC: Soportes 'tarjeta-chip 7816'
Revisión: D1
Fecha: 25-6-2006
Indice:

<u>CAPITULO</u>	<u>PAG.</u>
1 INTRODUCCION	3
2 LAS TARJETAS	5
3 LOS EMISORES	7
4 LAS POSIBILIDADES DE USO	11
5 LOS REQUERIMIENTOS	13
6 LOS INSTRUMENTOS	15
7 LA PUESTA EN MARCHA	19
8 EL FUTURO	23
9 RESUMEN	25

Observaciones:

Como norma general de interpretación de este documento, toda palabra, acrónimo o frase realizada en **negrilla** que no esté subrayada tiene su explicación en el capítulo GLOSARIO DE TERMINOS de este documento y/o de otro cuando así se indique, mientras que las palabras, acrónimos o frases que se inicien o se escriban totalmente con mayúsculas o entre apóstrofes hacen referencia a cosas o conceptos que se presume que son del conocimiento de los lectores a los que se dirige este documento (tanto por ser de uso común como por estar explicadas en el propio documento), quedando los entrecorillados como indicación de sentido virtual o de sentido circunstancial.

QONTINUUM PLUS, s.l. se reserva el derecho de modificar todas o cualquiera de las especificaciones que se indican en este documento sin previo aviso.

Tanto el contenido íntegro de este documento como los productos reales existentes y/o resultantes a los que se aluda constituyen una obra colectiva formada por las aportaciones de los técnicos asignados, directa o indirectamente, por QONTINUUM PLUS, s.l. a cada proyecto, siendo propiedad de QONTINUUM PLUS, s.l. los derechos de propiedad intelectual sobre los programas y los productos electrónicos realizados bajo la iniciativa y coordinación de ésta, de acuerdo con el artículo 8 de la Ley de Propiedad Intelectual.

R	FECHA	PAGINA/S	OBSERVACIONES
	22-10-1998	(total)	- 1ª edición
A	15-9-1999	(total)	- 2ª edición
B	31-8-2000	(total)	- 3ª edición
B1	19-8-2002	3 7-9 11-13 15-21 23-25	- correcciones y aclaraciones
C	20-11-2002	(total)	- 4ª edición (adaptación a la Revisión N de las especificaciones CONACC)
D	1-10-2005	(total)	- 5ª edición (introducción del nombre CPU para los Terminales de <i>Control de Accesos</i>)
D1	25-6-2006	1	- cambiado el título de "tarjetas 7816-4" a "Soportes 'tarjeta-chip 7816'"

1 INTRODUCCION

Toda palabra, acrónimo o frase realzada en negrilla que no esté subrayada tiene su explicación en el capítulo GLOSARIO DE TERMINOS del documento MRT019.

Por razones estrictamente comerciales, y a partir de la fecha de la Revisión D de este documento, los terminales para el *Control de Accesos* y los 'módulos Alfa' pasan a ser llamados CPU, de manera que también desaparece la clasificación existente hasta el momento de Terminales *Compactos*, Terminales *Kit-compactos* y Terminales *Modulares* para el *Control de Accesos*, aunque se mantiene la clasificación de Terminales *Portátiles* y Terminales *de Sobremesa*. De todos modos, y para evitar ambigüedades, se utilizará el nombre "Terminal" (entrecomillado) para hacer referencia a todos los elementos en conjunto (CPU y Cabezal) que se utilizan para controlar un punto de paso y tanto si el Cabezal es lector como si es lector/grabador como si es "en Kit", mientras que se seguirá usando el nombre Terminal para hacer referencia general a cualquier tipo de electrónica de control.

La evolución experimentada por las conocidas tarjetas bancarias de crédito o débito con la introducción de la tecnología "chip" (lo cual produce la llamada tarjeta microprocesada) ha supuesto un importante empuje a sus posibilidades de utilización en diferentes aplicaciones.

La amplia versatilidad de la tarjeta microprocesada dimana de su diseño: un circuito electrónico altamente integrado incrustado en una tarjeta de plástico del tamaño y grosor de una tarjeta de crédito o débito convencional (y por tanto cumpliendo con la norma ISO 7810). Tanto en sus orígenes (1974) como durante más de 15 años, fué el entorno financiero el objetivo deseado para el uso de las tarjetas microprocesadas. La frialdad general con que la banca acogió el tema convirtió a las tarjetas microprocesadas en la clásica "solución en busca de un problema", hasta que a principio de los 90 la situación empezó a cambiar dado que la tecnología había avanzado sustancialmente y, de manera especial, habían aparecido las normas internacionales que indicaban, si no el "donde", el "cuando" y el "porqué" de su utilización, si el "como".

Tan pronto como las Entidades Financieras constataron las ventajas que les podían aportar las tarjetas microprocesadas se lanzaron de manera más o menos masiva a preparar su intervención en un nuevo mercado que ahora aparecía mucho más claro: moneda única en Europa, lenta pero inexorable reducción de la banca directa en beneficio de la banca electrónica (especialmente las transacciones vía Internet), globalización mundial de los "monederos electrónicos" a instancias de Europay, Mastercard y Visa con la aparición de normas comunes (EMV 3.0), etc.

El interés que desde 1996 demuestran las Entidades Financieras para la popularización de las tarjetas microprocesadas es consecuencia de su permanente actitud ante el negocio que les es natural, de ahí su predisposición para patrocinar la implantación en colectivos que, por su tamaño, les aseguren el retorno de la inversión y un negocio atractivo en base a captar el máximo de pasivo y a formalizar otros acuerdos.

