6 NOTAS DE APLICACIÓN

Este capítulo aporta, en forma de Notas de Aplicación (QAN), recomendaciones y sugerencias para que aquellos que deban desarrollar programas **OEM** puedan hacerlo conociendo algunos detalles importantes del funcionamiento interno tanto de la API del **driver** como de los diversos FW utilizados en nuestros Terminales.

Hay que tener en cuenta que los Terminales de la Serie 4000 no están disponibles para los programas **OEM**.

código	título	relaciones
QAN-01	Lista_Actualización	- MRT019 : capítulo 3 (*Direcciones 23-24* y *53-54*) - BTP027 : capítulo 2.8

La Lista_Actualización es un recurso del **sistema CONACC** exclusivo para las **Acreditaciones** dotadas con la estructura **fS=4**.

Aunque los programas **OEM** pueden tratar a esta Lista como mejor les parezca, es necesario considerar lo siguiente:

- la existencia del **Sello**, que afecta a las modificaciones de los **datos específicos** y, si S1 no contiene el valor 255, a los **datos comunes**.
- los **marcajes normales** con CE=57, CE=58 y CE=60 hasta CE=68.
- cualquier cambio en la información contenida en una estructura **fS=4** sólo debería ser considerada como realizada cuando lo aseveren los correspondientes marcajes, de manera que las modificaciones que pretenda realizar el Operador del programa **OEM** no deberían ser consolidadas en los archivos de tal programa por el mero hecho de pretenderlas.
- para una misma estructura **fS=4**, una vez iniciado un proceso de actualización, no debería iniciarse ningún otro antes de concluir por completo el primero para evitar problemas de integridad (falta de coherencia) entre la información contenida en la estructura **fS=4** y la indicada por los archivos del programa **OEM**.

En los siguientes puntos se ejemplifican algunos de los usos más habituales de la Lista_Actualización, aunque no son los únicos posibles.

01.1 modificación del Perfil

El Operador del programa **OEM** quiere modificar el **Perfil** de un usuario, para lo cual utiliza el recurso que, al respecto, tenga implementado tal programa. Una vez indicado el nuevo **Perfil**, el programa genera un registro que enviará a la Lista_Actualización de todas aquellos Terminales que el Operador indique, grabando el programa (en la información maestra del usuario) una indicación de que tal cambio en el **Perfil** se pretende pero que todavía no debe ser considerado como realizado. Cuando el usuario presente su **Acreditación** a uno de tales Terminales, el cambio se producirá en la estructura **fS=4** y el FW del Terminal involucrado generará el/los marcaje(s) correspondiente(s) para indicarlo. Cuando el programa **OEM** recoja marcajes deberá filtrarlos para conocer la existencia de tal(es) marcaje(s) especialmente indicativos, y en caso de existir deberá actualizar (ahora si) en la información maestra del usuario el/los dato(s) cambiado(s).
Si no se sigue un procedimiento igual o parecido, y se yuxtaponen las modificaciones sobre una misma estructura **fS=4**, podría darse el caso de que los marcajes que indiquen una actualización (hay que recordar que los marcajes son independientes del **Sello** utilizado) correspondan a un Terminal que no disponga todavía de la última modificación pretendida, por lo que la información maestra del usuario y la existente en la estructura **fS=4** no será igual, provocando un problema de integridad de la información.

Supongamos dos Terminales a los que llamaremos ID3 e ID4; el programa **OEM** genera un registro (al que llamaremos RS1 por tener su **Sello** el valor 1) para cambiar el **grupo Usuario** del valor 7 (el original que consta en el campo **Perfil** de la estructura **fS=4** y en la información maestra del usuario) al valor 5; tal registro es enviado a los dos Terminales; el Operador del programa **OEM** se da cuenta de que ha cometido un error dado que el nuevo **grupo Usuario** tiene que ser el 8, por lo que modifica el registro y lo envía de nuevo (ahora lo llamaremos RS2 dado que el **Sello** tiene el valor 2); el registro RS2 llega al Terminal ID3 y el FW sustituye el anterior RS1 por RS2, pero antes de que RS2 llegue al Terminal ID4 el usuario presenta su **Acreditación** y el FW realiza todas las operaciones correspondientes a lo indicado por el registro RS1, por lo que la estructura **fS=4** se graba indicando **grupo Usuario** 5 y se genera el correspondiente **marcaje normal** con CE=58; a continuación el registro RS2 llega también al Terminal ID4, por lo que el programa **OEM** considera, acertadamente, que la Lista_Actualización está, ahora sí, correctamente preparada para que se realice la actualización; al recoger los marcajes del Terminal ID4, el programa **OEM** encuentra el que le indica que la actualización ha sido llevada a cabo y, por tanto, actualiza en la información maestra del usuario el **grupo Usuario** finalmente indicado (el 8), mientras que en la estructura **fS=4** de la **Acreditación** aparece el **grupo Usuario** con el valor (el 5) que existía en el registro RS1 del Terminal ID4, a partir de cuyo momento aparece una situación de incoherencia que puede ser muy dañina (al menos mientras el usuario no presente de nuevo su **Acreditación** en los Terminales ID3 o ID4, en cuyo momento se actualizaría a la información correcta indicada por el registro RS2).

01.2 cambiar la Fecha Caducidad

El dato **Fecha Caducidad** de las estructuras **fS=4** tiene, para algunos de los **tipo Usuario**, una evidente trascendencia dado que el FW realiza un estricto control operativo en base a su contenido, de manera que no sólo valida que el uso de la **Acreditación** no esté caducado sino que, y sólo cuando el acceso resulta posible, actualiza la **Fecha Caducidad** en base al "momento" y al contenido del parámetro 'RENOVACIÓN CADUCIDAD'. De esta manera, si se presenta una **Acreditación** con estructura **fS=4** caducada (su **Fecha Caducidad** es menor que la fecha del "momento") que corresponda a uno de los **tipo Usuario** a los que se les actualiza la caducidad a cada marcaje significa necesariamente que tal **Acreditación** ha estado fuera de circulación durante un tiempo superior al máximo previsto, en cuyo caso, y de manera preventiva, se le rechaza el marcaje, por lo cual deberá ser reactivado por el Supervisor del sistema o bien mediante recursos directos del programa **OEM** (utilizando el Terminal *de Sobremesa*) o bien mediante la Lista_Actualización.

Los ejemplos contenidos en el siguiente cuadro consideran que el "momento" corresponde a las 12:30 de la fecha en curso (día 31-3-2003):

#	**Fecha Caducidad** (valor inicial)	modificación indicada en la Lista_Actualización		**Fecha Caducidad** (valor final)	CE
		'Caduca'	'Miscelánea'		
1	15-08-2003 hh:mm:ss		*retrasar Fecha Caducidad* (bit b5)	15-08-2003 hh:mm:ss	
2	10-02-2003 hh:mm:ss		*retrasar Fecha Caducidad* (bit b5)	31-03-2003 23:59:59	65
3	15-08-2003 hh:mm:ss	25-04-2003	*fijar Fecha Caducidad* (bit b7)	25-04-2003 23:59:59	67
4	15-08-2003 hh:mm:ss	0	*fijar Fecha Caducidad* (bit b7)	00-00-0000 00:00:00 (caducidad ilimitada)	67
5	00-00-0000 00:00:00	15-08-2003	*fijar Fecha Caducidad* (bit b7)	15-08-2003 23:59:59	67

La pretensión # 1 no tiene efecto dado que la **Fecha Caducidad** que presenta la **Acreditación** no es inferior al "momento", por lo que su utilización sería totalmente inocua sino fuera porqué está ocupando espacio en la Lista_Actualización.
La pretensión # 2 es útil para actualizar la **Fecha Caducidad** de una **Acreditación** que está caducada (tal fecha ha sido cronológicamente superada); en esta situación, el programa **OEM** puede adelantarse al problema retrasando la caducidad, de manera que al primer intento de acceso se le actualizará la **Fecha Caducidad** a la actual más el tiempo indicado en el parámetro 'RENOVACIÓN CADUCIDAD'.
La pretensión # 3 es útil para fijar la **Fecha Caducidad** de una **Acreditación** a la fecha concreta que el programa **OEM** haya colocado en el campo 'Caduca' del registro preparado para afectar a la estructura **fS=4**.
La pretensión # 4 es útil para declarar que la **Fecha Caducidad** de una **Acreditación** pasa a ser de validez ilimitada (no caducará).
La pretensión # 5 muestra la manera de declarar **Fecha Caducidad** a una **Acreditación** con validez ilimitada.

01.3 reponer el PIN al valor por defecto

El programa **OEM** debería ofrecer esta posibilidad para ayudar a aquellos usuarios que hayan olvidado su vigente **PIN** (una explicación pormenorizada aparece en el capítulo <Metodología de uso del PIN> de la Revisión C y posteriores del documento BTP036).

Cuando se use S1 con un valor 255, para no afectar a los **datos específicos**, el recurso debería ser utilizado sólo en un Terminal (por comodidad del usuario en el más cercano al lugar desde el cual se utilice el programa **OEM**) para reponerle el **PIN** al valor por defecto “1234", dado que en este caso los cambios que afectan a los **datos comunes** no están controlados por el **Sello**, de manera que si se pretendiera la actualización desde más de un Terminal se podría producir el chocante y molesto efecto de que el **PIN** fuera repuesto en el primer Terminal, que el usuario cambiara (en un Terminal de la Serie 800 ó 900) tal **PIN** a uno de su solo conocimiento y que, al presentar la **Acreditación** en otro Terminal cualquiera en cuya Lista_Actualización también se indicara la reposición, le sería nuevamente restaurado el **PIN** al valor por defecto “1234" sin que el usuario fuera consciente de ello hasta que su intento de acceso resultara rechazado debido a que en la estructura **fS=4** de su **Acreditación** de nuevo constaría el **PIN** por defecto “1234", mientras que el usuario supondría la existencia del valor que él hubiera declarado.

código	título	relaciones
QAN-02	Tabla_Incidencias (utilizada en Terminales para C.A. dotados con pantalla)	- MRT019 : capítulo 3 (*Direcciones 81-82*) - BTP027 : capítulo 2.12

Aunque los programas **OEM** pueden tratar a los marcajes inherentes al uso de esta Tabla como mejor les parezca, y dado que el FW de los Terminales involucrados genera un **marcaje normal** de *Control de Accesos* seguido automáticamente por un **marcaje normal** de *Control de Presencia* (con la indicación de la Incidencia declarada(1)), parece muy razonable que aquellos marcajes que presenten el campo 'PI' en lugar del campo 'CE' (para más información hay que ver lo especificado para las *Direcciones 25 y 26* en el capítulo 3) sean ignorados a todos los efectos por la aplicación de *Control de Accesos* y sean "pasados" (usando para ello el medio que se haya establecido) a la aplicación de *Control de Presencia*.

Si en la Instalación no fuera necesaria la utilización de Incidencias pero se quisiera que el FW generara marcajes específicos para *Control de Presencia*, el programa **OEM** deberá asignar un valor válido al puntero Inicio_Tabla_Incidencias y grabar en ella un único **registro EOF** (en la práctica significa que tal Tabla existe pero está vacía, por lo cual se generarán **marcajes normales** con el campo 'PI').

En el siguiente cuadro se resume la factibilidad de la indicación de las Incidencias en función de la Versión de FW utilizada y de las condiciones expresadas:

Versión de FW	Indicación de Incidencias con anotación de ...		Tipos de **marcajes normales** generados
	... sentido de paso	... **NIS** (por teclado)	
05.03.00 y >>	NO	NO ('PI' = 0)	'CE' + 'PI'
05.03.04 y >>	NO	SI(2)(3)	'CE' + 'PI'
05.03.06 y >>	SI(4)	SI(2)(3)	'CE' + 'PI'
05.04.00 y >>	SI(4)	SI(2)(3)	'PI' + 'CE'
06.00.00 y >>	SI(4)	SI(2)(5)	'PI' + 'CE'
09.00.00 y >>	SI(4)(6)	SI(2)(5)	'PI' + 'CE'(6)

NOTAS

(1)
En la Versión 05.03.00 (y posteriores) del FW sólo se generaban **marcajes normales** con el campo 'PI' si el usuario anotaba una Incidencia, mientras que a partir de la Versión 05.03.06 los **marcajes normales** con el campo 'PI' se generan siempre (si la Tabla_Incidencias está declarada) aunque sólo si el marcaje resulta válido bajo el punto de vista del *Control de Accesos* (la naturaleza básica del Terminal). A partir de la Versión 05.04.00 quedó invertido el orden de generación de los dos marcajes, de manera que se genera primero un **marcaje normal** de *Control de Presencia* y a continuación un **marcaje normal** de *Control de Accesos*.

(2)
Cuando hay Incidencia requiere pulsar la tecla "Intro" para confirmar la Incidencia anotada e introducir el **NIS** por teclado.

(3)
Cuando no hay Incidencia requiere pulsar la tecla '0' seguida de la tecla "Intro" para introducir el **NIS** por teclado.

(4)
Sólo con teclados de más de 12 teclas.

(5)
Cuando hay Incidencia requiere pulsar la tecla F2 o F4[(4)] para iniciar la selección de Incidencias, y una vez seleccionada requiere pulsar la tecla "Intro" para confirmarla e introducir el **NIS** por teclado. Permite introducir el **NIS** directamente por teclado cuando no se desee introducir ninguna Incidencia.

(6)
No aplicable a las Incidencias de tipo "SxT", las cuales generan **marcajes Panel** (ver la Nota de Aplicación QAN-20).

código	título	relaciones
QAN-03	Lista_Marcajes Lista_Marcajes_CDP	- MRT019 : capítulo 3 (ver *Direcciones* en *NOTAS*) - MRT019 : capítulo 5 (función *1*) - BTP027 : capítulo 3

Ambas Listas son tratadas por el FW de la misma manera, lo cual significa que éste, una vez grabado el oportuno marcaje, incrementa el 'puntero dinámico'(1) en tantas unidades como Bytes tenga el marcaje grabado (tal cosa depende de la estructura de la Lista).
Si el valor resultante del 'puntero dinámico' resulta inferior al valor definido para el 'puntero final'(2), el FW acaba su actuación al respecto.
Si el valor resultante del 'puntero dinámico' resulta igual al valor definido para el 'puntero final'(2), el FW actúa de diferente manera:
- Para la Lista_Marcajes en C.A., el 'puntero dinámico' toma el valor indicado en el 'puntero inicial'(3) y se activa (= 1) el 'indicador'(4) y se permiten más marcajes (que destruyen a los más antiguos).
- Para la Lista_Marcajes en C.P., el 'puntero dinámico' queda igual y se activa (= 2) el 'indicador'(4) y no se permiten más marcajes, de manera que cada vez que un usuario intente realizar un nuevo marcaje le aparecerá el mensaje establecido para la situación LISTA_MARCAJES : LLENA (ver el capítulo B.3).
- Para la Lista_Marcajes_C.D.P., el 'puntero dinámico' queda igual y se activa (= 2) el 'indicador'(4) y no se permiten más marcajes, de manera que cada vez que un usuario intente realizar un nuevo marcaje le aparecerá el mensaje establecido para la situación LISTA_MARCAJES_CDP : LLENA (ver el capítulo B.3).

Para proceder a la recogida de los marcajes existentes en la Lista oportuna, el programa **OEM** tiene que obtener (mediante la función *16 Leer_RAM*) los valores del 'puntero inicial'(3), del 'puntero final'(2), del 'puntero dinámico'(1) y del 'indicador'(4), de manera que pueda compararlos para conocer si hay marcajes a ser recogidos (lo cual queda en evidencia cuando el 'puntero dinámico' es mayor que el 'puntero inicial').
Una vez recogidos los marcajes (mediante la función *16 Leer_RAM*), el programa **OEM** debe restaurar el valor del 'puntero dinámico' de manera que apunte al principio de la Lista (lo cual indica que no hay marcajes pendientes de ser recogidos), para lo cual puede utilizar directamente la función genérica *17 Grabar_RAM* (cargando en el 'puntero dinámico' el valor del 'puntero inicial') o utilizar la función específica *36 Inicializar_Lista_Marcajes* (pasando como parámetro el 'puntero dinámico' obtenido anteriormente) para que sea el FW el que se encargue de restaurar los punteros y de informar convenientemente si durante el proceso de recogida se hubiera producido algún nuevo marcaje, en cuyo caso retornará un código de estado 37. Realmente, y dado que el FW retorna tal código siempre que el 'puntero dinámico' recibido como parámetro es diferente del 'puntero dinámico' real, lo más probable es que exista uno o varios nuevos marcajes, por lo que el programa **OEM** debe iniciar de nuevo el proceso estándar de lectura de punteros (como mínimo el 'puntero dinámico') y la subsiguiente lectura de marcaje/s.

El **driver** de la Versión 06.05.04 (y anteriores) y el FW de la Versión 02.02.00 (y anteriores) de los **Adaptadores de protocolos** aplican el procedimiento estándar de Time-Out y Reintentos, pero a partir de la Versión 06.05.05 (y posteriores) del **driver** y de la Versión 02.02.01 (y posteriores) del FW de los **Adaptadores de protocolos**, no se aplica tal procedimiento, de manera que, si después de enviar al Terminal el comando *36 Inicializar_Lista_Marcajes* se agota el Time-Out establecido, tanto el **driver** como el **Adaptadores de protocolos** retornan de inmediato un ST=09 al programa **OEM**, el cual debe imperiosamente iniciar de nuevo el proceso estándar de lectura de punteros (como mínimo el 'puntero dinámico') y la subsiguiente lectura de marcaje/s. De esta manera se evita completamente que la repetición de la función por parte del programa **OEM** fuerce la pérdida de un posible nuevo marcaje realizado y todavía no recogido.

A partir de la Versión 05.03.06 de los FW, a la función *36 Inicializar_Lista_Marcajes* se retorna un código de estado 19 si el valor del 'puntero dinámico' (pasado como parámetro) es menor que el valor del 'puntero inicial' o es mayor que el valor del 'puntero final' o no corresponde al inicio de un registro (tal cosa depende de la estructura de la Lista).

A partir de la Versión 08.00.00 de los FW, la función *1 Petición_Status* retorna los bits b9 y/o b10 activados (valor 1) siempre que del análisis que corresponda de los parámetros:

'ESTADO_LISTA_MARCAJES',
'PUNTERO_LISTA_MARCAJES',
'INICIO_LISTA_MARCAJES',
'PUNTERO_LISTA_MARCAJES_CDP'
'INICIO_LISTA_MARCAJES_CDP'

se infiera la existencia de marcajes.
La principal ventaja de que el FW informe de la existencia de marcajes, reside en que el programa **OEM** no tiene porqué preocuparse de manera sistemática de tal existencia (mediante la función *16 Leer_RAM*) sino que puede iterar la función *1 Petición_Status* y tomar decisiones en razón de la información retornada, lo cual permite implantar el subsistema **VirGO** (ver la Nota de Aplicación QAN-11).