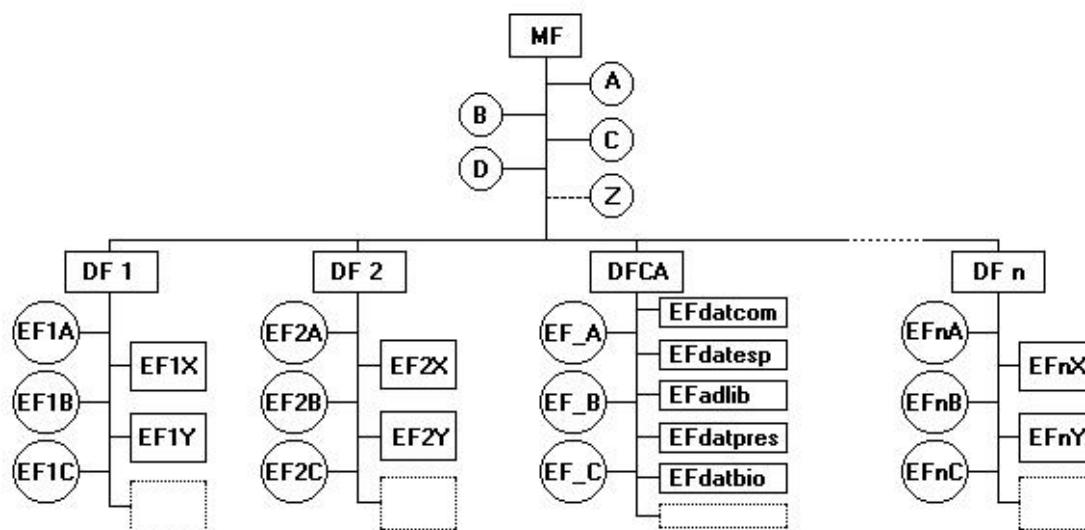
Para el sistema CONACC las tarjetas microprocesadas son aquellas que cumplen con las normas ISO/IEC 7816-1 a 7816-4 y el protocolo de comunicación es T=0. Tales tarjetas son referidas en toda la documentación CONACC como tarjetas 7816-4 o como tarjetas microprocesadas dotadas con estructura **fS=4** (ver el capítulo 4), mientras que, vulgarmente, también son conocidas como "tarjetas-chip", "tarjetas inteligentes" o, en razón de una de sus aplicaciones más conocidas, como "tarjetas monedero".

ESTA PAGINA HA SIDO DEJADA EN BLANCO INTENCIONADAMENTE

2 LAS TARJETAS

Dado que la tarjeta microprocesada es un elemento de fácil transporte, fácil de usar, que facilita la identificación personal y que facilita el uso masivo, ¿porqué no extender su abanico de facilidades fuera del entorno estrictamente financiero?. De la respuesta a la pregunta anterior nace el concepto de "multioperatividad". La tarjeta ya no es sólo un elemento para el crédito o el débito en determinadas aplicaciones de consumo o para la obtención directa de dinero en las máquinas dispensadoras (cajeros automáticos, etc.) sino que también es un "monedero electrónico" para los pequeños gastos (cabines telefónicas, transporte público, comedor de empresa, expendedores de todo tipo, etc.) y puede ser, también, la credencial que permita al usuario el acceso físico a determinados lugares generalmente restringidos y el acceso lógico a determinados recursos de suministro de información.

Para que la "multioperatividad" sea un hecho, las tarjetas han de disponer de un sistema operativo (conocido como "máscara") que permita la creación y el tratamiento de archivos de una manera tal que pueda existir una completa independencia entre las diferentes aplicaciones. En el siguiente esquema aparece una estructura de cuatro directorios que corresponden a otras tantas aplicaciones (el directorio DF1 podría corresponder a la aplicación de "monedero electrónico", el directorio DF2 a la aplicación de "monedero telefónico" y el directorio DF_n a una "aplicación Universitaria", mientras que el directorio DFCA corresponde a la aplicación CONACC para el Control de Accesos físicos):



El archivo MF (Master File) es la raíz del sistema de archivos y contiene información reservada del fabricante. Los archivos A, B, C, D ... Z (su número y contenido varían según la "máscara") contienen información sobre la tarjeta (por ejemplo su número de serie) y las claves de servicio necesarias para permitir la generación de los archivos DF (Dedicated File o Directory File) que, a su vez, engloban a los diferentes archivos EF (Elementary File) que son los que contienen a los datos pertenecientes a cada aplicación.

En el esquema anterior, los archivos esenciales que contienen a las claves administrativas o de gestión y a otros códigos (situados en el esquema a la izquierda en su árbol) son los necesarios para controlar el acceso a los archivos operativos que contienen a la información propia de la aplicación (situados en el esquema a la derecha en su árbol).

Aunque del planteamiento del esquema anterior se podría inferir que todos los archivos son accesibles dada su estructuración jerárquica, esto no es así. Dentro de cada directorio (normalmente cada aplicación ocupa un solo directorio) sólo tienen posibilidad de operar aquellos sistemas externos (Terminales de Control de Accesos, de Control de Presencia, máquinas de "vending", etc) que conozcan las claves administrativas o de gestión asignadas por el Emisor al directorio, de manera que la independencia entre aplicaciones está garantizada.

ESTA PAGINA HA SIDO DEJADA EN BLANCO INTENCIONADAMENTE

3 LOS EMISORES

En aquellas Instalaciones en las que se utilizan **Soportes** que no sean tarjetas-chip (por ejemplo, tarjetas de banda magnética, códigos de barras o 'tags' de proximidad vía radio) su emisión o creación la realiza, normalmente, el suministrador del sistema, aunque también puede ser realizada en la propia Instalación si se dispone de los medios adecuados (tales medios, más concretamente, consisten en grabadores y/o impresoras dotados con algún programa sencillo que permite la entrada de los datos y su serialización para que el **NIS** nunca se repita).

En el entorno de uso de las tarjetas microprocesadas reciben el nombre genérico de Emisores los organismos responsables de la definición de las claves lógicas que son necesarias para el tratamiento de las tarjetas (por extensión, también se asigna este nombre a los organismos que las emiten físicamente):

- si se trata de tarjetas microprocesadas no bancarias el Emisor puede ser la propia Instalación, en cuyo caso debe usar la CM⁽¹⁾ y definir la **CLAD** y el **CODSE** (en este caso el nombre del directorio DFCA consta predefinido en **TInACC**);
- si se trata de tarjetas microprocesadas bancarias el Emisor es una Entidad emisora especializada (Sistema 4B, CECA o Visa) que determina el nombre del directorio DFCA y define la **CLAD** y el **CODSE**.

Bajo el punto de vista de CONACC existen tres estados acumulativos (*Inicializada*, *Prepersonalizada* y *Personalizada*) en los que se puede encontrar una tarjeta microprocesada:

Inicializadas

Definición:

Son aquellas que han pasado por el proceso realizado por el Fabricante para generarles el archivo maestro (MF o "raiz") del que colgarán algunos archivos y otros directorios, entre ellos DFCA (ver el capítulo 2).

Circunstancias:

Las claves de servicio son las definidas por el Emisor y sólo afectan al MF, por lo que la tarjeta no es operativa para el Control de Accesos físicos.

Actores:

La *Inicialización* es responsabilidad exclusiva del Emisor.

Conclusión:

La *Inicialización* es una acción necesaria pero no suficiente para que una tarjeta microprocesada pueda ser integrada en cualquier aplicación (la estructura todavía no es **fS=4**).

Prepersonalizadas

Definición:

Son aquellas que, aunque contienen la estructura **fS=4**, sus archivos no disponen todavía de la información necesaria para que las tarjetas puedan operar.

Circunstancias:

A partir del archivo MF de cada tarjeta se ha creado el nuevo directorio (DFCA) con los archivos esenciales (EF_{KEY} , EF_{NT} y EF_{CODSE}) necesarios para la *Personalización* y con la estructura del archivo de **datos comunes** (EF_{DATCOM}) del usuario, la estructura del de **datos específicos** para el **centro operativo** primario (EF_{DATEP}) y la estructura del de **datos presencia** ($EF_{DATPRES}$). Con todo ello, la tarjeta queda directamente preparada para su uso en la Instalación (aunque sin contar todavía con el contenido del archivo de **datos específicos** y/o con el archivo de datos biométricos EF_{DATBIO}), los cuales no son imprescindibles para el funcionamiento de las tarjetas en un entorno de Control de Accesos físicos. La información básica para el Control de Accesos físicos está grabada en el archivo de **datos comunes** (EF_{DATCOM}), e incluye el **INST1**, el **NIS**, el **INST2** (contiene el nombre del archivo de **datos específicos**) y el **Perfil** del usuario. Mientras que el archivo de **datos comunes** es necesariamente único, puede haber un archivo de **datos específicos** para cada uno de los posibles **centros operativos** dentro del conjunto de la Instalación. Si no existen los antedichos archivos o el campo **INST1** no tiene información (valor nulo), se considerará que la tarjeta no esta *Prepersonalizada*.

Actores:

Normalmente, las tarjetas son *Prepersonalizadas* por el propio Emisor, pero también pueden serlo (de manera extraordinaria) por la propia Instalación, para lo cual el Emisor debería proporcionar un módulo SAM⁽²⁾. El nombre del directorio, los nombres de los archivos y las claves de acceso deben coincidir con los declarados en el iButton **TInCLA**.

Conclusión:

La *Prepersonalización* es una acción necesaria pero no suficiente para que una tarjeta microprocesada dotada con estructura **fS=4** pueda ser integrada en cualquier aplicación CONACC.

Personalizadas

Definición:

Son aquellas cuya estructura **fS=4** contiene información válida que define por completo a un usuario en la Instalación.

Circunstancias:

el archivo de **datos comunes** contiene toda la información operativa necesaria (**Perfil, NIS, Fecha Activación, Fecha Caducidad, PIN** y Control IDEP), mientras que el archivo de **datos específicos** contiene la suya (**Perfil y Niveles**). También puede haberse generado el archivo de datos libres y/o de datos biométricos.

Actores:

Las tarjetas son *Personalizadas* por el propio Emisor, mediante la información que le haya transferido la Instalación, o son *Personalizadas* por la propia Instalación utilizando los recursos CONACC implementados por el programa **OEM** (este caso es también conocido como "Personalización secundaria").

Conclusión:

La *Personalización* es la última acción (necesaria y suficiente) para que una tarjeta microprocesada dotada con estructura **fS=4** pueda ser integrada en cualquier aplicación CONACC.

NOTAS:

(1) La Clave Maestra es comunicada por el fabricante de las tarjetas al Emisor por medio de la llamada 'tarjeta de lote', siendo su finalidad la de permitir diversificar todas las demás claves.

(2) El módulo SAM (Secured Access Module) consiste en una electrónica controladora dotada con dos dispositivos para el procesado de tarjetas microprocesadas, de manera que en uno de ellos reside, de manera permanente, una tarjeta securizada que contiene las claves de servicio necesarias para poder derivar, desde el archivo MF de cada tarjeta introducida en el otro dispositivo, las claves que se asignarán para el tratamiento de los archivos del directorio DFCA, todos los cuales también son creados en este proceso en todas y cada una de las tarjetas que se presenten; como consecuencia se obtienen tarjetas *Prepersonalizadas* que deberán pasar por el programa **OEM** para quedar *Personalizadas* y ser, por tanto, finalmente operativas.

ESTA PAGINA HA SIDO DEJADA EN BLANCO INTENCIONADAMENTE

4 LAS POSIBILIDADES DE USO

Las tarjetas microprocesadas, dependiendo de como hayan sido emitidas, producen en la Instalación efectos distintos en cuanto se refiere a su uso para el control de accesos físicos, de manera que resulta fundamental conocer las posibilidades que son inherentes al tipo de emisión realizado.

Cuando las tarjetas son emitidas con (o acaban disponiendo de) la estructura definida por CONACC (el llamado **formato Soporte = 4**), presentan la posibilidad de uso al completo, en cuyo caso son referidas como *tarjetas microprocesadas dotadas con estructura fS=4* (aunque también como tarjetas 7816-4) en toda la documentación CONACC.

Cuando las tarjetas existen previamente y no disponen de la estructura definida por CONACC sólo presentan la posibilidad de uso degradado, lo cual las asimila a **Soportes** de "sólo lectura" (como son, por ejemplo, las tarjetas de banda magnética o de código de barras), en cuyo caso son referidas como tarjetas 7816 en toda la documentación CONACC.