NOTAS:
(1)
El 'puntero dinámico' corresponde al parámetro 'PUNTERO_LISTA_MARCAJES' (*Direcciones 29-30*) o al 'PUNTERO_LISTA_MARCAJES_CDP' (*Direcciones 33-34*).

(2)
El 'puntero final' corresponde al puntero 'FINAL_LISTA_MARCAJES' (*Direcciones 27-28*) o al 'FINAL_LISTA_MARCAJES_CDP' (*Direcciones 15-16*).

(3)
El 'puntero inicial' corresponde al puntero 'INICIO_LISTA_MARCAJES' (*Direcciones 25-26*) o al 'INICIO_LISTA_MARCAJES_CDP' (*Direcciones 13-14*).

(4)
El 'indicador' corresponde al parámetro 'ESTADO_LISTA_MARCAJES' (*Dirección 31*) o al parámetro 'ESTADO_LISTA_MARCAJES_CDP' (Dirección 37).

código	título	relaciones
QAN-04	Biometría en Instalaciones que usan **fS=4**	- MRT019 : capítulo 3 (*Direcciones 43-44,94*) - MRT019 : capítulo 5 (función *75*) (macrofunción *138*) - BTP036 (Revisión C y >>): subcapítulos 4.1, 5.1 y 6.1

Los programas **OEM** deben considerar la implementación de alguna facilidad para que el Operador del sistema pueda elegir la manera en la que el FW de los Terminales tratarán los errores de autenticación biométrica que se produzcan por parte de los usuarios en su interacción con los Terminales, para lo cual existe el subparámetro **tipo autenticación** del parámetro 'TRATAMIENTO **IDEP**'. Mediante este subparámetro, el FW controla los intentos fallidos (hasta un máximo de 3 acumulados) excepto que se indique **tipo autenticación** = 4 ó 6 (lo cual puede ser muy conveniente para evitar situaciones de **aplicación bloqueada** dada la dificultad de presentación biométrica, especialmente "digital" que, presumiblemente, pueden tener algunos usuarios). Como excepción, los FW correspondientes a Terminales para C.P. (*Control de Presencia*) y para C.D.P. *(Captura de Datos en Planta*) ignoran el posible valor declarado en **tipo autenticación**, y actúan como si tal valor fuera = 4 ó 6.

En lo concerniente a la captura y administración de los datos biométricos de los usuarios, los programas **OEM** deben considerar la implementación de tres o cuatro operativas que, aunque están conceptualmente relacionadas, son funcionalmente independientes:

Enrolar : el procedimiento a seguir para guiar al usuario con la intención de capturar su dato biométrico y grabarlo en la estructura **fS=4** de su **Acreditación**.

Verificar : el procedimiento a seguir para guiar al usuario con la intención de capturar su dato biométrico para verificarlo con el grabado en la estructura **fS=4** de su **Acreditación**.

Administrar : los procedimientos a seguir para cuando a un usuario haya que suministrarle una nueva **Acreditación** (sin necesidad de enrolarlo de nuevo).

Administrar especial : los procedimientos a seguir para grabar 'Templates' en la memoria de los propios lectores biométricos, para borrar 'Templates' de tales lectores y para cambiar (en tales lectores) el **NIS** asignado a un 'Template' concreto cuando, normalmente por pérdida, a un usuario se le haya suministrado una nueva **Acreditación** (el cual, siguiendo las recomendaciones del **sistema CONACC**, debe disponer de un **NIS** anteriormente inexistente).

Tales operativas dependen, de manera intrínseca, del tipo de lector biométrico instalado, lo cual debe ser declarado en el subparámetro 'TP' (Tipo Protocolo) de la macrofunción *138 Enrolar_fS=4*, siendo tales posibles lectores uno de los siguientes modelos:

'TP'	modelo	biometría	Clase	Familia	características
0	GEN-RSID3D	"de mano"	"1"	LPC	conectado por RS-485 al Bus auxiliar de un Terminal *de Sobremesa* modelo LPC-515 / 615
0	--	"de peso"	"5"	MIF DEF	anotación manual facilitada por el programa **OEM**
2	GEN-RSID3D	"de mano"	"1"	MIF DEF	conectado al PC (por RS-232 directo o adaptado a USB)
3	GEN-SF300	"de dedo"	"3"	LPC MIF DEF	conectado al PC (por USB directo)
4	GEN-FJ13S	"de palma"	"4"	MIF DEF	conectado al PC (por USB directo)

04.1 operativas para Tipo Protocolo (TP) = 0 y Clase "1"

04.1.1 Enrolar

En la operativa para *Enrolar* a los usuarios hay que seguir la siguiente secuencia de llamadas a la API (**driver** Q2_DRV32.DLL):

1) Macrofunción *131 Leer_fS=4* para la lectura de la estructura **fS=4** contenida en la **Acreditación**.

2) Macrofunción *138 Enrolar_fS=4, subfunción 0* para el enrolamiento completo (para lo cual hay que indicar al Operador que el usuario debe situar su mano en el lector), efectuando el propio lector biométrico tres lecturas consecutivas y su evaluación, tras la cual, y sólo si es positiva, el **driver** graba el 'Template' en el archivo $EF_{DATBIO1}$ dentro de la estructura **fS=4**.

3) Llegados a este punto, y con respecto a la biometría, el proceso ha terminado, por lo que el programa **OEM** debe implementar la expulsión de la **Acreditación** mediante la macrofunción *135 Acabar_fS=4* y seguir con el proceso general.

04.1.2 Verificar

En la operativa para *Verificar* a los usuarios hay que seguir la siguiente secuencia de llamadas a la API (**driver** Q2_DRV32.DLL):

1) Macrofunción *131 Leer_fS=4* para la lectura de la estructura **fS=4** contenida en la **Acreditación**.

2) Macrofunción *138 Enrolar_fS=4, subfunción 1* para la validación explícita de la constante biométrica (para lo cual hay que indicar al Operador que el usuario debe situar su mano en el lector).

3) Llegados a este punto, y con respecto a la biometría, el proceso ha terminado, por lo que el programa **OEM** debe implementar la expulsión de la **Acreditación** mediante la macrofunción *135 Acabar_fS=4* y seguir con el proceso general.

04.2 operativas para Tipo Protocolo (TP) = 0 y Clase "5"

Este tipo de protocolo corresponde a la biometría "de peso", debiendo el 'Template' correspondiente estar contenido en las estructuras **fS=4** para las Familias MIF y DEF.

04.2.1 Enrolar

En la operativa para *Enrolar* a los usuarios hay que seguir la siguiente secuencia de llamadas a la API (**driver** Q2_DRV32.DLL):

1) Macrofunción *131 Leer_fS=4* para la lectura de la estructura **fS=4** contenida en la **Acreditación**.

2) Anotación, por parte del Operador del programa **OEM**, del peso del usuario (se habrá obtenido por otros medios).

3) Macrofunción *138 Enrolar_fS=4, subfunción 0* para enrolar el 'Template'.

4) Macrofunción *138 Enrolar_fS=4, subfunción 3* para grabar el 'Template' generado en el correspondiente archivo dentro de la estructura **fS=4**.

5) Llegados a este punto la operativa ha terminado, por lo que el programa **OEM** debe implementar la "expulsión" de la **Acreditación** mediante la macrofunción *135 Acabar_fS=4* y seguir con el proceso general.

04.2.2 Administrar

Para la biometría contenida en las estructuras **fS=4**, la única operativa para *Administrar* de manera normal los datos biométricos de los usuarios está relacionada con la posible emisión de nuevas **Acreditaciones** (por pérdidas, etc.) sin necesidad de la presencia física de los usuarios, dado que su 'Template' no deberá ser regenerado al existir previamente en el repositorio (un archivo o una tabla en una Base de Datos) y poder ser tomado de él el elemento "biodato5" correspondiente al usuario (la descripción del elemento "biodato5" aparece en el capítulo <Elementos "biodato"> de la Revisión C y posteriores del documento BTP036), transfiriendolo al **driver** y grabando el 'Template' implícito en la **Acreditación**, para lo cual hay que hacer las siguiente acciones:

1) Macrofunción *131 Leer_fS=4* para la lectura de la estructura **fS=4** contenida en la **Acreditación**.

2) Leer en el repositorio el elemento "biodato5" que corresponda al **NIS** de la **Acreditación** perdida.

3) Macrofunción *138 Enrolar_fS=4, subfunción 6* para actualizar el **NIS** en el elemento "biodato5".

4) Macrofunción *138 Enrolar_fS=4, subfunción 3* para grabar dentro de la estructura **fS=4** (en la nueva **Acreditación** del usuario) el 'Template' extraído por el **driver** del elemento "biodato5" actualizado.

5) Macrofunción *138 Enrolar_fS=4, subfunción 4* para obtener el elemento "biodato5" actualizado.

6) Borrar en el repositorio el registro "biodato5" correspondiente al **NIS** eliminado y grabar el registro "biodato5" correspondiente al nuevo **NIS**.

04.3 operativas para Tipo Protocolo (TP) = 2

Pendiente de ser implementado en el **driver**.

04.4 operativas para Tipo Protocolo (TP) = 3

Este tipo de protocolo corresponde a la biometría "de dedo", pudiendo los 'Templates' correspondientes estar contenidos en las estructuras **fS=4** para las Familias LPC, MIF y DEF.

A partir de la Versión 07.00.00 de FW, existe un nuevo parámetro llamado 'TRATAMIENTO_COACCIÓN' cuya utilidad específica consiste en permitir a los programas **OEM** indicar el ordinal del 'Template' (en cuyo caso deberá estar necesariamente contenido en la memoria del Terminal, no pudiendo ser en ningún caso el 'Tempalte' contenido en la estructura **fS=4**) cuyo uso deberá ser considerado por el FW como indicativo de una situación de **coacción** (subcapítulo 04.4.5).

04.4.1 Enrolar

En la operativa para *Enrolar* a los usuarios hay que seguir la siguiente secuencia de llamadas a la API (**driver** Q2_DRV32.DLL):

1) Macrofunción *131 Leer_fS=4* para la lectura de la estructura **fS=4** contenida en la **Acreditación**.

2) Macrofunción *138 Enrolar_fS=4, subfunción 0* para la primera lectura de la constante biométrica (para lo cual hay que indicar al Operador que el usuario debe realizar la presentación biométrica); si el dedo ha sido mal colocado el **driver** retorna el código de estado *30 Identificación fallida*, por lo que el programa **OEM** debería advertir al Operador y éste al usuario(1); si el dedo no ha sido leído (quizá no lo han puesto) el **driver** retorna el código de estado *16 Excedida latencia Usuario*, por lo que el programa **OEM** debería advertir al Operador y éste al usuario.

3) Macrofunción *138 Enrolar_fS=4, subfunción 1* para la segunda lectura (con validación implícita) de la constante biométrica (para lo cual hay que indicar al Operador que el usuario debe realizar de nuevo la presentación biométrica). El **driver** retorna el código de estado *00 Operación/Situación correcta* si las dos lecturas son iguales considerando el nivel declarado de NiSeg en el parámetro 'NIVEL BIOMÉTRICO', o retorna el código de estado *30 Identificación fallida* si no coinciden, por lo que el programa **OEM** debería instruir al usuario para repetir la operación. En ambos casos puede ser muy ilustrativo para el Operador y/o para el usuario que el programa **OEM** muestre la "foto" de la huella(1).

4) Cuando las dos lecturas han sido iguales (código de estado *00 Operación/Situación correcta*) hay que utilizar la macrofunción *138 Enrolar_fS=4, subfunción 3* para grabar el 'Template' generado en el correspondiente archivo(1) dentro de la estructura **fS=4**.

5) Llegados a este punto la operativa ha terminado, por lo que el programa **OEM** debe implementar la "expulsión" de la **Acreditación** mediante la macrofunción *135 Acabar_fS=4* y seguir con el proceso general, aunque si se quiere que los 'Templates' residan también en los propios lectores biométricos(2), hay que ampliar el proceso encadenando los puntos A.2 y A.3 de la operativa *Administrar especial* (04.4.4).

04.4.2 Verificar

En la operativa para *Verificar* a los datos biométricos de los usuarios hay que seguir la siguiente secuencia de llamadas a la API (**driver** Q2_DRV32.DLL):

1) Macrofunción *131 Leer_fS=4* para la lectura global de la estructura **fS=4** contenida en la **Acreditación** (si el programa **OEM** implementa la operativa para *Verificar* a continuación de la operativa para *Enrolar* al mismo usuario, no es necesario repetir la lectura).

2) Macrofunción *138 Enrolar_fS=4, subfunción 2* para la lectura del 'Template' en el correspondiente archivo dentro de la estructura **fS=4**.

3) Macrofunción *138 Enrolar_fS=4, subfunción 1* para la lectura (con validación implícita) de la constante biométrica (para lo cual hay que indicar al Operador que el usuario debe realizar la presentación biométrica). El **driver** retorna el código de estado *00 Operación/Situación correcta* si las dos lecturas coinciden considerando el nivel declarado de NiSeg (biométrico "de dedo") en el parámetro 'NIVEL BIOMÉTRICO', o retorna el código de estado *30 Identificación fallida* si no coinciden, por lo que el programa **OEM** debería instruir al usuario para repetir la operación. En ambos casos puede ser muy ilustrativo para el Operador y/o para el usuario que el programa **OEM** muestre la "foto" de la huella(1).

4) Llegados a este punto, y con respecto a la biometría, la operativa ha terminado, por lo que el programa **OEM** debe seguir con el proceso general (cuando la **Acreditación** deje de ser necesaria debe implementar su "expulsión" mediante la macrofunción *135 Acabar_fS=4*).

04.4.3 Administrar

Para la biometría contenida en las estructuras **fS=4**, la única operativa para *Administrar* de manera normal los datos biométricos de los usuarios está relacionada con la posible emisión de nuevas **Acreditaciones** (por pérdidas, etc.) sin necesidad de la presencia física de los usuarios, dado que su 'Template' no deberá ser regenerado al existir previamente en el repositorio (un archivo o una tabla en una Base de Datos) y poder ser tomado de él el elemento "biodato3" correspondiente al usuario (la descripción del elemento "biodato3" aparece en el capítulo <Elementos "biodato"> de la Revisión C y posteriores del documento BTP036), transfiriendolo al **driver** y grabando el 'Template' implícito en la estructura **fS=4**, para lo cual hay que implementar la siguiente secuencia de operaciones:

1) Macrofunción *131 Leer_fS=4* para la lectura de la estructura **fS=4** contenida en la **Acreditación**.

2) Leer en el repositorio el elemento "biodato3" que corresponda al **NIS** de la estructura **fS=4** contenida en la **Acreditación** perdida.

3) Macrofunción *138 Enrolar_fS=4, subfunción 6* para actualizar el **NIS** en el elemento "biodato3".

4) Macrofunción *138 Enrolar_fS=4, subfunción 3* para grabar dentro de la estructura **fS=4** (en la nueva **Acreditación** del usuario) el 'Template' extraído por el **driver** del elemento "biodato3" actualizado.

5) Macrofunción *138 Enrolar_fS=4, subfunción 4* para obtener el elemento "biodato3" actualizado.

6) Borrar en el repositorio el registro "biodato3" correspondiente al **NIS** eliminado y grabar el registro "biodato3" correspondiente al nuevo **NIS**.

04.4.4 Administrar especial

En la operativa para *Administrar* de manera especial los datos biométricos de los usuarios, y dependiendo de la intención, hay que seguir una de las tres siguientes secuencias (A, B, C) de llamadas a la API (**driver** Q2_DRV32.DLL):

Secuencia A

En aquellas Instalaciones en las que se quiera que los 'Templates' residan en los propios lectores biométricos(2), hay que implementar un proceso para transmitir los 'Templates' a todos y cada uno de los Terminales (de los modelos cuyo nombre acabe con el número 5), para lo cual hay que implementar los siguientes puntos (los puntos A.1 y A.2 sólo serían necesarios mientras no existiera un repositorio):

A.1) Macrofunción *138 Enrolar_fS=4, subfunción 2* para la lectura del 'Template' en el correspondiente archivo dentro de la estructura **fS=4**. Al acabar este punto la **Acreditación** habrá dejado de ser necesario, por lo que debe ser "expulsada" mediante la macrofunción *135 Acabar_fS=4*.

A.2) Macrofunción *138 Enrolar_fS=4, subfunción 4* para obtener el elemento "biodato3" (su descripción aparece en el capítulo <Elementos "biodato"> de la Revisión C y posteriores del documento BTP036) correspondiente al 'Template' recién leído y, así, poder transferirlo de inmediato a todos los Terminales adecuados o bien transferirlo posteriormente cuando resulte necesario por instalación de nuevos Terminales, por "preconfiguración" de uno existente, etc., de manera que, en ambos casos, el programa **OEM** debería grabar el elemento "biodato3" obtenido en un repositorio (un archivo o una tabla en una Base de Datos).

A.3) Función *75 BioPlex, subfunción 4* para la transferencia a un Terminal del elemento "biodato3" elegido y, como consecuencia, la transferencia del 'Template' a la memoria del lector biométrico solidario del Terminal (este proceso será relativamente lento dado que el **driver** fraccionará el elemento "biodato3" en varios paquetes por limitaciones estructurales del protocolo Q-II). Este punto deberá ser repetido para cada Terminal al que se quiera transferir el 'Template'.

Secuencia B

Función *75 BioPlex, subfunción 5* para borrar un 'Template' de la memoria del lector biométrico, lo cual no sería imprescindible (en el **sistema CONACC** lo habitual es añadir el **NIS** en la **Lista_Negra** o quitarlo de la **Lista_Blanca**) sino fuera por mantener la memoria del lector biométrico lo menos ocupada que sea posible.

Secuencia C

Función *75 BioPlex, subfunción 6* para actualizar un 'Template', cambiándolo del **NIS** actual a otro que lo sustituya (normalmente por pérdida de la **Acreditación**). El programa **OEM**, y para mantener el repositorio de elementos "biodato3" actualizado, tiene que borrar en tal repositorio el registro correspondiente al **NIS** eliminado y grabar un registro correspondiente al nuevo **NIS**, para lo cual deberá implementar la obtención del nuevo elemento "biodato3" mediante la función *75 BioPlex, subfunción 3* (este proceso será relativamente lento dado que el FW fraccionará el elemento "biodato3" en varios paquetes por limitaciones estructurales del protocolo Q-II).