4.1 uso al completo (fS=4)

Las tarjetas microprocesadas disponen de la estructura de archivos para el Control de Accesos especificada por CONACC, por lo cual tales tarjetas son tratadas (en el entorno CONACC) al completo de sus posibilidades y, por tanto, permiten desarrollar en la Instalación todo el potencial previsto:

- funcionamiento autónomo de los Terminales (ver el capítulo 1 del documento BTP027)
- posible utilización de **Lista_Blanca** (ver el capítulo 2.1.3 del documento BTP027)
- número ilimitado de usuarios controlados por **Lista_Negra** (ver el capítulo 2.2 del documento BTP027)
- actualización de datos, desatendida, en los archivos de las tarjetas (ver el capítulo 2.8 del documento BTP027)
- control anti **Pass-Back** interactivo entre los Terminales y las tarjetas (ver el capítulo 4 del documento BTP027)
- autenticación Biométrica
- facilidades para el Control de Presencia
- diferentes esquemas de permisos de acceso en diferentes edificios (fábricas, complejos, etc.) de una misma Instalación.

4.2 uso degradado (7816)

Debido al auge en la implantación de las tarjetas microprocesadas, hay entidades usuarias (como, por ejemplo, algunas Universidades) que disponen de ellas desde antes de que se hayan planteado sus propias necesidades operativas; se trata, por tanto, de tarjetas que disponen de todas las facilidades para su uso como "monedero electrónico" pero sin otras aplicaciones concretadas (a lo sumo disponen de algún directorio cuyos archivos son más para usos genéricos que, en la mayoría de los casos, para un buen control de los accesos físicos).

En esta situación acostumbran a darse las siguientes circunstancias:

- la entidad usuaria pretende un Control de Accesos físicos
- las tarjetas existen y (lo que es peor) están repartidas
- el Emisor bancario dice: "ahora es imposible rehacer las tarjetas, quizá más adelante cuando vayan caducando ...", o dice: "de acuerdo, pero quién asume el coste ..."
- la implantación de CONACC junto con la aplicación **OEM** le parece a la entidad usuaria la mejor solución, pero el resultado es la imposibilidad de hacerlo ante la carencia de información adecuada en las tarjetas (el directorio DFCA no existe).

Como consecuencia inmediata de tales circunstancias, no es posible desarrollar en la Instalación el potencial de CONACC sino que hay que conformarse con utilizar tales tarjetas como si se tratara de cualquier otro **Soporte** del tipo "sólo lectura", para lo cual hay que afrontar la implantación de la aplicación **OEM** vinculada a CONACC utilizando los recursos inherentes al **formato Soporte = 2** (ver el documento BTP029).

Para diferenciar a las tarjetas en su utilización hay que utilizar como **NIS** alguno de los datos "típicos" grabados por el Emisor, como pueden ser el DNI, el NIA (código universitario) o cualquier otro dato que resulte unívoco. Tales datos suelen existir en un archivo genérico normalmente llamado "datos universitarios". Aunque en el **formato Soporte = 2** se admite para el **NIS** un campo de hasta 10 dígitos decimales de longitud, los valores admitidos (para mantener la compatibilidad CONACC) forman la escala entre 1 y 2147483647. Otra limitación muy importante a tener en cuenta es que el campo escogido para que su contenido sea utilizado como **NIS** no puede contener valores que no sean numéricos, además de que, obviamente, deben estar todos ellos justificados a la derecha. La utilización del **INST1** puede ser evitada sin menoscabo de la seguridad dado que en **TInACC/2** consta el nombre del archivo "genérico" que se utilizará y que es diferente de una a otra Instalación (aunque esto sólo puede garantizarse cuando en tales Instalaciones coincida el mismo Emisor). Para las tarjetas 7816 no hay mayores requerimientos en cuanto a seguridad que el uso obligado de **TInACC/2** como soporte de toda la información necesaria para tratar a las tarjetas, por lo cual este iButton es preparado directamente por Qontinuum.

5 LOS REQUERIMIENTOS

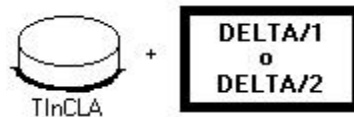
En las Instalaciones que vayan a usar tarjetas microprocesadas (en la modalidad de uso al completo) se producen unos requerimientos, en cuanto a seguridad, que vienen impuestos tanto por los Emisores como por el propio concepto implícito de "multioperatividad" que hace que diferentes suministradores puedan desarrollar distintas aplicaciones para una misma Instalación, siendo el único punto en común la tarjeta microprocesada.

En razón de tales requerimientos se ha diseñado una operativa que involucra a todas las partes intervinientes:

- Los Emisores de las tarjetas microprocesadas
- La Instalación (como usuario global)
- Los programas CONACC

El primer requerimiento consiste en que el Emisor de las tarjetas microprocesadas ceda a la Instalación las claves administrativas o de gestión necesarias para que tales tarjetas (que tienen que estar *Inicializadas*) puedan ser tratadas de manera restringida y sólo por los programas CONACC, evitando así posibles interferencias con otras aplicaciones.

Para atender a tal requerimiento, Qontinuum suministra al Emisor el iButton **TInCLA** y el programa de utilidad DELTA/1 o el programa de utilidad DELTA/2.

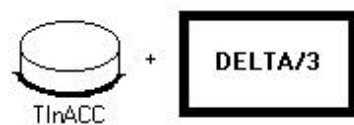


El segundo requerimiento consiste en que la Instalación disponga de la información lógica necesaria para operar en las tarjetas microprocesadas dotadas con estructura **fS=4** (que tienen que estar *Prepersonalizadas*):

- tipo/s de la/s tarjeta/s microprocesadas usadas (uno como mínimo y tres como máximo)
- nombre del directorio asignado por el Emisor para el directorio DFCA
- nombres de los archivos esenciales utilizados por los sistemas operativos CEN-WG10 y TIBC (claves administrativas, claves de gestión, código secreto y/o clave de servicio)
- nombre del archivo de **datos comunes**
- nombre del archivo de **datos específicos** primario
- nombre para los posibles archivos de **datos específicos** secundarios
- nombre para el posible archivo de datos "libres"
- nombre para el posible archivo de **datos presencia**
- nombre para el posible archivo de datos biométricos

Toda esta información está contenida en el iButton **TInACC**, el cual resulta imprescindible tanto para la seguridad de la aplicación como para la eficacia de su uso.