04.4.5 Uso de biometría en situación de coacción

Para indicar el 'Template' que deberá activar la **coacción**, los programas **OEM** deben facilitar información a los usuarios para que sean muy conscientes de cual de sus dedos (de los hasta diez posibles) es el enrolado para poder indicar una actuación bajo **coacción** (los errores, aunque sean involuntarios, pueden provocar situaciones incómodas).

Cuando el usuario presenta un dedo el FW compara el 'Template' resultante con el que consta en la estructura **fS=4**, y si la autenticación falla pasa a comparar el 'Template' fruto de la presentación con todos los que puedan existir (hasta diez) de ese mismo **NIS** en la memoria del Terminal, de manera que si el 'Template' finalmente autenticado coincide en tener el ordinal indicado en el parámetro 'TRATAMIENTO COACCIÓN', el FW asume la existencia de una situación de **coacción**. En el caso de que finalmente no se produzca la autenticación, el usuario es rechazado de la manera normal (tal y como está descrito en el capítulo <Biometría en Instalaciones que usan fS=4> de la Revisión C y posteriores del documento BTP036).

Este mecanismo sólo resulta aplicable si está implementado el control de la **coacción**.

04.5 operativas para Tipo Protocolo (TP) = 4

Este tipo de protocolo corresponde a la biometría "de palma", pudiendo el 'Template' correspondiente estar contenido en las estructuras **fS=4** pero sólo para la Familia DEF.

Existe un parámetro llamado 'TRATAMIENTO_COACCIÓN' cuya utilidad específica consiste en permitir a los programas **OEM** indicar el ordinal del 'Template' (en cuyo caso deberá estar necesariamente contenido en la memoria del Terminal, no pudiendo ser en ningún caso el 'Tempalte' contenido en la estructura **fS=4**) cuyo uso deberá ser considerado por el FW como indicativo de una situación de **coacción** (subcapítulo 04.5.5).

04.5.1 Enrolar

En la operativa para *Enrolar* a los usuarios hay que seguir la siguiente secuencia de llamadas a la API (**driver** Q2_DRV32.DLL):

1) Macrofunción *131 Leer_fS=4* para la lectura de la estructura **fS=4** contenida en la **Acreditación**.

2) Macrofunción *138 Enrolar_fS=4, subfunción 0* para iniciar el proceso de lectura de la constante biométrica (para lo cual hay que advertir al Operador que el usuario debe realizar la presentación biométrica); a partir de este momento, el 'driver' específico del lector biométrico "de palma" inicia el proceso de enrolamiento y, en función de las circunstancias, retorna el control y un Status indicativo de la situación, de manera que el programa **OEM** debe implementar un bucle compuesto de la macrofunción *138 Enrolar_fS=4, subfunción 9* para 'Consultar' el estado del proceso y, en consecuencia, informar al Operador del programa (y éste al usuario) de las diversas circunstancias que se pueden dar durante el proceso; mientras se esté ejecutando el proceso el **driver** retornará el código de estado *14 Terminal ocupado* y, en el campo DATO, un valor (todos los posibles valores están relacionados en la Nota 15 de la macrofunción *138 Enrolar_fS=4*) que informa de la situación para que el programa **OEM** indique al Operador (y éste al usuario) las instrucciones que deben ser seguidas; cuando el código de estado retornado sea *00 Operación/Situación correcta* significa que el enrolamiento ha finalizado correctamente. El programa **OEM** debería facilitar la 'Cancelación' del proceso en cualquier momento, para lo cual debe utilizar la macrofunción *138 Enrolar_fS=4, subfunción 10*.

3) Macrofunción *138 Enrolar_fS=4, subfunción 1* para la segunda lectura (con validación implícita) de la constante biométrica (para lo cual hay que indicar al Operador que el usuario debe realizar de nuevo la presentación biométrica). En este momento el 'driver' específico del lector biométrico "de palma" inicia el proceso de verificación. El programa **OEM** debe implementar un bucle compuesto de la macrofunción *138 Enrolar_fS=4, subfunción 9* para 'Consultar' el estado del proceso y, en consecuencia, informar al Operador del programa (y éste al usuario) de las diversas circunstancias que se pueden dar durante el proceso; mientras el código de estado recibido al 'Consultar' sea *14 Terminal ocupado*, el **driver** retornará en el campo DATO un valor (todos los posibles valores están relacionados en la Nota 15 de la macrofunción *138 Enrolar_fS=4*) que informa de la situación para que el programa **OEM** indique al Operador (y éste al usuario) las instrucciones que deben ser seguidas; cuando el código de estado retornado por el **driver** sea *00 Operación/Situación correcta* significa que las dos lecturas son coincidentes, mientras que si el **driver** retorna el código de estado *30 Identificación fallida* significa que las dos lecturas no coinciden, por lo que el programa **OEM** debería instruir al Operador para repetir la operación. El programa **OEM** debería facilitar la 'Cancelación' del proceso en cualquier momento, para lo cual debe utilizar la macrofunción *138 Enrolar_fS=4, subfunción 10*.

4) Cuando las dos lecturas han sido iguales (código de estado *00 Operación/Situación correcta*) hay que utilizar la macrofunción *138 Enrolar_fS=4, subfunción 3* para grabar el 'Template' generado en el correspondiente archivo dentro de la estructura **fS=4**.

5) Llegados a este punto la operativa ha terminado, por lo que el programa **OEM** debe implementar la "expulsión" de la **Acreditación** mediante la macrofunción *135 Acabar_fS=4* y seguir con el proceso general, aunque si se quiere que los 'Templates' residan también en los propios lectores biométricos[3], hay que ampliar el proceso encadenando los puntos A.2 y A.3 de la operativa *Administrar especial* (04.5.4).

04.5.2 Verificar

En la operativa para *Verificar* a los datos biométricos de los usuarios hay que seguir la siguiente secuencia de llamadas a la API (**driver** Q2_DRV32.DLL):

1) Macrofunción *131 Leer_fS=4* para la lectura global de la estructura **fS=4** contenida en la **Acreditación** (si el programa **OEM** implementa la operativa para *Verificar* a continuación de la operativa para *Enrolar* al mismo usuario, no es necesario repetir la lectura).

2) Macrofunción *138 Enrolar_fS=4, subfunción 2* para la lectura del 'Template' en el correspondiente archivo dentro de la estructura **fS=4**.

3) Macrofunción *138 Enrolar_fS=4, subfunción 1* para la lectura (con validación implícita) de la constante biométrica (para lo cual hay que indicar al Operador que el usuario debe realizar la presentación biométrica). En este momento el 'driver' específico del lector biométrico "de palma" inicia el proceso de verificación. El programa **OEM** debe implementar un bucle compuesto de la macrofunción *138 Enrolar_fS=4, subfunción 9* para 'Consultar' el estado del proceso y, en consecuencia, informar al Operador del programa (y éste al usuario) de las diversas circunstancias que se pueden dar durante el proceso; mientras el código de estado recibido al 'Consultar' sea *14 Terminal ocupado*, el **driver** retornará en el campo DATO un valor (todos los posibles valores están relacionados en la Nota 15 de la macrofunción *138 Enrolar_fS=4*) que informa de la situación para que el programa **OEM** indique al Operador (y éste al usuario) las instrucciones que deben ser seguidas; cuando el código de estado retornado por el **driver** sea *00 Operación/Situación correcta* significa que las dos lecturas son coincidentes, mientras que si el **driver** retorna el código de estado *30 Identificación fallida* significa que las dos lecturas no coinciden, por lo que el programa **OEM** debería instruir al Operador para repetir la operación. El programa **OEM** debería facilitar la 'Cancelación' del proceso en cualquier momento, para lo cual debe utilizar la macrofunción *138 Enrolar_fS=4, subfunción 10*.

4) Llegados a este punto, y con respecto a la biometría, la operativa ha terminado, por lo que el programa **OEM** debe seguir con el proceso general (cuando la **Acreditación** deje de ser necesaria debe implementar su "expulsión" mediante la macrofunción *135 Acabar_fS=4*).

04.5.3 Administrar

Para la biometría contenida en las estructuras **fS=4**, la única operativa para *Administrar* de manera normal los datos biométricos de los usuarios está relacionada con la posible emisión de nuevas **Acreditaciones** (por pérdidas, etc.) sin necesidad de la presencia física de los usuarios, dado que su 'Template' no deberá ser regenerado al existir previamente en el repositorio (un archivo o una tabla en una Base de Datos) y poder ser tomado de él el elemento "biodato4" correspondiente al usuario (la descripción del elemento "biodato4" aparece en el capítulo <Elementos "biodato"> de la Revisión C y posteriores del documento BTP036), transfiriendolo al **driver** y grabando el 'Template' implícito en la estructura **fS=4** contenida en la **Acreditación**, para lo cual hay que implementar la siguiente secuencia de operaciones:

1) Macrofunción *131 Leer_fS=4* para la lectura de la estructura **fS=4** contenida en la **Acreditación**.

2) Leer en el repositorio el elemento "biodato4" que corresponda al **NIS** de la estructura **fS=4** contenida en la **Acreditación** perdida.

3) Macrofunción *138 Enrolar_fS=4, subfunción 6* para actualizar el **NIS** en el elemento "biodato4".

4) Macrofunción *138 Enrolar_fS=4, subfunción 3* para grabar dentro de la estructura **fS=4** (en la nueva **Acreditación** del usuario) el 'Template' extraído por el **driver** del elemento "biodato4" actualizado.

5) Macrofunción *138 Enrolar_fS=4, subfunción 4* para obtener el elemento "biodato4" actualizado.

6) Borrar en el repositorio el registro "biodato4" correspondiente al **NIS** eliminado y grabar el registro "biodato4" correspondiente al nuevo **NIS**.

04.5.4 Administrar especial

En la operativa para *Administrar* de manera especial los datos biométricos de los usuarios, y dependiendo de la intención, hay que seguir una de las tres siguientes secuencias (A, B, C) de llamadas a la API (**driver** Q2_DRV32.DLL):

Secuencia A

En aquellas Instalaciones en las que se quiera que los 'Templates' residan en los propios lectores biométricos(3), hay que implementar un proceso para transmitir los 'Templates' a todos y cada uno de los Terminales (de los modelos cuyo nombre acabe con el número 5), para lo cual hay que implementar los siguientes puntos (los puntos A.1 y A.2 sólo serían necesarios mientras no existiera un repositorio):

A.1) Macrofunción *138 Enrolar_fS=4, subfunción 2* para la lectura del 'Template' en el correspondiente archivo dentro de la estructura **fS=4**. Al acabar este punto la **Acreditación** habrá dejado de ser necesaria, por lo que debe ser "expulsada" mediante la macrofunción *135 Acabar_fS=4*.

A.2) Macrofunción *138 Enrolar_fS=4, subfunción 4* para obtener el elemento "biodato4" (su descripción aparece en el capítulo <Elementos "biodato"> de la Revisión A y superiores del documento BTP036) correspondiente al 'Template' recién leído y, así, poder transferirlo de inmediato a todos los Terminales adecuados o bien transferirlo posteriormente cuando resulte necesario por instalación de nuevos Terminales, por "preconfiguración" de uno existente, etc., de manera que, en ambos casos, el programa **OEM** debería grabar el elemento "biodato4" obtenido en un repositorio (un archivo o una tabla en una Base de Datos).

A.3) Función *75 BioPlex, subfunción 4* para la transferencia a un Terminal del elemento "biodato4" elegido y, como consecuencia, la transferencia del 'Template' a la memoria del lector biométrico solidario del Terminal (este proceso será relativamente lento dado que el **driver** fraccionará el elemento "biodato4" en varios paquetes por limitaciones estructurales del protocolo Q-II). Este punto deberá ser repetido para cada Terminal al que se quiera transferir el 'Template'.

Secuencia B

Función *75 BioPlex, subfunción 5* para borrar un 'Template' de la memoria del lector biométrico, lo cual no sería imprescindible (en el **sistema CONACC** lo habitual es añadir el **NIS** en la **Lista_Negra** o quitarlo de la **Lista_Blanca**) sino fuera por mantener la memoria del lector biométrico lo menos ocupada que sea posible.

Secuencia C

Función *75 BioPlex, subfunción 6* para actualizar un 'Template', cambiándolo del **NIS** actual a otro que lo sustituya (normalmente por pérdida de la **Acreditación**). El programa **OEM**, y para mantener el repositorio de elementos "biodato4" actualizado, tiene que borrar en tal repositorio el registro correspondiente al **NIS** eliminado y grabar un registro correspondiente al nuevo **NIS**, para lo cual deberá implementar la obtención del nuevo elemento "biodato4" mediante la función *75 BioPlex, subfunción 3* (este proceso será relativamente lento dado que el FW fraccionará el elemento "biodato4" en varios paquetes por limitaciones estructurales del protocolo Q-II).

04.5.5 Uso de biometría en situación de coacción

Para indicar el 'Template' que deberá activar la **coacción**, los programas **OEM** deben facilitar información a los usuarios para que sean muy conscientes de cual de sus palmas de mano (de las hasta dos posibles) es la enrolada para poder indicar una actuación bajo **coacción** (los errores, aunque sean involuntarios, pueden provocar situaciones incómodas).

Cuando el usuario presenta una palma de mano el FW compara el 'Template' resultante con el que consta en la estructura **fS=4**, y si la autenticación falla pasa a comparar el 'Template' fruto de la presentación con todos los que puedan existir (hasta dos) de ese mismo **NIS** en la memoria del Terminal, de manera que si el 'Template' finalmente autenticado coincide en tener el ordinal indicado en el parámetro 'TRATAMIENTO COACCIÓN', el FW asume la existencia de una situación de **coacción**. En el caso de que finalmente no se produzca la autenticación, el usuario es rechazado de la manera normal (tal y como está descrito en el capítulo <Biometría en Instalaciones que usan **fS=4**> de la Revisión C y posteriores del documento BTP036).

Este mecanismo sólo resulta aplicable en la Familia DEF y sólo si está implementado el control de la **coacción**.

NOTAS:

(1)

Como medio de ilustración visual, a cada lectura de la huella del dedo utilizado por el usuario (con independencia del resultado final obtenido) puede ser muy conveniente mostrar en la pantalla del PC "la foto" de dicha huella, de manera que el Operador pueda juzgar si la captura es suficiente (bien contrastada, bien centrada, etc.) o si sería conveniente repetir el proceso para evitar dificultades futuras en los procesos de autenticación a realizar en los Terminales; para ello, el **driver** proporciona un recurso colateral que consiste en un archivo preparado al efecto y llamado BIO.BMP (el **driver** lo sitúa en la misma carpeta en la que resida el programa **OEM**, y a partir de la Versión 09.08.03 del **driver** también lo sitúa en la carpeta indicada en 'PathCommonData' en el Registry de Windows (*HKEY_LOCAL_MACHINE* / SOFTWARE / Qontinuum / CONACC); este archivo es borrado y creado por el **driver** en cada ejecución de la macrofunción *138 Enrolar_fS=4, subfunción 0 y subfunción 1*), por lo que el programa **OEM** (si usa tal archivo) deberá haberlo cerrado para evitar que el **driver** retorne el código de estado *75 Conflicto entorno Win*. Este recurso sólo es posible para la biometría de la Clase "3".

(2)

El motivo principal por el que en un entorno **fS=4** pueda quererse tal cosa es para incrementar la rapidez de la autenticación, dado que resulta obvio que el tiempo de acceso del propio lector biométrico a su RAM para buscar y leer el 'Template' siempre será menor que el tiempo necesario para la lectura del archivo $XX_{DATBIO3}$ (ocupa 384 Bytes), los cuales tienen que ser leídos de la **Acreditación** y transmitidos vía serie (además, en el caso de la Familia MIF, hay que autenticar 8 Sectores para acceder a los 24 Bloques).

El motivo secundario sería el habilitar hasta diez 'Templates' por usuario (frente al único 'Template' utilizable desde la **Acreditación**).

Sin embargo, hay que tener en cuenta que al almacenar los 'Templates' en la memoria del propio lector biométrico estamos atentando contra uno de los paradigmas de la estructura **fS=4** (el "principio de localidad") dado que el número de 'Templates' almacenables pasa a ser finito (del orden de entre 190 y 1900, dependiendo del número de "dedos" enrolados por usuario, en el modelo de lector biométrico "de dedo" de Clase "3" usado en nuestros Terminales), así como también hay que tener en cuenta que, necesariamente, todos los 'Templates' tienen que ser transmitidos a todos los Terminales (dotados con lector biométrico), con toda la sobrecarga en las comunicaciones que tal cosa pueda producir, además de la lentitud inherente a la grabación de los 'Templates' en la memoria de los lectores biométricos (debido a la creación sistemática 'Template'-por-'Template' de los índices para facilitar las posteriores búsquedas).

El programa **OEM** deberá utilizar el bit b11 del parámetro 'IM' en la macrofunción *129 Instalar_fS=4* para indicar al FW del Terminal cómo deberá efectuar las autenticaciones.

(3)

El motivo principal por el que en un entorno **fS=4** pueda quererse tal cosa es para incrementar la rapidez de la autenticación, dado que resulta obvio que el tiempo de acceso del propio lector biométrico a su RAM para buscar y leer el 'Template' siempre será menor que el tiempo necesario para la lectura del archivo $SF_{DATBIO4}$ (ocupa 832 Bytes), los cuales tienen que ser leídos de la **Acreditación** y transmitidos vía serie.

El motivo secundario sería el habilitar hasta dos 'Templates' por usuario (frente al único 'Template' utilizable desde la **Acreditación** de la Familia DEF).

Sin embargo, hay que tener en cuenta que al almacenar los 'Templates' en la memoria del propio lector biométrico estamos atentando contra uno de los paradigmas de la estructura **fS=4** (el "principio de localidad"), así como también hay que tener en cuenta que, necesariamente, todos los 'Templates' tienen que ser transmitidos a todos los Terminales (dotados con lector biométrico), con toda la sobrecarga en las comunicaciones que tal cosa pueda producir.

El programa **OEM** deberá utilizar el bit b11 del parámetro 'IM' en la macrofunción *129 Instalar_fS=4* para indicar al FW del Terminal cómo deberá efectuar las autenticaciones.

código	título	relaciones
QAN-05	Biometría en Instalaciones que no usan **fS=4**	- MRT019 : capítulo 3 (*Direcciones 43-44,50,92-94*) - MRT019 : capítulo 5 (función *34*, subfunción 3) (función *75*) - BTP036 (Revisión C y >>): subcapítulo 4.2

Si en la Instalación existe un Terminal *de Sobremesa* específico para la biometría (modelo GEN-SF300), también debe estar instalado el **driver** Versión 07.01.00 (o superior), en cuyo caso tanto la operativa para *Enrolar* a los usuarios como la operativa para *Verificar* a los datos biométricos de los usuarios deben ser realizadas por el programa **OEM** utilizando subfunciones específicas de la función *75 BioPlex* (por tal razón, las operativas expuestas en los subcapítulos 05.1 y 05.2 no son aplicables, aunque si es aplicable la operativa expuesta en el subcapítulo 05.3).

Si en la Instalación no existe un Terminal *de Sobremesa* específico para la biometría, el Operador del programa **OEM** deberá decidir sobre cual Terminal *Compacto* de los existentes en la Instalación (el cual necesariamente debe disponer de lector biométrico y de pantalla) será formalizado el *Enrolamiento* y la *Verificación* de cada usuario (en esta Nota de Aplicación llamamos 'Terminal primario' a tal Terminal). Como consecuencia, y dado que el 'Terminal primario' no es sino uno de uso habitual, hay que colocarlo en 'Situación: Bloqueado' durante la ejecución de las subfunciones 3, 4 y 6 de la función *75 BioPlex*. En lo concerniente a la captura y administración de los datos biométricos de los usuarios, los programas **OEM** deben considerar la implementación de tres operativas que, aunque están conceptualmente relacionadas, son funcionalmente independientes:

Enrolar : el procedimiento a seguir para guiar al usuario con la intención de capturar su dato biométrico y grabarlo en la memoria del lector que forma parte del Terminal (subcapítulo 05.1).

Verificar : el procedimiento a seguir para guiar al usuario con la intención de capturar su dato biométrico para verificarlo con el grabado en la memoria del lector que forma parte del Terminal (subcapítulo 05.2).

Administrar : los procedimientos a seguir para borrar 'Templates' y para cambiar el **NIS** asignado a un 'Template' cuando, normalmente por pérdida, a un usuario haya que suministrarle una nueva **Acreditación** (subcapítulo 05.3).

A partir de la Versión 07.00.00 de FW, existe un recurso llamado 'Tabla_Excepción_Biometría' cuya utilidad específica consiste en permitir a los programas **OEM** indicar el **NIS** y el **PIN** asignado a aquellos usuarios que, por razones fisiológicas, no puedan enrolar ninguno de sus dedos (subcapítulo 05.4).

A partir de la Versión 07.00.00 de FW, existe un nuevo parámetro llamado 'TRATAMIENTO_COACCIÓN' cuya utilidad específica consiste en permitir a los programas **OEM** indicar el ordinal del 'Template' cuyo uso deberá ser considerado por el FW como indicativo de una situación de **coacción** (subcapítulo 05.5).

05.1 Enrolar

En la operativa para *Enrolar* a los usuarios hay que seguir la siguiente secuencia de llamadas a la API (**driver** Q2_DRV32.DLL):

1) El 'Terminal primario' será puesto en 'subModo: Enrolamiento' mediante la función *34 Modo: Supervisado, subfunción 3*, de manera que el FW de tal Terminal quedará a la espera de que el usuario pertinente presente, tanto por la vía de la **Acreditación** como por anotación directa (sólo si el terminal ha sido parametrizado para ello), el **NIS** esperado(1) (que el FW habrá recibido en tal función 34); mientras tal **NIS** no sea presentado, el FW del 'Terminal primario' seguirá actuando en 'Modo: Autónomo', de manera que su comportamiento será el habitual(2).

2) Cuando el **NIS** presentado sea el esperado, el FW del 'Terminal primario' pasará a 'Modo: Supervisado' y retornará el código de estado *11 Acreditación detectada*(3) a la última función *1 Petición_Status* recibida del programa **OEM**, de manera que tal programa deberá mostrar entonces en la pantalla del 'Terminal primario' (funciones *10 Borrar_Pantalla* y *12 Escribir_Pantalla*) el mensaje establecido (en el propio programa **OEM**) para indicar al usuario que ponga el dedo en el lector biométrico, seguido de inmediato por la función *75 BioPlex, subfunción 0* para la captura de la imagen del dedo del usuario y de la función *75 BioPlex, subfunción 1* para enrolar el 'Template' resultante; mientras el usuario no formalice su presentación biométrica, el FW del 'Terminal primario' retornará el código de estado *14 Terminal ocupado*, ante lo cual el programa **OEM** tiene que insistir enviando la función *75 BioPlex, subfunción 1* (aunque puede ser conveniente introducir un pequeño lapso de espera para permitir trabajar más libremente al FW); si el usuario dejara agotar todo el tiempo indicado en el subparámetro **latencia Usuario** (forma parte del parámetro **IDEP**) sin formalizar su presentación biométrica, el FW retornaría el código de estado *16 Excedida latencia Usuario* y el programa **OEM** deberá informar debidamente al Operador para, posiblemente, repetir la operación.

3) Si se considera oportuno el realizar una verificación del Enrolamiento, el programa **OEM** deberá mostrar en la pantalla del 'Terminal primario' (funciones *10 Borrar_Pantalla* y *12 Escribir_Pantalla*) el mensaje establecido (en el propio programa **OEM**) para indicar al usuario que ponga de nuevo el dedo en el lector biométrico, seguido de inmediato por la función *75 BioPlex, subfunción 0* para la captura de la imagen del dedo del usuario y de la función *75 BioPlex, subfunción 2* para verificar el 'Template' resultante con el enrolado existente en la memoria del lector biométrico; mientras el usuario no formalice su nueva presentación biométrica, el FW del 'Terminal primario' retornará el código de estado *14 Terminal ocupado*, ante lo cual el programa **OEM** tiene que insistir enviando la función *75 BioPlex, subfunción 2* (aunque puede ser conveniente introducir un pequeño lapso de espera para permitir trabajar más libremente al FW); si el usuario dejara agotar todo el tiempo indicado en el subparámetro **latencia Usuario** (forma parte del parámetro **IDEP**) sin formalizar su nueva presentación biométrica, el FW retornaría el código de estado *16 Excedida latencia Usuario* y el programa **OEM** deberá informar debidamente al Operador para, posiblemente, repetir la operación.

4) El **driver** retorna el código de estado *00 Operación/Situación correcta* si los dos 'Templates' (el original contenido en la memoria del lector biométrico y el actual obtenido en la captura) son iguales considerando el nivel declarado de NiSeg (parámetro 'NIVEL BIOMÉTRICO'), o retorna el código de estado *30 Identificación fallida* si no coinciden, por lo que el usuario debería repetir la operación (desde el punto 2, aunque es posible hacerlo desde el punto 3). En ambos casos, el programa **OEM** deberá mostrar entonces en la pantalla del 'Terminal primario' (funciones *10 Borrar_Pantalla* y *12 Escribir_Pantalla*) el mensaje establecido (en el propio programa **OEM**) para indicar al usuario la situación objetiva, acabando con la función *7 Terminar_Bien* o con la función *8 Terminar_Mal* (sin expulsión de la **Acreditación**).

5) Opcionalmente, repetir los pasos 2) y 3) para registrar otros dedos del mismo usuario[5]. Llegados a este punto, el proceso ha terminado en lo que respecta a la participación del usuario, pero el programa **OEM** debe ahora obtener el 'Template' creado en el 'Terminal primario', archivarlo convenientemente y transmitirlo a todos y cada uno de los demás posibles Terminales (de los modelos cuyo nombre acabe con el número 5), para lo cual hay que considerar los siguientes puntos.

6) Función *75 BioPlex, subfunción 3* para obtener el elemento "biodato" (ver el capítulo <Elementos "biodato"> de la Revisión B o posteriores del documento BTP036) correspondiente al usuario recién enrolado y, así, poder transferirlo de inmediato a todos los Terminales adecuados o bien transferirlo posteriormente cuando resulte necesario por instalación de nuevos Terminales, por "preconfiguración" de uno existente, etc., de manera que, en ambos casos, el programa **OEM** debería grabar el elemento "biodato" obtenido en un repositorio (archivo o Base de Datos).

7) Función *75 BioPlex, subfunción 4* para la transferencia a un Terminal del elemento "biodato" elegido y, como consecuencia, la transferencia del 'Template' a la memoria del lector biométrico solidario.

8) Llegados a este punto, y con respecto a la biometría, la operativa habrá terminado, por lo que el programa **OEM**, antes de seguir con el proceso general, deberá utilizar la función *34 Modo: Supervisado, subfunción 0* para que el 'Terminal primario' regrese al 'Modo: Autónomo', de manera que su comportamiento vuelva a ser el habitual.

05.2 Verificar

En la operativa para *Verificar* a los datos biométricos de los usuarios hay que seguir la siguiente secuencia de llamadas a la API (**driver** Q2_DRV32.DLL):

1) Si se considera oportuno el realizar una verificación del Enrolamiento existente en un Terminal concreto, el programa **OEM** deberá poner tal Terminal (pasa a ser considerado como 'Terminal primario') en 'subModo: Enrolamiento' mediante la función *34 Modo: Supervisado, subfunción 3*, de manera que el FW de tal Terminal quedará a la espera de que el usuario pertinente presente, tanto por la vía de la **Acreditación** como por anotación directa (sólo si el terminal ha sido parametrizado para ello), el **NIS** esperado(1) (que el FW habrá recibido en tal función 34); mientras tal **NIS** no sea presentado, el FW del 'Terminal primario' seguirá actuando en 'Modo: Autónomo', de manera que su comportamiento será el habitual(2).

2) Cuando el **NIS** presentado sea el esperado, el FW del 'Terminal primario' pasará a 'Modo: Supervisado' y retornará el código de estado *11 Acreditación detectada*(3) a la última función *1 Petición_Status* recibida del programa **OEM**,

3) El programa **OEM** deberá mostrar entonces en la pantalla del 'Terminal primario' (funciones *10 Borrar_Pantalla* y *12 Escribir_Pantalla*) el mensaje establecido (en el propio programa **OEM**) para indicar al usuario que ponga el dedo en el lector biométrico, seguido de inmediato por la función *75 BioPlex, subfunción 0* para la captura de la imagen del dedo del usuario; mientras el usuario no formalice su presentación biométrica, el FW del 'Terminal primario' retornará el código de estado *14 Terminal ocupado*, ante lo cual el programa **OEM** tiene que insistir enviando la función *75 BioPlex, subfunción 2* (aunque puede ser conveniente introducir un pequeño lapso de espera para permitir trabajar más libremente al FW); si el usuario dejara agotar todo el tiempo indicado en el subparámetro **latencia Usuario** sin formalizar su presentación biométrica, el FW retornaría el código de estado *16 Excedida latencia Usuario* y el programa **OEM** deberá informar debidamente al Operador para, posiblemente, repetir la operación.

4) El **driver** retorna el código de estado *00 Operación/Situación correcta* si los dos 'Templates' (el original contenido en la memoria del lector biométrico y el actual obtenido en la captura) son iguales considerando el nivel declarado de NiSeg (parámetro 'NIVEL BIOMÉTRICO'), o retorna el código de estado *30 Identificación fallida* si no coinciden, por lo que el usuario debería repetir la operación (desde el punto 2, aunque es posible hacerlo desde el punto 3). En ambos casos, el programa **OEM** deberá mostrar entonces en la pantalla del 'Terminal primario' (funciones *10 Borrar_Pantalla* y *12 Escribir_Pantalla*) el mensaje establecido (en el propio programa **OEM**) para indicar al usuario la situación objetiva, acabando con la función *7 Terminar_Bien* o con la función *8 Terminar_Mal* (sin expulsión de la **Acreditación**).

5) Llegados a este punto, y con respecto a la biometría, la operativa habrá terminado, por lo que el programa **OEM**, antes de seguir con el proceso general, deberá utilizar la función *34 Modo: Supervisado, subfunción 0* para que el 'Terminal primario' regrese al 'Modo: Autónomo', de manera que su comportamiento vuelva a ser el habitual.

05.3 Administrar

En la operativa para *Administrar* los datos biométricos de los usuarios, y dependiendo de la intención, hay que seguir una de las dos siguientes secuencias de llamadas a la API (**driver** Q2_DRV32.DLL):

A) Función *75 BioPlex, subfunción 5* para borrar un 'Template' de la memoria del lector biométrico, lo cual no sería imprescindible (en el **sistema CONACC** lo habitual es añadir el **NIS** en la **Lista_Negra** o quitarlo de la **Lista_Blanca**) sino fuera por mantener la memoria del lector biométrico lo menos ocupada que sea posible.

B) Función *75 BioPlex, subfunción 6* para reasignar un 'Template' del **NIS** actual a otro que lo sustituya (normalmente por pérdida de la **Acreditación**). Para mantener el repositorio (un archivo o una Base de Datos) de elementos "biodato" actualizado, el programa **OEM** tiene que borrar el registro correspondiente al **NIS** eliminado y grabar un registro correspondiente al nuevo **NIS**, para lo cual deberá implementar la obtención del nuevo elemento "biodato" mediante la función *75 BioPlex, subfunción 3* (este proceso será relativamente lento dado que el FW fracciona el elemento "biodato" en varios paquetes por limitaciones estructurales del protocolo Q-II, por lo que es posible que deba ajustarse, mediante la función *0 Ini_PORT* el valor asignado al Time-Out en la parametrización de los Puertos de comunicaciones).

05.4 Exclusión de usuarios

Los programas **OEM** deben definir la 'Tabla_Excepción_Biometría' en aquellos Terminales en los que aquellos usuarios afectados por la limitación fisiológica deban ser autenticados. El **NIS** puede ser obtenido tanto por presentación de la **Acreditación** (lo más habitual) como por anotación directa en el teclado[6], pero en ambos casos el FW comprueba si ha sido definida la 'Tabla_Excepción_Biometría'. Si no ha sido definida prosigue normalmente, esto es activando el lector biométrico para que el usuario presente su dedo y prosiga la autenticación biométrica. Si ha sido definida inicia el proceso de petición del **PIN** asignado al usuario (el que esté contenido en el elemento de la Tabla), controlando y actuando normalmente en lo referente a los posibles reintentos.

05.5 Uso de biometría en situación de coacción

Para indicar el 'Template' que deberá activar la **coacción**, los programas **OEM** deben facilitar información a los usuarios para que sean muy conscientes de cual de sus dedos (de los hasta diez posibles) es el enrolado para poder indicar una actuación bajo **coacción** (los errores, aunque sean involuntarios, pueden provocar situaciones incómodas).

Cuando el usuario presenta un dedo el FW compara el 'Template' resultante con todos los que puedan existir de ese mismo **NIS** en la memoria del Terminal, de manera que si el 'Template' finalmente autenticado coincide en tener el ordinal indicado en el parámetro 'TRATAMIENTO COACCIÓN', el FW asume la existencia de una situación de **coacción**. En el caso de que finalmente no se produzca la autenticación, el usuario es rechazado de la manera normal (tal y como está descrito en el capítulo <Biometría en Instalaciones que no usan **fS=4**> Revisión C y posteriores del documento BTP036).

NOTAS:

(1)
La definición de la longitud del **NIS** debe hacerse según lo especificado para la *Dirección 8* en el capítulo 3.

(2)
Cuando no se pretenda que el Terminal utilizado para las operativas de *Enrolamiento* y de *Verificación* siga siendo de uso habitual durante tales operativas (por tanto, no deba ser el llamado 'Terminal primario'), es posible forzar a tal Terminal a ser usado directamente para tales operativas enviando el **NIS** con valor 0 en la función *34 Modo_Supervisado, subfunción 3*, de manera que el FW coloque al Terminal de inmediato en 'Modo: Supervisado', lo cual permite que el programa **OEM** envíe mensajes a la pantalla de tal Terminal incluso para dirigir a los usuarios para que procedan a presentar su **Acreditación**, etc.

(3)
Si desde que el FW ha detectado a la **Acreditación** el programa **OEM** no comunica o no puede comunicar con el Terminal y, por tanto, transcurre todo el tiempo indicado en el subparámetro 'tiempo máximo de latencia' del parámetro 'DURACIÓN MENSOP', el FW abortará la operativa y volverá al 'Modo' en el que estuviera anteriormente(4), aunque seguirá manteniendo el 'subModo: Enrolamiento', al igual que también ocurrirá tal cosa si, durante esta operativa, el usuario pulsa la tecla < C > o se produce un 'Reset' del Terminal o el programa **OEM** decide cancelar el proceso mediante la función *8 Terminar_Mal* (también ocurrirá si envía la función *7 Terminar_Bien*, aunque no parece que sea apropiado usarla).

(4)
'Modo: Autónomo' si el **NIS** pasado en la función *34 Modo_Supervisado, subfunción 3* había sido mayor de 0 ó 'Modo: Supervisado' si el **NIS** pasado en la función *34 Modo_Supervisado, subfunción 3* había sido igual a 0.

(5)
Hasta un máximo de dos dedos por usuario en los terminales de la Clase "2" y hasta un máximo de diez dedos por usuario en los terminales de la Clase "3" (para conocer la Clase hay que analizar el código de Producto que se obtiene mediante la función *19 Leer_FW*).

(6)
La posibilidad de anotación del **NIS** por teclado queda indicada al activar el bit b1 del parámetro 'MÁSCARA MISCELÁNEA 2'.

código	título	relaciones
QAN-06	Biometría en Instalaciones que no usan **Acreditaciones** (Familia BIO)	- MRT019 : capítulo 3 (*Direcciones 43-44,50,92-94*) - MRT019 : capítulo 5 (función *34*, subfunción 3) (función *75*) - BTP036 (Revisión C y >>): subcapítulos 4.3

Si en la Instalación existe un Terminal *de Sobremesa* específico para la biometría (modelo GEN-SF300), también debe estar instalado el **driver** Versión 07.01.00 (o superior), en cuyo caso tanto la operativa para *Enrolar* a los usuarios como la operativa para *Verificar* a los datos biométricos de los usuarios deben ser realizadas por el programa **OEM** utilizando subfunciones específicas de la función *75 BioPlex* (por tal razón, las operativas expuestas en los subcapítulos 06.1 y 06.2 no son aplicables, aunque si es aplicable la operativa expuesta en el subcapítulo 06.3).