Para atender a tal requerimiento, Qontinuum suministra **TInACC** y el programa de utilidad DELTA/3 a la Instalación.



El tercer requerimiento consiste en operar con las tarjetas de manera segura pero aprovechando la flexibilidad que introduce la gestión realizada por los programas **OEM** de CONACC.

Para atender a tal requerimiento, Qontinuum suministra una API específica y la documentación conveniente, las cuales permiten a los **OEM** desarrollar robustas aplicaciones.

ESTA PAGINA HA SIDO DEJADA EN BLANCO INTENCIONADAMENTE

6 LOS INSTRUMENTOS

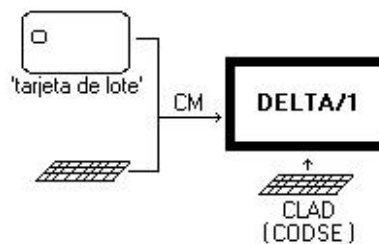
Con la finalidad de facilitar el cumplimiento de los Requerimientos explicados en el anterior capítulo, hemos desarrollado unos programas de utilidad (llamados de manera genérica DELTA al ser tres y estar vinculados) que son suministrados a las Instalaciones formando parte del Kit modelo LPC-500.

6.1 DELTA/1

Este programa de utilidad debe ser usado cuando la Instalación se constituye en Entidad Emisora de sus tarjetas microprocesadas para dotarlas con estructura **fS=4**.

Este programa posibilita grabar en **TInCLA** las claves administrativas o de gestión que corresponderán a las tarjetas que serán objeto de emisión, así como también posibilita la emisión de tales tarjetas en base a la información contenida en un archivo de datos (opcional) preparado por el programa **OEM**.

El funcionamiento esquemático para aportar las claves administrativas o de gestión es el siguiente:



Las claves administrativas o de gestión que hay que aportar son:

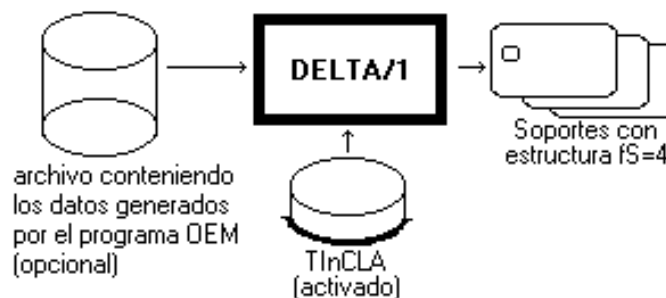
- la **CM** : es la Clave Maestra definida por el Fabricante de las tarjetas, la cual puede ser introducida (mediante la 'tarjeta de lote' suministrada por el Fabricante) o puede ser declarada.
- la **CLAD** : es definida libremente y declarada por la propia Instalación.
- el **CODSE** : es definido libremente y declarado por la propia Instalación.

Las claves administrativas o de gestión aportadas son grabadas en **TInCLA** para que éste quede activado:



Una vez que **TInCLA** está activado ya es posible generar en las tarjetas microprocesadas el directorio DFCA y los archivos esenciales (la estructura **fS=4**). Con tal de evitar el tener que manipular las tarjetas más de una vez, DELTA/1 puede grabar en cada tarjeta los datos correspondientes que estén contenidos en un archivo externo generado por el programa **OEM**, de manera que, en el caso de que tales datos completen la mínima información necesaria, las tarjetas resulten operativas de inmediato. Si no existe tal archivo también se genera en las tarjetas el directorio DFCA y los archivos esenciales, pero sólo queda grabado el **INST1** por lo que las tarjetas (que estarán sólo *Prepersonalizadas*) deberán ser procesadas posteriormente y de manera unitaria por el programa **OEM** para que éste grave en cada una de ellas la información necesaria para operar (habrán quedado *Personalizadas*). Una condición indispensable para poder grabar las tarjetas es que éstas han de haber sido *Inicializadas* por parte del Fabricante.

El funcionamiento esquemático para generar el directorio DFCA, los archivos esenciales y los archivos operativos en las tarjetas es el siguiente:



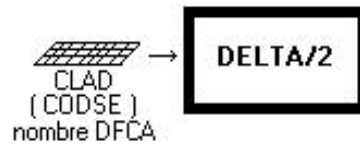
El proceso de grabación puede ser detenido y reiniciado cuantas veces se quiera dado que la información de control está consolidada en **TInCLA** y los datos para cada tarjeta son tomados del archivo externo (opcional) generado por el programa **OEM**.

En el Kit modelo LPC-500, este programa DELTA/1 es mutuamente excluyente con el programa DELTA/2.

6.2 DELTA/2

Este programa de utilidad debe ser usado por la Entidad Emisora de las tarjetas microprocesadas para aportar y trasladar a la Instalación (de manera segura mediante **TInCLA**) la **CLAD**, el **CODSE** y el nombre del DFCA que correspondan a las tarjetas que han sido objeto de *Prepersonalización* o de *Personalización* y que serán (o ya habrán sido) entregadas a la Instalación para su utilización en la modalidad de uso al completo.

El funcionamiento esquemático para aportar las claves administrativas o de gestión es el siguiente:



Las claves administrativas o de gestión que hay que aportar son:

- la **CLAD** : calificada como secreta; es generada por el Emisor de manera securizada.
- el **CODSE** : calificado como secreto; es definido por el Emisor.
- el DFCA : calificado como público; es definido por el Emisor.

Las claves administrativas o de gestión aportadas son grabadas en **TInCLA** para que éste quede activado:



La Entidad Emisora debe hacer llegar el iButton **TInCLA** a la Instalación para que ésta pueda integrar las claves administrativas o de gestión en su sistema.

En el Kit modelo LPC-500, este programa DELTA/2 es mutuamente excluyente con el programa DELTA/1.

6.3 DELTA/3

Este programa de utilidad debe ser usado en la Instalación para satisfacer las diferentes necesidades que se producen al trabajar con tarjetas microprocesadas dotadas con estructura **fS=4**.