Si en la Instalación no existe un Terminal *de Sobremesa* específico para la biometría, el Operador del programa **OEM** deberá decidir sobre cual Terminal de los existentes en la Instalación será formalizado el *Enrolamiento* y la *Verificación* de cada usuario (en esta Nota de Aplicación llamamos 'Terminal primario' a tal Terminal). Como consecuencia, y dado que el 'Terminal primario' no es sino uno de uso habitual, hay que colocarlo en 'Situación: Bloqueado' durante la ejecución de las subfunciones 3, 4 y 6 de la función *75 BioPlex*. En lo concerniente a la captura y administración de los datos biométricos de los usuarios, los programas **OEM** deben considerar la implementación de tres operativas que, aunque están conceptualmente relacionadas, son funcionalmente independientes:

Enrolar : el procedimiento a seguir para guiar al usuario con la intención de capturar su dato biométrico y grabarlo en la memoria del lector que forma parte del Terminal (subcapítulo 06.1).

Verificar : el procedimiento a seguir para guiar al usuario con la intención de capturar su dato biométrico para verificarlo con el grabado en la memoria del lector que forma parte del Terminal (subcapítulo 06.2).

Administrar : los procedimientos a seguir para borrar 'Templates' y para cambiar el **NIS** asignado a un 'Template' concreto cuando (por circunstancias realmente extraordinarias) se decida cambiar el **NIS** al usuario (subcapítulo 06.3).

A partir de la Versión 07.00.00 de FW, existe un nuevo recurso llamado 'Tabla_Excepción_Biometría' (subcapítulo 06.4), así como también existe un nuevo parámetro llamado 'TRATAMIENTO_COACCIÓN' (subcapítulo 06.5).

06.1 Enrolar

En la operativa para *Enrolar* a los usuarios hay que seguir la siguiente secuencia de llamadas a la API (**driver** Q2_DRV32.DLL):

1) El 'Terminal primario' será puesto en 'subModo: Enrolamiento' mediante la función *34 Modo: Supervisado, subfunción 3*, de manera que el FW de tal Terminal quedará a la espera de que el usuario pertinente anote el **NIS** esperado(1) (que el FW habrá recibido en tal función 34); mientras tal **NIS** no sea anotado, el FW del 'Terminal primario' seguirá actuando en 'Modo: Autónomo', de manera que su comportamiento será el habitual(2).

2) Cuando el **NIS** anotado sea el esperado, el FW del 'Terminal primario' pasará a 'Modo: Supervisado' y retornará el código de estado *11 Acreditación detectada*(3) a la última función *1 Petición_Status* recibida del programa **OEM**, de manera que tal programa deberá mostrar entonces en la pantalla del 'Terminal primario' (funciones *10 Borrar_Pantalla* y *12 Escribir_Pantalla*) el mensaje establecido (en el propio programa **OEM**) para indicar al usuario que ponga el dedo en el lector biométrico, seguido de inmediato por la función *75 BioPlex, subfunción 0* para la captura de la imagen del dedo del usuario y de la función *75 BioPlex, subfunción 1* para enrolar el 'Template' resultante; mientras el usuario no formalice su presentación biométrica, el FW del 'Terminal primario' retornará el código de estado *14 Terminal ocupado*, ante lo cual el programa **OEM** tiene que insistir enviando la función *75 BioPlex, subfunción 1* (aunque puede ser conveniente introducir un pequeño lapso de espera para permitir trabajar más libremente al FW); si el usuario dejara agotar todo el tiempo indicado en el subparámetro **latencia Usuario** sin formalizar su presentación biométrica, el FW retornaría el código de estado *16 Excedida latencia Usuario* y el programa **OEM** deberá informar debidamente al Operador para, posiblemente, repetir la operación.

3) Si se considera oportuno el realizar una verificación del Enrolamiento, el programa **OEM** deberá mostrar en la pantalla del 'Terminal primario' (funciones *10 Borrar_Pantalla* y *12 Escribir_Pantalla*) el mensaje establecido (en el propio programa **OEM**) para indicar al usuario que ponga de nuevo el dedo en el lector biométrico, seguido de inmediato por la función *75 BioPlex, subfunción 0* para la captura de la imagen del dedo del usuario y de la función *75 BioPlex, subfunción 2* para verificar el 'Template' resultante con el enrolado existente en la memoria del lector biométrico; mientras el usuario no formalice su nueva presentación biométrica, el FW del 'Terminal primario' retornará el código de estado *14 Terminal ocupado*, ante lo cual el programa **OEM** tiene que insistir enviando la función *75 BioPlex, subfunción 2* (aunque puede ser conveniente introducir un pequeño lapso de espera para permitir trabajar más libremente al FW); si el usuario dejara agotar todo el tiempo indicado en el subparámetro **latencia Usuario** sin formalizar su nueva presentación biométrica, el FW retornaría el código de estado *16 Excedida latencia Usuario* y el programa **OEM** deberá informar debidamente al Operador para, posiblemente, repetir la operación.

4) El **driver** retorna el código de estado *00 Operación/Situación correcta* si los dos 'Templates' (el original contenido en la memoria del lector biométrico y el actual obtenido en la captura) son iguales considerando el nivel declarado de NiSeg (parámetro 'NIVEL BIOMÉTRICO'), o retorna el código de estado *30 Identificación fallida* si no coinciden, por lo que el usuario debería repetir la operación (desde el punto 2, aunque es posible hacerlo desde el punto 3). En ambos casos, el programa **OEM** deberá mostrar entonces en la pantalla del 'Terminal primario' (funciones *10 Borrar_Pantalla* y *12 Escribir_Pantalla*) el mensaje establecido (en el propio programa **OEM**) para indicar al usuario la situación objetiva, acabando con la función *7 Terminar_Bien* o con la función *8 Terminar_Mal* (sin expulsión de la **Acreditación**).

5) Opcionalmente, repetir los pasos 2) y 3) para registrar otros dedos del mismo usuario[5]. Llegados a este punto, el proceso ha terminado en lo que respecta a la participación del usuario, pero el programa **OEM** debe ahora obtener el 'Template' creado en el 'Terminal primario', archivarlo convenientemente y transmitirlo a todos y cada uno de los demás posibles Terminales (de la Familia BIO), para lo cual hay que considerar los siguientes puntos.

6) Función *75 BioPlex, subfunción 3* para obtener el elemento "biodato" (ver el capítulo <Elementos "biodato"> de la Revisión C o posteriores del documento BTP036) correspondiente al usuario recién enrolado y, así, poder transferirlo de inmediato a todos los Terminales adecuados o bien transferirlo posteriormente cuando resulte necesario por instalación de nuevos Terminales, por "preconfiguración" de uno existente, etc., de manera que, en ambos casos, el programa **OEM** debería grabar el elemento "biodato" obtenido en un repositorio (archivo o Base de Datos).

7) Función *75 BioPlex, subfunción 4* para la transferencia a un Terminal del elemento "biodato" elegido y, como consecuencia, la transferencia del 'Template' a la memoria del lector biométrico solidario.

8) Llegados a este punto, y con respecto a la biometría, la operativa habrá terminado, por lo que el programa **OEM**, antes de seguir con el proceso general, deberá utilizar la función *34 Modo: Supervisado, subfunción 0* para que el 'Terminal primario' regrese al 'Modo: Autónomo', de manera que su comportamiento vuelva a ser el habitual.

06.2 Verificar

En la operativa para *Verificar* a los datos biométricos de los usuarios hay que seguir la siguiente secuencia de llamadas a la API (**driver** Q2_DRV32.DLL):

1) Si se considera oportuno el realizar una verificación del Enrolamiento existente en un Terminal concreto, el programa **OEM** deberá poner tal Terminal (pasa a ser considerado como 'Terminal primario') en 'subModo: Enrolamiento' mediante la función *34 Modo: Supervisado, subfunción 3*, de manera que el FW de tal Terminal quedará a la espera de que el usuario pertinente anote el **NIS** esperado(1) (que el FW habrá recibido en tal función 34); mientras tal **NIS** no sea anotado, el FW del 'Terminal primario' seguirá actuando en 'Modo: Autónomo', de manera que su comportamiento será el habitual(2).

2) Cuando el **NIS** anotado sea el esperado, el FW del 'Terminal primario' pasará a 'Modo: Supervisado' y retornará el código de estado *11 Acreditación detectada*(3) a la última función *1 Petición_Status* recibida del programa **OEM**,

3) El programa **OEM** deberá mostrar entonces en la pantalla del 'Terminal primario' (funciones *10 Borrar_Pantalla* y *12 Escribir_Pantalla*) el mensaje establecido (en el propio programa **OEM**) para indicar al usuario que ponga el dedo en el lector biométrico, seguido de inmediato por la función *75 BioPlex, subfunción 0* para la captura de la imagen del dedo del usuario; mientras el usuario no formalice su presentación biométrica, el FW del 'Terminal primario' retornará el código de estado *14 Terminal ocupado*, ante lo cual el programa **OEM** tiene que insistir enviando la función *75 BioPlex, subfunción 2* (aunque puede ser conveniente introducir un pequeño lapso de espera para permitir trabajar más libremente al FW); si el usuario dejara agotar todo el tiempo indicado en el subparámetro **latencia Usuario** sin formalizar su presentación biométrica, el FW retornaría el código de estado *16 Excedida latencia Usuario* y el programa **OEM** deberá informar debidamente al Operador para, posiblemente, repetir la operación.

4) El **driver** retorna el código de estado *00 Operación/Situación correcta* si los dos 'Templates' (el original contenido en la memoria del lector biométrico y el actual obtenido en la captura) son iguales considerando el nivel declarado de NiSeg (parámetro 'NIVEL BIOMÉTRICO'), o retorna el código de estado *30 Identificación fallida* si no coinciden, por lo que el usuario debería repetir la operación (desde el punto 2, aunque es posible hacerlo desde el punto 3). En ambos casos, el programa **OEM** deberá mostrar entonces en la pantalla del 'Terminal primario' (funciones *10 Borrar_Pantalla* y *12 Escribir_Pantalla*) el mensaje establecido (en el propio programa **OEM**) para indicar al usuario la situación objetiva, acabando con la función *7 Terminar_Bien* o con la función *8 Terminar_Mal* (sin expulsión de la **Acreditación**).

5) Llegados a este punto, y con respecto a la biometría, la operativa habrá terminado, por lo que el programa **OEM**, antes de seguir con el proceso general, deberá utilizar la función *34 Modo: Supervisado, subfunción 0* para que el 'Terminal primario' regrese al 'Modo: Autónomo', de manera que su comportamiento vuelva a ser el habitual.

06.3 Administrar

En la operativa para *Administrar* los datos biométricos de los usuarios, y dependiendo de la intención, hay que seguir una de las dos siguientes secuencias de llamadas a la API (**driver** Q2_DRV32.DLL):

A) Función *75 BioPlex, subfunción 5* para borrar un 'Template' de la memoria del lector biométrico, lo cual no sería imprescindible (en el **sistema CONACC** lo habitual es añadir el **NIS** en la **Lista_Negra** o quitarlo de la **Lista_Blanca**) sino fuera por mantener la memoria del lector biométrico lo menos ocupada que sea posible.

B) Función *75 BioPlex, subfunción 6* para reasignar un 'Template' del **NIS** actual a otro que lo sustituya (situación realmente extraordinaria). Para mantener el repositorio (un archivo o una Base de Datos) de elementos "biodato" actualizado, el programa **OEM** tiene que borrar el registro correspondiente al **NIS** eliminado y grabar un registro correspondiente al nuevo **NIS**, para lo cual deberá implementar la obtención del nuevo elemento "biodato" mediante la función *75 BioPlex, subfunción 3* (este proceso será relativamente lento dado que el FW fracciona el elemento "biodato" en varios paquetes por limitaciones estructurales del protocolo Q-II, por lo que es posible que deba ajustarse, mediante la función *0 Ini_PORT* el valor asignado al Time-Out en la parametrización de los Puertos de comunicaciones).

06.4 Exclusión de usuarios

Los programas **OEM** deben definir la Tabla_Excepción_Biometría para indicar el **NIS** y el **PIN** asignado a aquellos usuarios que, por razones fisiológicas, no puedan enrolar ninguno de sus dedos. Partiendo de la base de que haya sido definida tal Tabla, y una vez que el **NIS** asignado al usuario ha sido anotado por el teclado[(6)]) el FW comprueba si tal **NIS** aparece en dicha Tabla; en caso negativo pasa a formalizar la autenticación por biometría, mientras que, en caso positivo, pasa a esperar la anotación del **PIN** asignado (el contenido en el elemento de la Tabla), para lo cual el FW opera de manera estándar tanto en la manera de pedirlo como en el control de los hasta tres reintentos.

06.5 Uso de biometría en situación de coacción

Para indicar el 'Template' que deberá activar la **coacción**, los programas **OEM** deben facilitar información a los usuarios para que sean muy conscientes de cual de sus dedos (de los hasta diez posibles) es el enrolado para poder indicar una actuación bajo **coacción** (los errores, aunque sean involuntarios, pueden provocar situaciones incómodas).

Cuando el usuario presenta un dedo el FW compara el 'Template' resultante con todos los que puedan existir de ese mismo **NIS** en la memoria del Terminal, de manera que si el 'Template' finalmente identificado coincide en tener el ordinal indicado en el parámetro 'TRATAMIENTO COACCIÓN', el FW asume la existencia de una situación de **coacción**. En el caso de que finalmente no se produzca la identificación, el usuario es rechazado de la manera normal (tal y como está descrito en el capítulo <Biometría en Instalaciones que no usan **Acreditaciones**> de la Revisión C y posteriores del documento BTP036).

NOTAS:

(1)

La definición de la longitud del **NIS** debe hacerse según lo especificado para la *Dirección 8* en el capítulo 3.

(2)

Cuando no se pretenda que el Terminal utilizado para las operativas de *Enrolamiento* y de *Verificación* siga siendo de uso habitual durante tales operativas (por tanto, no deba ser el llamado 'Terminal primario'), es posible forzar a tal Terminal a ser usado directamente para tales operativas enviando el **NIS** con valor 0 en la función *34 Modo_Supervisado, subfunción 3*, de manera que el FW coloque al Terminal de inmediato en 'Modo: Supervisado', lo cual permite que el programa **OEM** envíe mensajes a la pantalla de tal Terminal incluso para dirigir a los usuarios para que procedan a presentar su(s) dedo(s), etc.

(3)

Si desde que el FW ha detectado la anotación del **NIS** el programa **OEM** no comunica o no puede comunicar con el Terminal y, por tanto, transcurre todo el tiempo indicado en el subparámetro 'tiempo máximo de latencia' del parámetro 'DURACIÓN MENSOP', el FW abortará la operativa y volverá al 'Modo' en el que estuviera anteriormente(4), aunque seguirá manteniendo el 'subModo: Enrolamiento', al igual que también ocurrirá tal cosa si, durante esta operativa, el usuario pulsa la tecla < C > o se produce un 'Reset' del Terminal o el programa **OEM** decide cancelar el proceso mediante la función *8 Terminar_Mal* (también ocurrirá si envía la función *7 Terminar_Bien*, aunque no parece que sea apropiado usarla).

(4)

'Modo: Autónomo' si el **NIS** pasado en la función *34 Modo_Supervisado, subfunción 3* había sido mayor de 0 ó 'Modo: Supervisado' si el **NIS** pasado en la función *34 Modo_Supervisado, subfunción 3* había sido igual a 0.

(5)

Hasta un máximo de dos dedos por usuario en los terminales de la Clase "2" y hasta un máximo de diez dedos por usuario en los terminales de la Clase "3" (para conocer la Clase hay que analizar el código de Producto que se obtiene mediante la función *19 Leer_FW*).

(6)

La posibilidad de anotación del **NIS** por teclado queda indicada al activar el bit b1 del parámetro 'MÁSCARA MISCELÁNEA 2'.

código	título	relaciones
QAN-07	El tratamiento de las estructuras **fS=4** (generación asistida)	- MRT019 : capítulo 5.3 (macrofunciones fS=4) - QAN-19 - BTP021: **Acreditaciones** 'tarjeta-chip7816' - BTP031: **Acreditaciones** 'MIFARE' y 'DESFire' - BTP027 y BTP036: referencias al formato **fS=4** - BTP024 (Revisión -- y >>) - Q2_DRV32 : Versión 8.7 y >>

Cuando los programas **OEM** quieran efectuar el tratamiento directo de una **Acreditación** dotada con estructura **fS=4** para su **Prepersonalización** y/o su **Personalización** (proceso de generación asistida)[5] o para modificar parte del contenido o para leer datos preexistentes, etc., necesita usar los recursos del **driver** y del Terminal *de Sobremesa* (ID = 1). Para una mejor comprensión de tales recursos hay que considerar que se trata de macrofunciones que para el **driver** resultan atómicas, de manera que, excepto cuando se indique lo contrario, son de uso independiente entre ellas. Tales macrofunciones agrupan una serie de procedimientos que, aún siendo internamente complejos, pueden resultar en operativas simples para el Operador del programa. En todas las llamadas a la API que afecten a las estructuras **fS=4**, el **driver** comprueba la estabilidad del entorno analizando los datos básicos contenidos en **TInACC** o en **TInACC/1** o en **TInACC/2** (necesariamente debe estar presente uno de ellos).

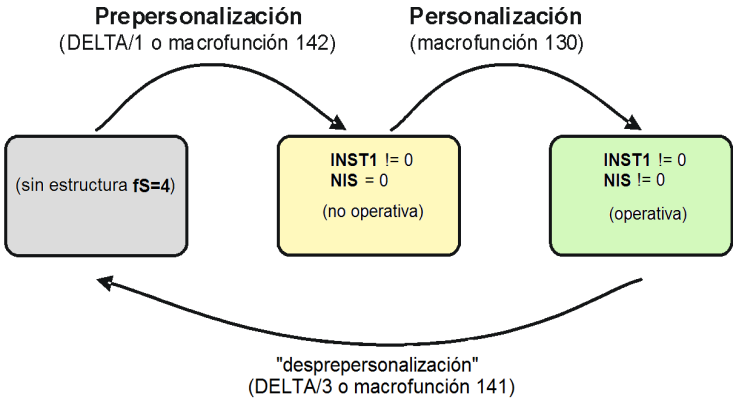
En los siguientes puntos se desarrollan conceptos y métodos básicos tanto para las **Acreditaciones** constituídas por tarjetas-chip 7816-4 como para las dotadas de un componente 'MIFARE' como para las dotadas de un componente 'DESFire'.

Las operaciones elementales para poder trabajar con tales **Acreditaciones** son:

- Prepersonalizar : permite generar la estructura **fS=4**, aunque sin contenido (**NIS**=0) a excepción del código de instalación **INST1**, a partir de una **Acreditación** virgen o de una sin una estructura **fS=4** previa[1], o de una con una estructura **fS=4** inválida (siempre que sea posible). Para las tarjetas-chip 7816-4 sólo la Entidad Emisora puede realizar dicha tarea, aunque si la Entidad Emisora es la propia Instalación es posible realizarla desde el programa de utilidad DELTA/1. Para las **Acreditaciones** 'MIFARE' y 'DESFire' se puede realizar tanto desde el programa de utilidad DELTA/1 como desde el programa **OEM** si éste hace uso de la macrofunción *142 Prepersonalizar_fS=4*. Todas las **Acreditaciones** que todavía no hayan sido sometidas al proceso de **Prepersonalización** provocan que el **driver** retorne el código de estado *08 fS=4: estructura inválida*[2] al ejecutar cualquier macrofunción que intente acceder a dicha estructura (la cual es inexistente). Una vez establecida la **Prepersonalización**, la **Acreditación** todavía deberá ser sometida al proceso de **Personalización**.

- Personalizar : permite llenar de contenido específico la estructura **fS=4** de una **Acreditación** que ya ha sido sometida al proceso de **Prepersonalización** (entre otras cosas se le asigna un **NIS** que debe ser único). El programa **OEM** debe realizar dicha acción mediante la macrofunción *130 Grabar_fS=4*, a partir de cuyo momento la **Acreditación** pasa a ser operativa. Cuando cualquier otra macrofunción retorna el código de estado *76 Archivo **datos comunes** inexistente* indica que la estructura **fS=4** de la **Acreditación** aún no ha sido sometida al proceso de **Personalización** dado que proviene de una **Prepersonalización** o de una situación de "colapso" resuelta desde el programa de utilidad DELTA/3[2]. Por otro lado, también se permite complementar una estructura **fS=4** existente creando y llenando de contenido los **datos específicos** necesarios para operar en un **centro operativo** "secundario". Para ello, el programa **OEM** debe usar la macrofunción *130 Grabar_fS=4* pero pasando solamente los **datos específicos** pertinentes. Tanto en el primer caso (grabación completa) como en este segundo (grabación parcial), el **driver** devolverá un código de estado *78 Archivo **datos específicos** existente* si el archivo de **datos específicos** implicado ya existe[3]. Si lo que se pretende es modificar datos ya existentes, el programa **OEM** debe recurrir a la macrofunción *132 Actualizar_fS=4* (ésta obliga a la ejecución previa de una macrofunción *131 Leer_fS=4*)[4].

- "desprepersonalizar" : esta acción pretende eliminar, en la medida de lo posible, la estructura **fS=4** de la **Acreditación**. Sólo es aplicable en las **Acreditaciones** 'MIFARE' y 'DESFire'. Aunque esta operativa se puede realizar desde el programa de utilidad DELTA/3, el programa **OEM** también la puede incorporar llamando a la macrofunción *141 Transformar_14443*.



En los apartados siguientes aparece información detallada de cada operación para cada tipo de **Acreditación**.

Para el tratamiento específico de la biometría hay que ver la nota de aplicación QAN-04.

NOTAS:
(1)
Si se pretende la **Prepersonalización** en una **Acreditación** que ya dispone de **Personalización** el **driver** alerta de tal circunstancia en primera instancia, aunque se permite forzar la **Prepersonalización** en segunda instancia.
En primera instancia, la macrofunción *142 Prepersonalizar_fS=4* retornará el código de estado *82 fS=4 :* ***Personalización*** *preexistente*, por lo que el programa **OEM**, en segunda instancia, podrá forzar la operativa ejecutando de nuevo tal macrofunción pero con el valor 1 en el campo ADDR.

(2)
Los **driver** con una Versión inferior a la 08.06.01, y en casos muy marginales, podían retornar el código de estado *76 Archivo* ***datos comunes*** *inexistente* incluso en la macrofunción *130 Grabar_fS=4* cuando la estructura **fS=4** era incompleta. Si se diera tal caso, hay someter a la **Acreditación** a un proceso de **Prepersonalización**.

(3)
El **centro operativo** 'primario' de una **Acreditación** viene determinado por el **INST2** del **centro operativo** donde se realice la **Personalización** completa.
La **Personalización** parcial de una **Acreditación** sólo se permite realizar en los **centros operativos** 'secundarios', es decir, cuando el **INST2** contenido en el archivo de **datos comunes** y el **INST2** del **centro operativo** (contenido en el **TInACC**, **TInACC**/**1** o **TInACC**/**2**) no coincidan, de manera que si coinciden el **driver** retorna un código de estado *04 Violación de límites*.

(4)
La macrofunción *132 Actualizar_fS=4* sólo permite la modificación de los datos leídos (excepto el **NIS**) en la previa macrofunción *131 Leer_fS=4*.

(5)
En contraposición, y a partir de la Versión 09.00.00 del FW de los Terminales de la Familia DEF de la Serie 3000, también existe la posibilidad de crear la estructura **fS=4** por generación desasistida (ver la Nota de Aplicación QAN-19).

07.1 Tarjetas-chip 7816-4

A grandes rasgos debe producirse la siguiente secuencia de acontecimientos:

- El programa **OEM** prepara los datos necesarios, muestra la petición de tarjeta para que el Operador la introduzca y ejecuta una macrofunción (por ejemplo, la *130 Grabar_fS=4*) llamando al **driver**.
- El **driver** comunica con el Terminal *de Sobremesa* (si hay problemas aborta retornando un Status adecuado) y envía una serie de comandos hasta que el Terminal *de Sobremesa* conteste indicando que dispone del ATR o hasta que el **driver** agote el contador decremental del subparámetro 'latencia_ATR' (contenido en **TInACC**, **TInACC/1** o **TInACC/2**) que habrá iniciado para detectar la situación de Time-Out. Cuando el Terminal *de Sobremesa* retorna el código de estado *00 Operación/Situación correcta* al último comando enviado por el **driver**, éste analiza la respuesta del FW y decide si ya puede interactuar con los archivos contenidos en la estructura **fS=4** de la tarjeta. A partir de ese momento el **driver** usa a discreción los comandos necesarios como consecuencia tanto de los requerimientos de la macrofunción en curso de ejecución como de todas las demás que el programa **OEM** ejecute.
- El programa **OEM** decide acabar con el procesamiento de la tarjeta introducida, para lo cual ejecuta la macrofunción *135 Acabar_fS=4*. Dependiendo de lo indicado por el programa **OEM** en la macrofunción, el **driver** indica al FW del Terminal *de Sobremesa* como debe acabar el tratamiento de la tarjeta.

Este tipo de **Acreditaciones** sólo pueden ser sometidos a **Prepersonalización** por la Entidad Emisora, por lo que si al ejecutar cualquier macrofunción sobre una **Acreditación** el **driver** retorna el código de estado *08 fS=4: estructura inválida* hay que asumir que la **Acreditación** está averiada o que no ha sido emitida correctamente, debiendo entonces avisar al Emisor para que, en la medida de lo posible, éste resuelva el problema.

Sin embargo, si la Instalación es su propia Entidad Emisora, la **Prepersonalización** se podrá realizar desde el programa de utilidad DELTA/1.

En ningún caso es posible la “desprepersonalización” en las tarjetas-chip 7816-4.

OBSERVACIONES:
1) El Terminal *de Sobremesa* (ID = 1), que se conecta al Bus RS-485, utiliza el Tipo de Protocolo TP = 0, como el resto de Terminales en la Instalación.

2) Aunque el Operador no debería introducir la tarjeta en el Terminal *de Sobremesa* antes de que el programa **OEM** se lo indique, el FW considera que siempre puede ser interrumpido por la presencia extemporánea de una tarjeta. En este caso, y dado que el FW todavía no ha recibido la orden específica por parte del **driver**, no inicia la secuencia de activación de la tarjeta sino que expulsa la tarjeta con indicación de error ('Terminar Mal').

3) Si el Terminal **de Sobremesa** recibe la orden específica por parte del **driver** pero el Operador todavía no ha introducido la tarjeta (debería ser el caso más habitual) el FW no inicia la secuencia de activación de la tarjeta (según ISO/IEC 7816-3) porque la electrónica de la tarjeta puede quedar dañada si cuando es introducida hay tensión en los contactos del palpador. En este caso, el FW carga un 'flag', activa el parpadeo del LED verde (con una frecuencia de 1/2"), arranca un contador decremental desde el subparámetro 'latencia_ATR' (contenido en **TInACC**, **TInACC/1** o **TInACC/2**) que le ha sido comunicado por el **driver** y queda a la espera de que el Operador introduzca una tarjeta. Durante ese tiempo de espera, el FW responde con rl código de estado *14 Terminal ocupado* a todos los comandos recibidos del **driver**.
Si durante ese tiempo el **driver** decide abortar el proceso envía al Terminal *de Sobremesa* un comando para que el FW desactive el parpadeo del LED verde y el decremento del contador y restaure el 'flag').
Si cuando el Operador introduce la tarjeta el 'flag' sigue cargado y el decremento del contador no ha terminado, el FW desactiva el LED verde y el decremento del contador y el Terminal *de Sobremesa* deja de responder a los comandos enviados por el **driver** dado que realmente el FW no los recibe al estar comunicando con la electrónica de la tarjeta, por lo que el **driver** asume que hay una tarjeta introducida y controla el Time-Out consecuente y los reintentos de comunicación según los parámetros aportados por el programa **OEM** desde la función *0 Ini_PORT*.
Cuando el FW ha validado al ATR, arranca un contador decremental desde el subparámetro 'latencia_COM' (contenido en **TInACC**, **TInACC/1** o **TInACC/2**) que le ha sido comunicado desde el **driver**, quedando a la espera de recibir algún otro comando desde el **driver**. Si se agota el contador decremental el FW expulsa la tarjeta con indicación de error ('Terminar_Mal'), por lo que responde con el código de estado *02 Acreditación no detectada* al primer comando finalmente recibido del **driver**.

4) Los archivos de la estructura **fS=4** contenidos en las tarjetas 7816-4 son actualizados sobre la marcha por el **driver** como consecuencia inmediata del uso, por el programa **OEM**, de las macrofunciones, de manera que, mientras permanece introducida, una misma tarjeta puede ver su contenido alterado varias veces consecutivas. Si como consecuencia del resultado producido por alguna de tales macrofunciones el programa **OEM** decide dar por terminado el proceso con la indicación de error ('Terminar_Mal'), hay que asumir que el contenido de la estructura **fS=4** en la tarjeta puede haber variado como consecuencia de alguna macrofunción ejecutada previamente, y que, por tanto, tal manera de acabar el proceso es sólo indicativa para el Operador y que no implica que permanezca en la tarjeta el contenido original de la estructura **fS=4**.

07.2 Acreditaciones 'MIFARE'

Para este tipo de **Acreditaciones**, las macrofunciones no esperan a que se presente la **Acreditación** en el Terminal *de Sobremesa*, sino que la **Acreditación** debe estar presente antes de que las macrofunciones sean llamadas.

A grandes rasgos, el programa **OEM** debe formalizar la siguiente secuencia de acciones:

- Preparación de los datos necesarios, según las macrofunciones a ejecutar.
- Mostrar en pantalla un mensaje de petición al Operador para que éste presente la oportuna **Acreditación** en el Terminal *de Sobremesa* (ID = 1), pudiendo comprobar que realiza tal cosa por medio de una de tres posibilidades:
  - -- función *1 Petición_Status* si retorna el código de estado *11 Acreditación detectada* (ver lo especificado en el capítulo 5 para esta función);
  - -- función *2 Leer_Acreditación* si retorna el código de estado *0 Operación/Situación correcta* (ver lo especificado en el capítulo 5 para esta función);
  - -- macrofunción *140 Lectura_14443*, si retorna el código de estado *0 Operación/Situación correcta* (ver lo especificado en el capítulo 5 para esta macrofunción).
- Ejecución, una vez detectada la presencia de la **Acreditación**, de la macrofunción o macrofunciones aplicables. Si el proceso encadena la **Prepersonalización** (ver el punto 07.2.1) con la **Personalización** (ver el punto 07.2.2) se puede evitar la repetición al Operador de la presentación de la **Acreditación** (dado que ésta permanece presente).
- Para acabar con el procesamiento de la **Acreditación** presentada, ejecución de la macrofunción *135 Acabar_fS=4* seguida por la aparición en pantalla de un mensaje de petición al Operador para que éste retire la **Acreditación** del Terminal *de Sobremesa*. Es importante que la **Acreditación** no sea retirada antes de tiempo, ya que si no han finalizado las tareas de grabación sobre la estructura **fS=4**, ésta podría quedar incompleta o, incluso, quedar inválida.

OBSERVACIONES:

1) El Puerto COM del PC, utilizado por los Terminales *de Sobremesa* (ID = 1), tiene que ser configurado para trabajar con el Tipo de Protocolo TP = 1. Los Terminales más antiguos, tales como los modelos MIF-1067, MIF-8200 y MIF-8240, deben ser conectados a un Puerto COM configurado a 9600 b.p.s, mientras que el modelo MIF-8310, se conecta a un Puerto USB aunque es redireccionado a un Puerto COM virtual, el cual debe configurarse a 19200 b.p.s.

2) Aunque el Operador presente la **Acreditación** en el Terminal *de Sobremesa* modelo MIF-nnnn antes de que el programa **OEM** se lo indique, no se produce ninguna reacción. Los archivos de la estructura **fS=4** contenidos en las **Acreditaciones** 'MIFARE' son actualizados sobre la marcha por el **driver** como consecuencia inmediata del uso, por el programa **OEM**, de las macrofunciones, de manera que, mientras permanece presentada, una misma **Acreditación** puede ver su contenido alterado varias veces consecutivas. Si como consecuencia del resultado producido por alguna de tales macrofunciones el programa **OEM** decide dar por terminado el proceso con la indicación de error ('Terminar_Mal'), hay que asumir que el contenido de la estructura **fS=4** en la **Acreditación** puede haber variado como consecuencia de alguna macrofunción ejecutada previamente, y que, por tanto, tal manera de acabar el proceso es sólo indicativa para el Operador y que no implica que permanezca en la **Acreditación** el contenido original de la estructura **fS=4**.

07.2.1 Prepersonalización

Hasta la publicación de la Versión 7 del **driver** de nivel bajo Q2_DRV32.DLL, la **Prepersonalización** tan solo podía formalizarse mediante el programa de utilidad DELTA/1, mientras que a partir de tal publicación los programas **OEM** pueden formalizarla usando directamente la API de bajo nivel contenida en el **driver** (macrofunción *142 Prepersonalizar_fS=4*). Evidentemente, este proceso podría ser seguido, sin solución de continuidad, por el proceso de **Personalización** (ver punto 07.2.2) antes de acabar el procesamiento de la **Acreditación** presentada, en cuyo caso se minimizarían las manipulaciones a realizar por el Operador del programa **OEM**.

07.2.2 Personalización

Para este tipo de **Acreditaciones** puede ser interesante, aunque no obligatorio, utilizar el NUID (Non-Unique IDentifier) de la propia **Acreditación** para obtener el **NIS**. Esto puede tener la ventaja de la compatibilización con el formato **fS=3** (ver la Nota de Aplicación QAN-08) y con la posible utilización concurrente de Terminales de la Clase "T" de la Familia SEP, los cuales son específicos para la 'identificación automática de vehículos en Tránsito' (iavT). Por otro lado, simplemente puede ser útil para facilitar la elección de un **NIS** que, aunque pudiera llegar a estar duplicado, difícilmente lo estará y que, en última instancia, es responsabilidad del programa **OEM** garantizar que no exista nunca un duplicado de **NIS**.

Para ello el **driver** facilita el uso de la función *2 Leer_Acreditación* y de la macrofunción *140 Lectura_14443*. El programa **OEM** deberá tener en cuenta que de los 32 bits originales del NUID, en el **sistema CONACC** sólo son aceptables 31, por lo se tendrá que eliminar el bit de mayor peso. Sin embargo es posible obtener el NUID ya adaptado si se indica adecuadamente:

- función *2 Leer_Acreditación*: activando el bit b1 del Byte bajo del campo ADDR.
- macrofunción *140 Lectura_14443*: indicando el valor C en el parámetro ‘F’ (formato).

07.2.3 "desprepersonalización"

Partiendo de la base de que toda **Acreditación** 'MIFARE' dispone de una memoria que es finita en su tamaño, en ocasiones es posible que resulte necesario habilitar, para nuevo uso, un Sector (o Sectores) utilizados por una estructura **fS=4** cuya utilidad haya periclitado.

Un ejemplo podría ser el de una gran organización dotada con muchos **centros operativos**(1), en la que cada uno de ellos, debido a que superaran en número al máximo permitido por el **sistema CONACC** para **centros operativos** 'secundarios', requiere de su propia estructura **fS=4**. Para poder trabajar con un número 'ilimitado' de **centros operativos** , independientemente del tamaño de la memoria disponible en la **Acreditación**, el programa **OEM** deberá pasar por un proceso de "desprepersonalización" a la estructura **fS=4** de la **Acreditación** del usuario que deba abandonar un centro para recuperar la memoria ocupada por la estructura **fS=4** que deja de tener vigencia(2). Cuando tal usuario ingrese en otro centro su **Acreditación** podrá ser sometida a una nueva **Prepersonalización** y **Personalización** (ver los puntos 07.2.1 y 07.2.2) y así hacer uso de los recursos de *Control de Accesos* en dicho **centro operativo**. Para tal proposito, las estructuras **fS=4** de los diferentes centros deben estar ubicadas en la misma posición dentro de la memoria de la **Acreditación** (lo cual implica utilizar el mismo nombre para el archivo, lo cual está predeterminado en la información contenida en **TInACC**, **TInACC/1** o **TInACC/2**).

El programa **OEM** debería facilitar el acceso a los recursos que, para todo lo expuesto, aporta el **sistema CONACC**, para lo cual hay que utilizar la macrofunción *141 Transformar_14443* indicando el valor 0 en el parámetro 'TS' (Tipo Subfunción) y el valor adecuado al objetivo deseado en el parámetro 'O' (opciones)(3).