Este programa dispone de seis opciones especializadas (la séptima opción, al ser genérica, no está recogida en este documento sino en la Ayuda en línea correspondiente a este programa):

- cuatro de las opciones se especializan en cumplir con el esquema de seguridad impuesto por CONACC para el tratamiento de las claves administrativas o de gestión del Emisor y en su extensión por toda la Instalación:

Integrar TInCLA

Gestión 'centros operativos'

Crear 'unidades operativas'

Emisores secundarios

- una opción se especializa en aportar soporte lógico a las tarjetas microprocesadas dotadas con estructura **fS=4**, liberando de tal servicio a los programas **OEM**:

Situación DFCA

- una opción se especializa en definir las claves privadas de la Instalación (sólo para los Terminales de la serie 600) que permiten establecer la situación de **aplicación asegurada**:

Asegurar 'aplicación'

Las diferentes opciones especializadas dotan a la Instalación de la capacidad de operar (de la manera indicada en cada caso) los siguientes iButton:

- **TInACC** : puede ser activado para el **centro operativo** básico al integrarle la información grabada en **TInCLA** por el/los Emisor(es)
- **TInACC/1** : puede activarse uno para cada posible **centro operativo** que no sea el básico
- **TInACC/2** : puede activarse uno para cada posible **unidad operativa**
- **TInCLA** : puede prepararse uno para cada Emisor secundario
- **TInACC/S** : puede activarse uno para cada Terminal de la serie 600

Dada la complejidad e importancia de las opciones especializadas, la explicación detallada de cada una de ellas hay que verla en la Ayuda en línea correspondiente al programa DELTA/3.

7 LA PUESTA EN MARCHA

Para una eficaz puesta en marcha, el primer paso hay que darlo instalando físicamente los Terminales y el Bus de comunicaciones que los une. La explicación detallada para hacerlo se puede encontrar en el grupo *Paso a paso* en la Ayuda del programa de utilidad Q2_UTIL.

Aunque en la Ayuda de Q2_UTIL queda muy claro cuales son los pasos que hay que dar para realizar la instalación física, existe un condicionante esencial para la instalación lógica que está relacionado con las claves administrativas o de gestión utilizadas por el Emisor o Emisores de las tarjetas 7816-4.

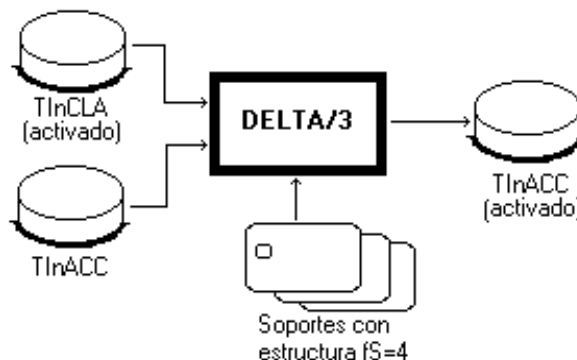
7.1 Un solo Emisor

En circunstancias normales existe un solo Emisor para una misma Instalación, por lo cual será éste el que defina y declare las claves administrativas o de gestión utilizadas en sus tarjetas.

Para preparar el esquema de seguridad hay que utilizar la opción *Integrar TinCLA* del programa de utilidad DELTA/3.

Esta opción debe ser usada una primera vez al arrancar la Instalación dado que valida las claves administrativas o de gestión recibidas en **TinCLA** (que han sido generadas por el Emisor) y las integra en **TinACC**.

Antes de integrar en **TinACC** las claves administrativas o de gestión recibidas mediante **TinCLA**, esta opción comprueba que tales claves coincidan con las utilizadas en una o en varias de las tarjetas microprocesadas dotadas con estructura **fS=4** (escogida/s al azar para realizar la prueba). Si no hay coincidencia hay que suponer que se trata de un error del Emisor al declarar en **TinCLA** las claves administrativas o de gestión utilizadas en la emisión de las tarjetas. Si hay coincidencia de claves **TinACC** queda "activado" y, por tanto, en situación de operar:



Una vez que **TinACC** ha quedado "activado" ya está disponible para completar todo el esquema de seguridad, por lo que ahora es posible (y necesario):

- generar los posibles **TinACC/1** (si existe más de un **centro operativo**);
- generar los posibles **TinACC/2** (si existen **unidades operativas**);
- instalar "lógicamente" todos los Terminales utilizando la opción *Instalar fS=4* del programa de utilidad Q2_UTIL (o la equivalente que pueda implementar el programa **OEM**) utilizando, según corresponda, a **TinACC** y a los posibles **TinACC/1** y/o **TinACC/2**.

7.2 Más de un Emisor

En circunstancias excepcionales puede darse el caso de que no exista un solo Emisor sino que vaya a existir un segundo y hasta un tercero, en cuyo caso hay que hacerle/s conocedor/es del **CODSE** utilizado en la Instalación (el que definió el primer Emisor) para que las nuevas tarjetas microprocesadas dotadas con estructura **fS=4** sean compatibles con las existentes (la **CLAD** siempre es definida por cada Emisor).

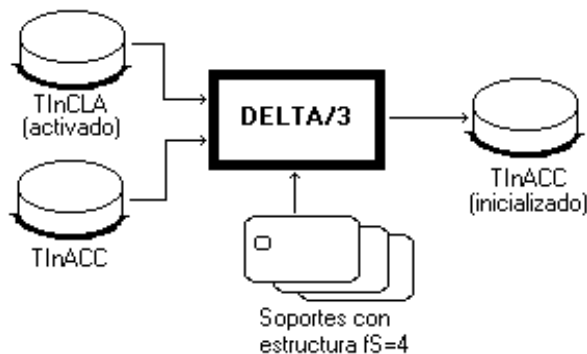
En este caso, el escenario de partida es el siguiente:

- La Instalación está usando las tarjetas generadas por el Emisor original, por lo cual **TinACC** es operativo (está en situación de "activado").
- La instalación comunica que quiere utilizar también tarjetas de un segundo (o tercer) Emisor.
- Se entrega a la Instalación un nuevo **TinACC** preparado por Qontinuum para acoger los datos correspondientes a los dos (o tres) Emisores.