Si se utiliza autenticación por biometría "de dedo" y al "desprepersonalizar" la **Acreditación** se ha respetado el 'Template' existente, el programa **OEM** deberá también implementar un recurso para que el 'Template' contenido en el archivo $NB_{DATBIO3}$ pueda ser integrado en la estructura **fS=4** generada en el **centro operativo** al que se adscribe la **Acreditación**. Para ello deberá utilizar la macrofunción *134 Desbloquear_fS=4* desactivando el bit b5 del mapa de bits existente en el quinto Byte que se habrá obtenido mediante la macrofunción *133 Analizar_fS=4* (la cual deberá haber sido ejecutada previamente).

07.2.4 Toma de datos preexistentes en las Acreditaciones

Cuando en una Instalación existan, de manera previa, **Acreditaciones** 'MIFARE' con Sectores ocupados por información de otras aplicaciones, podría darse el caso de que algunos de los datos contenidos (por ejemplo el nombre del usuario, su DNI, etc.) coincidieran en ser los mismos que el programa **OEM** deba pasar a su Base de Datos, por lo que parece muy razonable que, tanto para evitar trabajo manual al Operador como equivocaciones de transcripción, los datos existentes en las **Acreditaciones** 'MIFARE' que deban ser replicados puedan ser extraídos directamente por el programa **OEM** (de manera previa o integrada) como parte de la fase de **Personalización**.

El programa **OEM** debería facilitar el acceso a los recursos que, para todo lo expuesto, aporta el **sistema CONACC**, para lo cual hay que utilizar la macrofunción *140 Tratamiento_libre_14443* indicando el valor 1 en el parámetro 'TS' (Tipo Subfunción) y los valores adecuados al objetivo deseado en el parámetro 'CVVVVVVSB'(4).

07.2.5 Transformar las claves de acceso para ciertos Sectores

Además de servir para las circunstancias descritas en el punto 07.2.3, la transformación de claves puede ser necesaria cuando en una Instalación existan, de manera previa, **Acreditaciones** 'MIFARE' con Sectores ocupados por información de otras aplicaciones y se decida que, por razones objetivas, tales Sectores deben ser recuperados para ser utilizados en el **sistema CONACC**. Para ello hay que conocer la clave utilizada en cada uno de tales Sectores y asumir que la información original contenida en los Bloques subsidiarios se perderá (si fuera conveniente utilizar toda o parte de tal información, habría que leerla antes, para lo cual se debería utilizar el procedimiento descrito en el punto 07.2.4).

El programa **OEM** debería facilitar el acceso a los recursos que, para todo lo expuesto, aporta el **sistema CONACC**, para lo cual hay que utilizar la macrofunción *141 Transformar_14443* indicando el valor 1 en el parámetro 'TS' (Tipo Subfunción) y los valores adecuados al objetivo deseado en el parámetro 'CVVVVVVS'(5).

Como consecuencia inmediata de la transformación de la clave de un Sector, éste pasa a ser accesible por la CM (Clave Maestra) tanto en la clave A como en la clave B, de manera que tal Sector podrá o ser utilizado en cualquier aplicación que no sea del **sistema CONACC** o pasar a formar parte de una estructura **fS=4** al poder ser tratado por la macrofunción *142 Prepersonalizar_fS=4* y/o por el programa de utilidad DELTA/1 como fase previa a la **Personalización** típica (ver el punto 07.2.2).

NOTAS:

(1)
Para obtener información detallada de los diferentes recursos que el **sistema CONACC** ofrece para tratar con varios **centros operativos**, hay que ver el documento BTP024.

(2)
Si en la Instalación se utiliza autenticación por biometría "de dedo", la única excepción a tal recuperación podría ser el espacio ocupado por el 'Template', dado que tal información se refiere estrictamente al usuario y, muy probablemente, también deba ser utilizada en el nuevo **centro operativo**.

(3)
Como consecuencia de esta actuación, desaparece de la **Acreditación** la estructura **fS=4** correspondiente al **centro operativo** que el usuario abandona, quedando tal Sector (o Sectores) accesibles por la CM (Clave Maestra), por lo que la misma **Acreditación** podrá ser sometida a un proceso de **Prepersonalización** y **Personalización** en el nuevo **centro operativo** al que vaya destinado el usuario. La "desprepersonalización" también es posible realizarla desde la utilidad DELTA/1 aunque en este caso siempre se realiza sobre toda la estructura **fS=4**.

(4)
El Operador debe poder declarar el número del Sector y (opcionalmente) del Bloque a cuya información se quiere acceder así como el valor hexadecimal de la clave existente para tal Sector (tal clave debe tener necesariamente permiso de lectura); con independencia de si la información se obtiene de un Sector o de un Bloque, es responsabilidad del programa **OEM** tanto la definición de los datos a ser tomados ('offset', longitud, etc.) como el posible tratamiento y almacenamiento de tal información.

(5)
El Operador debe poder declarar el número del Sector cuya clave se quiere transformar así como el valor hexadecimal de la clave original existente (tal clave debe tener necesariamente permiso de grabación para el Bloque de claves de tal Sector).

07.3 Acreditaciones 'DESFire' ***Versión de driver 08.00.00 y >>***

Para este tipo de **Acreditaciones**, las macrofunciones no esperan a que se presente la **Acreditación** en el Terminal *de Sobremesa*, sino que la **Acreditación** debe estar presente antes de que las macrofunciones sean llamadas.

A grandes rasgos, el programa **OEM** debe formalizar la siguiente secuencia de acciones:

- Preparación de los datos necesarios, según las macrofunciones a ejecutar.
- Mostrar en pantalla un mensaje de petición al Operador para que éste presente la oportuna **Acreditación** en el Terminal *de Sobremesa* (ID = 1), pudiendo comprobar que realiza tal cosa por medio de una de dos posibilidades:
  - -- función *1 Petición_Status* si retorna el código de estado *11 Acreditación detectada* (ver lo especificado en el capítulo 5 para esta función);
  - -- función *2 Leer_Acreditación* si retorna el código de estado *0 Operación/Situación correcta* (ver lo especificado en el capítulo 5 para esta función).
- Ejecución, una vez detectada la presencia de la **Acreditación**, de la macrofunción o macrofunciones aplicables.
- Para acabar con el procesamiento de la **Acreditación** presentada, ejecución de la macrofunción *135 Acabar_fS=4* seguida por la aparición en pantalla de un mensaje de petición al Operador para que éste retire la **Acreditación** del Terminal *de Sobremesa*. Es importante que la **Acreditación** no sea retirada antes de tiempo, ya que si no han finalizado las tareas de grabación sobre la estructura **fS=4**, ésta podría quedar incompleta o, incluso, quedar inválida.

OBSERVACIONES:

1) Los Terminales *de Sobremesa* (ID = 1) modelo DEF-8311 o modelo DEF-3311 van conectados a un Puerto USB del PC que se redirecciona a un Puerto COM virtual, el cual debe ser configurado a 115200 b.p.s. También hay que configurar el Tipo de Protocolo para trabajar con **Acreditaciones** 'DESFire' (TP = 5), aunque también es posible configurarlo para trabajar con **Acreditaciones** 'MIFARE' (TP = 1).

2) Aunque el Operador presente la **Acreditación** en el Terminal *de Sobremesa* modelo DEF-8311 o modelo DEF-3311 antes de que el programa **OEM** se lo indique, no se produce ninguna reacción.
Los archivos de la estructura **fS=4** contenidos en las **Acreditaciones** 'DESFire' son actualizados sobre la marcha por el **driver** como consecuencia inmediata del uso de las macrofunciones por el programa **OEM**, de manera que, mientras permanece presentada, una misma **Acreditación** puede ver su contenido alterado varias veces consecutivas. Si como consecuencia del resultado producido por alguna de tales macrofunciones el programa **OEM** decide dar por terminado el proceso con la indicación de error ('Terminar_Mal'), hay que asumir que el contenido de la estructura **fS=4** en la **Acreditación** puede haber variado como consecuencia de alguna macrofunción ejecutada previamente, y que, por tanto, tal manera de acabar el proceso es sólo indicativa para el Operador y que no implica que permanezca en la **Acreditación** el contenido original de la estructura **fS=4**.

07.3.1 Prepersonalización

La **Prepersonalización** puede ser formalizada tanto mediante el programa de utilidad DELTA/1 como (desde los programas **OEM**) mediante el uso directo de la API de bajo nivel contenida en el **driver** Q2_DRV32.DLL (macrofunción *142 Prepersonalizar_fS=4*). Evidentemente, este proceso podría ser seguido, sin solución de continuidad, por el proceso de **Personalización** (ver punto 07.3.2) antes de acabar el procesamiento de la **Acreditación** presentada, en cuyo caso se minimizarían las manipulaciones a realizar por el Operador del programa **OEM**.

07.3.2 Personalización

Para este tipo de **Acreditaciones** puede ser interesante, aunque no obligatorio, utilizar parte del **NUFAB**, formado por el 'Cascade Tag' y el UID (Unique IDentifier) de la propia **Acreditación**, para obtener el **NIS**. Esto puede tener la ventaja de la compatibilización con el formato **fS=3** (ver la Nota de Aplicación QAN-08).

Para ello el **driver** facilita el uso de la función *2 Leer_Acreditación*. El programa **OEM** deberá definir (Byte alto del campo ADDR) a partir de cual de los Bytes del **NUFAB** hay que empezar a leer los 4 Bytes que formarán el **NIS**. También debe tener en cuenta que, de tales 4 Bytes, sólo 31 bits serán válidos para el **NIS** (formato estándar del **sistema CONACC**), por lo que si activa el bit b1 del Byte bajo del campo ADDR se ahorrará tener que eliminar el bit de mayor peso.

Aunque el UID es único, hay que recortarlo para obtener el **NIS**. Es por tanto responsabilidad del programa **OEM** comprobar los **NIS** ya creados para garantizar que no exista nunca un duplicado.

07.3.3 "desprepersonalización"

Partiendo de la base de que toda **Acreditación** 'DESFire' dispone de una memoria que es finita en su tamaño, en ocasiones es posible que resulte necesario habilitar, para nuevo uso, la parte de memoria utilizada por una estructura **fS=4** cuya utilidad haya periclitado. Un ejemplo podría ser el de una gran organización dotada con muchos **centros operativos**(1), en la que cada uno de ellos, debido a que superaran en número al máximo permitido por el **sistema CONACC** para **centros operativos** 'secundarios', requiere de su propia estructura **fS=4**. Para poder trabajar con un número "ilimitado" de **centros operativos**, independientemente del tamaño de la memoria disponible en la **Acreditación**, el programa **OEM** deberá pasar por un proceso de "desprepersonalización" a la **Acreditación** del usuario que deba abandonar un centro para recuperar la memoria ocupada por la estructura **fS=4** que deja de tener vigencia(2). Cuando tal usuario ingrese en otro centro su **Acreditación** podrá ser sometida a una nueva **Prepersonalización** y **Personalización** (ver los puntos 07.3.1 y 07.3.2) y así hacer uso de los recursos de *Control de Accesos* en dicho **centro operativo**. Para tal proposito, las estructuras **fS=4** de los diferentes centros deberán utilizar el mismo nombre para el archivo, lo cual está predeterminado en la información contenida en **TInACC**, **TInACC/1** o **TInACC/2**) .

El programa **OEM** debería facilitar el acceso a los recursos que, para todo lo expuesto, aporta el **sistema CONACC**, para lo cual hay que utilizar la macrofunción *141 Transformar_14443* indicando el valor 0 en el parámetro 'TS' (Tipo Subfunción) y el valor adecuado al objetivo deseado en el parámetro 'O' (opciones)(3).

Si se utiliza autenticación por biometría "de dedo" o "de palma" y al "desprepersonalizar" la **Acreditación** se ha respetado el 'Template' existente, el programa **OEM** deberá también implementar un recurso para que el 'Template' contenido en el archivo $SF_{DATBIO3}$ o $SF_{DATBIO4}$ pueda ser integrado en la estructura **fS=4** generada en el **centro operativo** al que se adscribe la **Acreditación**. Para ello deberá utilizar la macrofunción *134 Desbloquear_fS=4* desactivando el bit b5 del mapa de bits existente en el quinto Byte que se habrá obtenido mediante la macrofunción *133 Analizar_fS=4* (la cual deberá haber sido ejecutada previamente).

NOTAS:
(1)
Para obtener información detallada de los diferentes recursos que el **sistema CONACC** ofrece para tratar con varios **centros operativos**, hay que ver el documento BTP024.

(2)
Si en la Instalación se utiliza autenticación por biometría “de dedo”, la única excepción a tal recuperación podría ser el espacio ocupado por el ‘Template’ dado que tal información se refiere estrictamente al usuario y, muy probablemente, también deba ser utilizada en el nuevo **centro operativo**.

(3)
Como consecuencia de esta actuación, desaparece de la **Acreditación** la estructura **fS=4** correspondiente al **centro operativo** que el usuario abandona. Sin embargo, sólo se produce una liberación teórica de la memoria, de manera que la Aplicación eliminada habrá desaparecido de manera lógica pero el espacio que ocupaba físicamente seguirá sin estar disponible, por lo que hay que tener en cuenta que la liberación física sólo podrá ser completa si no existe otra Aplicación (tanto de Qontinuum como de terceros) y los permisos actuales de la **Acreditación** lo permiten. De todos modos, si, por las razones anteriormente expuestas, no es posible 'vaciar' la **Acreditación** por completo, un uso reiterado de este recurso puede dejar a la **Acreditación** sin memoria disponible, para evitar lo cual el programa **OEM** puede activar el bit de más peso en el parámetro ‘O’ de la macrofunción *141 Transformar_14443* (**driver** Q2_DRV32.DLL Versión 08.07.00 y superiores). Con ello, el **driver** no elimina ni los archivos ni la Aplicación implicados, aunque si que borra el contenido de tales archivos y de sus claves, de tal manera que es posible generar otra estructura **fS=4** (mediante la pertinente **Prepersonalización**) encima de la que hubiera existido anteriormente sin ocupar un nuevo espacio físico en la memoria del elemento ‘DESFire’. La “desprepersonalización” también es posible realizarla desde el programa de utilidad DELTA/1, aunque en este caso siempre se realiza sobre toda la estructura **fS=4** y de manera completa, con la antedicha pérdida de memoria utilizable.

07.4 Coexistencia de Acreditaciones 'MIFARE' con Acreditaciones 'DESFire' en fS=4

En las instalaciones donde coexistan **Acreditaciones** 'MIFARE' y 'DESFire' y ambas deban ser usados de manera simultánea, puede ser conveniente que el programa **OEM** pueda diferenciar entre los dos tipos de **Acreditación**, para lo cual dispone de los siguientes métodos según el tipo de Terminal utilizado:

- Terminal *de Sobremesa* modelo MIF-8310 (y modelos anteriores compatibles):
  sólo admiten tratar la estructura **fS=4** en **Acreditaciones** 'MIFARE'.
- Terminales *de Sobremesa* modelo DEF-8311 y modelo DEF-3311(2):
  sólo admiten el tipo de elemento determinado por el campo 'TP' de la configuración de su Puerto COM(1):
  'TP' = 1 para **Acreditaciones** 'MIFARE'.
  'TP' = 5 para **Acreditaciones** 'DESFire'.
- Terminales normales de la Familia MIF:
  sólo aceptan **Acreditaciones** 'MIFARE'.
- Terminales normales de la Familia DEF(con FW Versión 08.02.00 o >>)(2):
  Es posible, al hacer una lectura con la función *2 Leer_Acreditación*, determinar la naturaleza de la **Acreditación** mediante el campo CR:
  CR = 101 en **Acreditaciones** 'MIFARE'.
  CR = 105 en **Acreditaciones** 'DESFire'.

De todos modos, y para averiguar de que tipo de **Acreditación** ('MIFARE' o 'DESFire') se trata cuando no existe grabada en ella ninguna estructura **fS=4**, es posible aplicar la metodología descrita en el punto 08.1 de la Nota de Aplicación QAN-08.

NOTAS:

(1)

Cuando la **Acreditación** no corresponda, el **driver** retornará un código de estado *05* ***fS=4*** *: estructura ilegible*, aunque para versiones de **driver** anteriores a la 08.06.01 puede retornar un código de estado *08* ***fS=4*** *: estructura inválida* con **Acreditaciones** 'DESFire' cuando TP=1.

(2)

Para poder tratar ambos tipos de **Acreditaciones** en **fS=4** es imprescindible que el **TInACC** utilizado este preparado para ello, de no ser así se rechazaran las **Acreditaciones** cuya naturaleza no coincida con la especificada en el **TInACC**.

código	título	relaciones
QAN-08	Terminales de la Familia MIF operando en formato **fS=3**	- MRT019 : capítulo 3 (*Direcciones 8 y 91*) - MRT019 : capítulos 4.6 - BTP033: referencias a la Familia MIF - Q2_UTIL : Versión 5.8 y >>
	Terminales de la Familia DEF operando en formato **fS=3**	- MRT019 : capítulo 3 (*Direcciones 8 y 91*) - MRT019 : capítulos 4.7 - BTP033: referencias a la Familia DEF - Q2_UTIL : Versión 6.0 y >>

La Familia MIF y la Familia DEF son específicas para operar con **Acreditaciones** dotadas con estructura **fS=4**. Sin embargo, y de manera excepcional, a partir de la Versión 06.02.00 del FW para los Terminales de la Familia MIF y de la Versión 08.00.00 del FW para los Terminales de la Familia DEF resulta posible instalar y tratar las **Acreditaciones** en "modo degradado", esto es en formato f**S=3** (por tanto, leyendo sólo el número de serie de la **Acreditación**).

Para tratar las **Acreditaciones** 'MIFARE' o 'DESFire' en formato **fS=3** existen en la Familia SEP, respectivamente, los Terminales de la Clase "F" y los Terminales de la Clase "D", por lo que la única razón justificable para aceptar tal disminución en las prestaciones (hay que tener en cuenta que los Terminales de la Familia MIF y de la Familia DEF resultan más caros al presentar más prestaciones) consiste en querer iniciar el funcionamiento de la Instalación sin requerir o sin utilizar la infraestructura necesaria para el formato **fS=4** (por ejemplo, el Kit MIF-500 o el Kit DEF-500) y sin, por tanto, la responsabilidad de tener que acometer la **Prepersonalización** y la **Personalización** de las **Acreditaciones** 'MIFARE' o 'DESFire'.