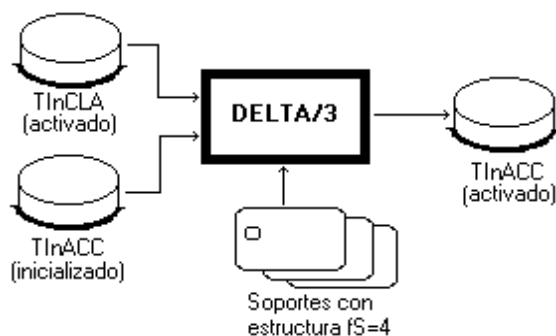
Cuando se concreta un nuevo Emisor para una misma Instalación hay que hacerle conocedor del **CODSE** utilizado en la Instalación para que las nuevas tarjetas microprocesadas dotadas con estructura **fS=4** sean compatibles con las antiguas. Para ello hay que proceder según se explica en los siguientes pasos:

- El Supervisor de la Instalación utiliza la opción *Integrar TinCLA* del programa de utilidad DELTA/3 para cargar los datos del Emisor original en el nuevo **TinACC** (si antes de cumplimentar todo el proceso hubiera que utilizar la opción *Instalar fS=4* del programa de utilidad Q2_UTIL y/o hubiera que operar con las tarjetas existentes desde el Terminal de *Sobremesa*, habría que volver a utilizar el **TinACC** antiguo).
- El Supervisor de la Instalación utiliza la opción *Emisores secundarios* del programa de utilidad DELTA/3 para traspasar el **CODSE** vigente (definido en su momento por el Emisor original a instancias propias o a elección de la Instalación) al **TinCLA** para el nuevo Emisor.
- El nuevo Emisor recibe el **TinCLA** y el programa de utilidad DELTA/2; obtiene el **CODSE** vigente en la Instalación (para utilizarlo en las tarjetas que tiene que emitir) y declara el nombre del directorio DFCA y la **CLAD** que utilizará en las tarjetas que tiene que emitir; finalmente remite el **TinCLA** activado a la Instalación.
- El Supervisor de la Instalación utiliza de nuevo la opción *Integrar TinCLA* del programa de utilidad DELTA/3 para cargar los datos del segundo (y/o tercer) Emisor en el nuevo **TinACC**.

Antes de integrar en el nuevo **TinACC** las claves administrativas o de gestión recibidas mediante cada **TinCLA**, la opción *Integrar TinCLA* del programa de utilidad DELTA/3 comprueba que tales claves coincidan con las utilizadas en una o en varias de las tarjetas microprocesadas dotadas con formato **fS=4** (escogida/s al azar para realizar la prueba). Si no hay coincidencia hay que suponer que se trata de un error del Emisor al declarar en **TinCLA** las claves administrativas o de gestión utilizadas en la emisión de las tarjetas. Si hay coincidencia de claves el nuevo **TinACC** sólo queda “inicializado” y, por tanto, no está todavía en situación de operar (dado que en la Instalación concurren tarjetas provenientes de más de un Emisor, el paso del nuevo **TinACC** a la situación de “activado” sólo se producirá al ejecutar esta opción con el último **TinCLA** previsto, por lo que mientras tanto sólo está en situación de “inicializado”):



Al ejecutar el proceso de integración con el último **TinCLA** previsto, el nuevo **TinACC** queda “activado”:



Una vez todos los **TinCLA** (uno por cada Emisor ahora existente) han sido integrados en el nuevo **TinACC**, éste ha quedado “activado” y disponible para completar todo el esquema de seguridad, por lo que ahora es posible (y necesario):

- regenerar los posibles **TinACC/1** (si existe más de un **centro operativo**);
- regenerar los posibles **TinACC/2** (si existen **unidades operativas**);
- reinstalar “lógicamente” todos los Terminales utilizando la opción *Instalar fS=4* del programa de utilidad Q2_UTIL (o la equivalente que pueda implementar el programa **OEM**) utilizando tanto el nuevo **TinACC** como los posibles **TinACC/1** y/o **TinACC/2** una vez regenerados.

ESTA PAGINA HA SIDO DEJADA EN BLANCO INTENCIONADAMENTE

8 EL FUTURO

En el entorno de las actuales tarjetas microprocesadas se están produciendo avances técnicos que resultarán significativos para la popularización sostenida del uso generalista de las tarjetas. Uno de tales avances es la compatibilización de uso de algunos “monederos electrónicos”, pero hay otros dos (que no son excluyentes entre ellos) que son los que más van a marcar el futuro:

- tarjetas sin contacto físico ('contactless')
- tarjetas dotadas con tecnología 'Java Card'.

8.1 'contactless'

Desde su aparición en 1974 las tarjetas microprocesadas tienen que ser insertadas por los usuarios en los llamados 'palpadores'⁽¹⁾ porque tanto la alimentación eléctrica como las señales electrónicas utilizan el contacto físico para propagarse.

Aunque la tecnología para la lectura de tarjetas (o 'tags') en la manera llamada “manos libres”⁽²⁾ no es nueva, nunca antes de la aprobación de las normas ISO 10373, 14443A y 15693 se había aplicado a las tarjetas microprocesadas. Ahora esto empieza a cambiar dado que han hecho su aparición las tarjetas microprocesadas “sin contacto” (o 'contactless' en su nombre original) que para ser leídas y/o grabadas no necesitan ser introducidas en ningún 'palpador' sino tan solo acercadas a la antena o cabezal intercomunicador. Aunque para el Control de Accesos la distancia es corta (de 2 a 10 cm) presentan la mejora de no sufrir desgaste alguno por la fricción y añaden la ventaja de la facilidad de uso (“no-hay-que-introducirlas-y-además-hacerlo-sólo-de-la-manera-correcta”).

La tecnología existe y es eficaz (ver el documento BTP031), pero, al menos en lo referente a las “tarjetas monedero”, tardaremos un tiempo bastante notable antes de que las Entidades Financieras acepten esta nueva modalidad funcional en las tarjetas microprocesadas. Esto es debido a que son todavía muy pocos los fabricantes de tarjetas microprocesadas que las proporcionan con la “doble tecnología” (contacto físico y 'contactless') que permitiría a las Entidades Financieras justificar el paso tecnológico dada la enorme inversión que han realizado (y de momento siguen en ello) para popularizar el uso de las “tarjetas-chip” tal y como las conocemos actualmente.

8.2 'Java Card'

En las tarjetas microprocesadas actuales el sistema operativo es un programa residente llamado “máscara”⁽³⁾. La “máscara” controla las comunicaciones con el Terminal siguiendo el muy estricto protocolo impuesto por la norma ISO/IEC 7816-3, además de ejecutar los comandos transmitidos desde el Terminal. Aunque tales comandos son los previstos por la norma ISO/IEC 7816-4, cada fabricante introduce ligeras variantes debido a lo cual no existen dos “máscaras” exactamente iguales (esta es la razón por la que CONACC admite la coexistencia de tarjetas con diferente “máscara”). Sin embargo, las tarjetas actuales no permiten la modificación de la “máscara” durante la vida de las tarjetas, por lo que si fuera necesario añadir o modificar métodos operativos o prestaciones del sistema operativo habría que rediseñar la “máscara” y producir nuevos “chips” y nuevas tarjetas (a las que habría que trasladar el contenido de los archivos, etc., lo cual lo hace del todo inviable).

Dado que la “máscara” forma parte del “chip” son los fabricantes de tarjetas quienes, normalmente, escriben el programa que regirá el funcionamiento de las tarjetas. Esto produce un cierto monopolio en el desarrollo de las “máscaras” pero también produce una incapacidad de hecho para que “cualquiera” pueda diseñar y desarrollar aplicaciones. Es en este campo donde se empiezan a producir los cambios más trascendentales al hacer su aparición las nuevas tarjetas microprocesadas compatibles con las especificaciones 'Java Card 2.0'.

Tales tarjetas disponen, por tanto, de capacidad para ejecutar los pequeños programas escritos en lenguaje Java (llamados 'applets') y que aportan todas las ventajas inherentes al concepto Java de "máquina virtual", de manera que, ya ahora pero especialmente en el futuro, los diseñadores podrán trabajar sin tener que preocuparse por las posibilidades operativas de las tarjetas existentes dado que el producto de su desarrollo serán programas que se cargarán a voluntad en las tarjetas y se ejecutarán los unos con independencia de los otros.

En este nuevo planteamiento, los fabricantes de las tarjetas asumirán la responsabilidad de que la "máscara" (que por supuesto sigue y seguirá existiendo) cumpla, como mínimo, con las especificaciones 'Java Card 2.0', y serán otros los que programen las aplicaciones que se cargarán en la memoria de los "chips" de manera voluntaria (por ejemplo haciendo uso de los teléfonos móviles, de los cajeros automáticos o de otros medios similares). De esta manera los programas se escribirán pensando únicamente en la aplicación y no en las prestaciones de una u otra "máscara".

Para clarificar el planteamiento podemos establecer una analogía con el entorno de los PC y de los PDA:

la "máscara" pasa a ser llamada 'máquina virtual Java' y se convierte en la plataforma operativa de la tarjeta microprocesada como lo es DOS, Windows o Linux (por citar sólo algunos) para el PC o Palm OS o Windows CE para los PDA, mientras que los 'applets' son directamente ejecutables por cualquier tarjeta de cualquier fabricante como lo son los programas de aplicación en las plataformas citadas.

NOTAS:

(1) Los 'palpadores' son los elementos donde se insertan las tarjetas microprocesadas para establecer el contacto físico-eléctrico necesario entre la electrónica de control (la CPU y el Cabezal de lectura/grabación) y el "chip" incrustado en la tarjeta.

(2) Los sistemas "manos libres" (o 'hands free' en su nombre original) utilizados comercialmente han sido casi siempre de sólo lectura y ha existido y existe una vasta oferta que cubre desde los 3 hasta los 150 cm de distancia entre el 'tag' y la antena o cabezal lector así como también existe una incompatibilidad casi total entre los productos de los distintos fabricantes. En el catálogo de Qontinuum existen diversas Clases en la familia SEP para cubrir necesidades de este entorno.

(3) El nombre "máscara" se utiliza por mimetismo semántico con la máscara de litografía utilizada para diseñar el circuito electrónico que constituye el "chip" incrustado en la tarjeta.

9 RESUMEN

Las tarjetas microprocesadas aportan un potencial notable para la “multioperatividad”, por lo que las necesidades del mercado y, en menor medida, la imaginación de los diseñadores harán que nuevas aplicaciones coexistan con las típicas del entorno bancario (principalmente los “monederos electrónicos”). CONACC es, sin duda alguna, una de tales aplicaciones.

El diseño de CONACC aporta, entre otras, las siguientes características diferenciales ante otras aplicaciones existentes en el mercado:

- capacidad para la coexistencia operativa en una misma Instalación de tarjetas de hasta tres Emisores distintos, lo que permite utilizar indistintamente tarjetas con máscara CEN-WG10 (emitidas tanto por Sistema 4B como por CECA) y tarjetas con máscara TIBC (emitidas por Visa/Sermepa).
- definición y uso en las tarjetas de un directorio propio para el Control de Accesos físicos (incluye los posibles archivos de datos para el Control de Presencia y la identificación Biométrica) totalmente independiente de cualquier otra aplicación.
- número "ilimitado" de usuarios en una misma Instalación al residir la información esencial en la propia tarjeta y no en los Terminales, los cuales utilizan entonces **Lista Negra**.
- capacidad para modificar de manera automática y desde cualquier Terminal parte de la información contenida en las tarjetas.
- control anti **Pass-Back** de funcionamiento autónomo entre los Terminales y las tarjetas.
- integración de lectores Biométricos (perfil de mano o huella dactilar) para puntos de acceso de alta seguridad.
- futura adaptación a las tarjetas 'Java Card'.

ESTA PAGINA HA SIDO DEJADA EN BLANCO INTENCIONADAMENTE