Para las Instalaciones dotadas con **Acreditaciones** 'MIFARE' y que dispongan del **driver** Versión 07.00.00 y >> y del FW Versión 06.02.00 y >>, al trabajar en formato **fS=3**, de los 4 Bytes que contienen el NUID (Non-Unique IDentifier) el FW de los Terminales toma sólo los 31 bits de menor peso para formar el **NIS**, de manera que los valores posibles quedan situados entre 1 y 2147483647. Esta limitación también se aplica al **NIS** al trabajar en formato **fS=4** (esto es así dado que el concepto que justifica al **NIS** es común en el **sistema CONACC**), por lo que en aquellas Instalaciones en las que se comience trabajando en formato **fS=3** para, posteriormente, pasar a trabajar en formato **fS=4**, el **NIS** se mantiene (y con él todos los marcajes existentes hasta el momento del cambio).

Para las Instalaciones dotadas con **Acreditaciones** 'MIFARE' y que dispongan del **driver** Versión 07.01.00 y >> y del FW Versión 06.04.00 y >> y para las Instalaciones dotadas con **Acreditaciones** 'DESFire' que dispongan del **driver** Versión 08.00.00 y >> y del FW Versión 08.00.00 y >>, al trabajar en formato **fS=3**, de los 4 Bytes que contienen el NUID (en **Acreditaciones** 'MIFARE') o de los 7 Bytes que contienen el UID (en **Acreditaciones** 'DESFire') el FW de los Terminales tomará los 31 bits de menor peso (como en el caso anterior) o tomará los 32 bits, de manera que el **NIS** quedará formado por el NUID al completo ('MIFARE') o por los 4 Bytes menos significativos del UID ('DESFire').

Para utilizar los 32 bits, el programa **OEM** deberá definir la **Lista_Blanca** o la **Lista_Negra** y/o la Lista_Especial y/o la Lista_Otras_Prestaciones indicando la existencia del Byte extra llamado *marcador* (ver lo especificado para el bit b7 del Nibble alto de la *Dirección 8* en el capítulo 3), aunque entonces se producirá una incompatibilidad formal de los **NIS** así construídos entre el formato **fS=3** y el formato **fS=4**, de manera que, cuando tal conversión sea necesaria(1), el programa **OEM** deberá eliminar el bit de mayor peso (una manera de hacerlo sería pasar el valor de cada **NIS** de decimal a hexadecimal, forzar a cero el bit de mayor peso del Byte de mayor peso y pasar el nuevo valor hexadecimal a decimal); en el muy remoto caso de que se produzca un duplicado del valor obtenido (una posibilidad entre 2.147.483.647), el programa **OEM** debería advertirlo y forzar el cambio de una de las dos **Acreditaciones** por otra (por supuesto, con las comprobaciones de rigor para evitar un nuevo duplicado de **NIS**)(2).

Una de las características de las Instalaciones que usan **Acreditaciones** dotadas con la estructura **fS=4** es el necesario uso concurrente de los **TInCap** (**TInCLA**, **TInACC**, etc.), de manera que una Instalación no puede funcionar con Terminales de la Familia MIF o de la Familia DEF sin la presencia del elemento **TInCap** adecuado. Sin embargo, es posible forzar a los Terminales de la Familia MIF (usando el FW Versión 06.02.00 y posteriores y el programa de utilidad Q2_UTIL Versión 05.08.00 y posteriores) y a los Terminales de la Familia DEF (usando el FW Versión 08.00.00 y posteriores y el programa de utilidad Q2_UTIL Versión 06.00.00 y posteriores) a operar en formato **fS=3**, para lo cual, y con independencia de la presencia o no de un **TInCap**, no hay que "preconfigurar" al Terminal utilizando la opción *Instalar_fS=4* del grupo *Funciones* del programa de utilidad Q2_UTIL sino utilizando la opción *Instalar_Terminal* del mismo grupo, en cuyo caso, y dado que se pretende efectuar la "preconfiguración" de un Terminal de la Familia MIF o de la Familia DEF a un formato **fS=n** que no es el 4, el Operador de Q2_UTIL recibirá una advertencia al respecto. Con idéntica intención de informar al Operador, el programa **OEM** debería advertir al Operador de tal situación si la "preconfiguración" se realiza desde el programa **OEM** utilizando la función *28 Instalar_Terminal* en detrimento de la macrofunción *129 Instalar_fS=4* (ambas forman parte de la API de bajo nivel contenida en el **driver** Q2_DRV32.DLL), para lo cual deberá analizar el 'código Producto' (mediante la función *19 Leer_FW*) y deducir si el Terminal es de la Familia MIF o de la Familia DEF (la relación entre las Familias y cada 'código Producto' aparece en la Ayuda para Q2_UTIL en la entrada : *código Producto*).

NOTAS:
(1)
La conversión no sería necesaria en el caso de que, aunque la Instalación quisiera pasar de formato **fS=3** a formato **fS=4**, no tuviera importancia alguna la información existente hasta el momento (numeración de las **Acreditaciones** 'MIFARE' o 'DESFire' entregadas a los usuarios, marcajes recogidos, etc.), de manera que, en la práctica, resultaría en una puesta en marcha partiendo de cero y en la que, por tanto, la generación de los **NIS** podría ser por completo independiente de los NUID o de los UID de las **Acreditaciones**.

(2)
Como dato para ser evaluado, la mayoría de los Cabezales sólo lectores existentes en el mercado que tratan **Acreditaciones** 'MIFARE' lo hacen leyendo sólo el NUID y comunicándolo por medio de un interfaz 'Wiegand 26' (así llamado por transmitir 24 bits de datos y dos de paridad), de manera que ante una resolución de 24 bits sobre 32 la posibilidad de duplicado es de 1 entre 16.777.215, y tal cosa ocurre sin tener en cuenta, además, la problemática que se produce actualmente al existir duplicidades en los NUID dado que se están fabricando clónicos (para más información hay que ver el documento "MIFARE : las preguntas".

08.1 Coexistencia de Acreditaciones 'MIFARE' con Acreditaciones 'DESFire'

En las Instalaciones donde coexistan **Acreditaciones** 'MIFARE' y 'DESFire' y ambas deban ser usadas de manera simultánea, puede ser conveniente que el programa **OEM** pueda diferenciar entre los dos tipos de **Acreditación**, para lo cual dispone de los siguientes métodos según el tipo de Terminal utilizado:

- Terminal *de Sobremesa* modelo MIF-8310 (y modelos anteriores compatibles):
  hay que utilizar la función *2 Leer_Acreditación* y analizar el Byte de menor peso(1).
- Terminal *de Sobremesa* modelo DEF-8311 y modelo DEF-3311 :
  depende del campo 'TP' de la configuración de su Puerto COM :
  'TP' = 1 : hay que utilizar la función *2 Leer_Acreditación* para leer el **NIS** y analizar el Byte de menor peso(1).
  'TP' = 5 : sólo se aceptan **Acreditaciones** 'DESFire' dado que las **Acreditaciones** 'MIFARE' son rechazadas sistemáticamente.
- Terminal normal de la Familia MIF :
  hay que utilizar la función *2 Leer_Acreditación* para leer el **NIS** y analizar el Byte de menor peso(1).
- Terminal normal de la Familia DEF :
  - si ha sido preconfigurado utilizando la función *28 Instalar_Terminal* para cargar el parámetro 'IM' con el bit b26 = 0, no hay duda posible ya que las **Acreditaciones** 'MIFARE' serán rechazadas sistemáticamente.
  - si ha sido preconfigurado utilizando la función *28 Instalar_Terminal* para cargar el parámetro 'IM' con el bit b26 = 1, es posible, haciendo una lectura con la función *2 Leer_Acreditación*, determinar la naturaleza de la **Acreditación** al analizar el Byte de menor peso(1) o, mejor todavía pero siempre y cuando el FW sea de la Versión 08.02.00 o >>, analizando el contenido del campo CR :
    CR = 101 : la **Acreditación** es 'MIFARE';
    CR = 105 : la **Acreditación** es 'DESFire'.

NOTAS:

(1)

Según la normativa ISO/IEC 14443-3, cuando el número de serie es simple, como en las **Acreditaciones** 'MIFARE' *Classic*, se entrega en una trama de 4 Bytes. Cuando el número de serie es doble (7 Bytes), como en las Acreditaciones 'DESFire', se fragmenta en dos tramas de 4 Bytes cada una, siendo el primer Byte de la primera trama un código llamado 'Cascade Tag' (CT) con valor 88h, para indicar que aún no se ha completado el número de serie. Dicho valor, al ser reservado, no es posible encontrarlo en el primer Byte de un número de serie simple. Cuando se lee el número de serie de una **Acreditación** 'DESFire' en un Cabezal 'MIFARE' se obtiene sólo la primera trama como si de un número de serie simple se tratara. Así pues, analizando el primer Byte (el de menor peso), podemos discernir de que tipo de **Acreditación** se trata (88h para 'DESFire' y cualquier otro valor para 'MIFARE'). Si se pretende hacer el análisis a partir del **NIS** obtenido por un Terminal de Qontinuum, se debe cumplir con los siguientes requisitos:

- el offset debe ser 0 : en los Terminales normales se declara este valor en el parámetro 'OFFSET NIS PARA FORMATO FS=3' (dirección 61 en el capítulo 3);
- si se invierte el orden modificando el tipo de notación a HL (bit b2 = 1 en el campo ADDR en la función *2 Leer_Acreditación* con Terminales *de Sobremesa* o con el bit b4 = 1 del parámetro 'MÁSCARA MISCELÁNEA 3' con Terminales normales), debe analizarse el último Byte y no el primero; en este caso, sin embargo, sólo es posible garantizar el resultado si se usa el formato ampliado del **NIS** (bit b1 = 1 en el campo ADDR en la función *2 Leer_Acreditación* con Terminales *de Sobremesa* o con el bit b7 = 1 del parámetro 'TIPO DE LISTA' con Terminales normales).

ESTA PÁGINA HA SIDO DEJADA EN BLANCO INTENCIONADAMENTE

código	título	relaciones
QAN-09	Consideraciones sobre la biometría "de dedo" y "de palma" en las Familias MIF y DEF (para **fS=4**)	- MRT019 : capítulo 5 (macrofunciones *133*, *134* y *138*) - BTP031: **Acreditaciones** 'MIFARE' y 'DESFire' - BTP036 (Revisión C y >>) : subcapítulos 4.1 y 5.1

Dado que esta Nota de Aplicación afecta tanto a los 'Templates' correspondientes a la biometría "de dedo" como a la "de palma", y para unificar nomenclatura, se hace referencia a los archivos que contienen a los 'Template' correspondientes no como $NB_{DATBIO3}$ ("de dedo" en Familia MIF) ni como $SF_{DATBIO3}$ ("de dedo" en Familia DEF) sino como $XX_{DATBIO3}$, mientras que se hace referencia al archivo $SF_{DATBIO4}$ ("de palma" en Familia DEF) dado que sólo existe en esta Familia.

09.1 Antecedentes

Una de las características fundacionales del **sistema CONACC** en lo que afecta a las estructuras **fS=4** es su capacidad para extender los recursos operativos no solo en la Instalación en la que han sido emitidas (el conocido **centro operativo** 'primario') sino también en otros centros físicamente separados pero lógicamente dependientes (los llamados **centros operativos** 'secundarios'). Sin embargo, y aunque no sea un planteamiento habitual, el **sistema CONACC** también contempla la posibilidad de que dos o más Instalaciones (por completo independientes entre ellas en lo que refiere a la emisión de **Acreditaciones** dotadas con estructuras **fS=4**) puedan ver necesario un cierto grado de colaboración para facilitar que las **Estructuras** emitidas en una de las Instalaciones también puedan ser operativas en las otras(1). Para ello se hace necesario que cada una de tales Instalaciones (además de la primera) generen y graben su propia estructura **fS=4** en las **Acreditaciones**, pero, y por ahorrar el máximo posible de la memoria disponible en ellas, aprovechando aquella información que es forzosamente de uso común dado que es inherente al usuario, cual es el 'Template' correspondiente a la biometría "de dedo" y/o "de palma".

El **sistema CONACC** establece unas condiciones de control muy estrictas para garantizar la integridad de la información contenida en cada estructura **fS=4**. El control de integridad también afecta al posible 'Template' grabado en una **Acreditación** 'MIFARE' o 'DESFire', de manera que, para que tal 'Template' pueda ser usado, el archivo $XX_{DATBIO3}$ y/o el archivo $SF_{DATBIO4}$ debe formar parte de tal estructura **fS=4**.

En el **sistema CONACC** llamamos 'integración de un 'Template' al proceso por el cual el archivo $XX_{DATBIO3}$ y/o el archivo $SF_{DATBIO4}$ (recién creado/s o proveniente/s de otro **centro operativo**) pasa/n a formar parte, bajo el punto de vista del antedicho control de integridad, de la estructura **fS=4** correspondiente al **centro operativo** del que se trate.

09.2 Integración de 'Template'

En términos generales, cuando en una Instalación (**centro operativo**) se establece la autenticación biométrica de los usuarios, éstos son enrolados desde el programa **OEM** y el 'Template' dimanante es grabado en la estructura **fS=4** juntamente con la información necesaria para la utilización de la **Acreditación**, todo ello en la fase de **Personalización** (ver la Nota de Aplicación QAN-04 y los puntos 07.2.2 y 07.3.2 en la Nota de Aplicación QAN-07). Sin embargo, y partiendo del punto de vista de una Instalación (a la que llamaremos A), puede darse el caso de que un usuario haya sido enrolado en otra Instalación (a la que llamaremos B), por lo cual su 'Template' está integrado en esa estructura **fS=4** (la correspondiente a la Instalación B), pero no está integrado en la estructura **fS=4** de la Instalación A. Como consecuencia, todo intento de autenticación biométrica del usuario en la Instalación A resulta fallida (el FW genera un **marcaje normal** con CE=81), por lo que tal **Acreditación** no será plenamente utilizable hasta que haya sido sometida a un proceso de integración.

Resumiendo, y dada una Instalación, la integración del archivo $XX_{DATBIO3}$ o del archivo $SF_{DATBIO4}$ en la estructura **fS=4** correspondiente se realiza por una de dos vías distintas:

1 - integración implícita en el proceso de **Personalización** por medio de la macrofunción *138 Enrolar_fS=4*;

2 - integración explícita por medio de la macrofunción *134 Desbloquear_fS=4*.

La utilización de la primera vía resulta obvia cuando en la **Acreditación** sólo existe una estructura **fS=4**, pero la utilización de la segunda vía resulta obligada cuando se trata de una **Acreditación** que contiene más de una estructura **fS=4** (la de la propia Instalación y una o más correspondientes a otra u otras Instalaciones)[(2)] y en el que el archivo $XX_{DATBIO3}$ o el archivo $SF_{DATBIO4}$ ha sido generado por cualquiera de ellas (excepto en la propia Instalación), de manera que cuando un usuario utiliza su **Acreditación** en un Terminal biométrico, éste lo rechaza al detectar que el archivo $XX_{DATBIO3}$ o el archivo $SF_{DATBIO4}$ no está integrado en la estructura **fS=4** correspondiente a la Instalación.

09.2.1 un ejemplo

Se trata de una gran organización en la que, por razones que están fuera del alcance de este documento, existen dos (aunque podrían llegar a ser más) **centros operativos** 'primarios', de manera que desde cada uno de ellos se define y administra toda la información correspondiente a sus usuarios (de manera coherente con la arquitectura del **sistema CONACC** para las estructuras **fS=4**, cada uno de tales **centros operativos** 'primarios' puede, a su vez, disponer de **centros operativos** 'secundarios' y/o de **unidades operativas**). Además, cada uno de tales **centros operativos** dispone de un programa **OEM** (que puede ser del mismo proveedor o no serlo, aunque todos deben integrar el **sistema CONACC**), disponiendo y administrando cada uno de tales programas de aplicación su propia Base de Datos.

Dado que en tal gran organización se pretende que los usuarios dispongan de una única **Acreditación**, se ha escogido 'MIFARE' o 'DESFire' (con independencia de que en la **Acreditación** coexistan otras tecnologías) por la facilidad que otorga para la llamada "multioperatividad" (característica ésta en la que se basa el concepto formato **fS=4** y todo el desarrollo dimanante). De manera consecuente, los programas **OEM** situados en cada **centro operativo** realizarán la **Personalización** en las **Acreditaciones**, incluyendo en la estructura **fS=4**, si fuera el caso, el 'Template' correspondiente a la biometría "de dedo" y/o "de palma" del usuario.

Todos los usuarios están adscritos únicamente a un **centro operativo**, razón por la cual en cada **Acreditación** existe la correspondiente estructura **fS=4** (a efectos de este ejemplo, se considera que también existe un 'Template'). En cualquier momento en el tiempo, un usuario debe ser adscrito a otro **centro operativo** (por traslado temporal, cursillo, etc.). Para ello, el usuario, al llegar al nuevo **centro operativo** (a efectos de este ejemplo lo llamaremos **centro operativo** "en curso"), entregará su **Acreditación** para que en ésta sea grabada la estructura **fS=4** correspondiente, para lo cual el programa **OEM** deberá implementar los siguientes pasos (utilizando los recursos de la API):

1) **Prepersonalización** de la **Acreditación** mediante la macrofunción *142 Prepersonalizar_fS=4*, de manera que quede generada la nueva estructura **fS=4** (la correspondiente al **centro operativo** "en curso");

2) **Personalización** de la **Acreditación** mediante la macrofunción *130 Grabar_fS=4* para el **centro operativo** "en curso", de manera que la estructura **fS=4** queda cargada con la información correspondiente al usuario;

3) análisis del contenido de la estructura **fS=4** correspondiente al **centro operativo** "en curso" mediante la macrofunción *133 Analizar_fS=4*, lo cual permite detectar la existencia del archivo $XX_{DATBIO3}$ y/o del archivo $SF_{DATBIO4}$ (el que contiene al 'Template' y que, en este ejemplo, fue grabado en origen); dado que tal/es archivo/s existe/n, el **driver** lo indica mediante el bit b6 y/o el bit b3 del sexto Byte, pero dado que tal/es archivo/s no está/n integrado/s en la estructura **fS=4** correspondiente al **centro operativo** "en curso", el **driver** también lo indica mediante el bit b5 y/o el bit b6 del quinto Byte.

4) como consecuencia, el archivo $XX_{DATBIO3}$ y/o el archivo $SF_{DATBIO4}$ existente/s en la **Acreditación** debe/n ser integrado/s en la estructura **fS=4** correspondiente al **centro operativo** "en curso", para lo cual se utiliza la macrofunción *134 Desbloquear_fS=4* una vez cambiado el valor del bit b5 y/o el bit b6 del quinto Byte, aunque tal cosa sólo debe ser hecha después de que, y por estrictas razones de seguridad, el programa **OEM** haya forzado la verificación del usuario, para lo cual deberá implementar en el programa la lógica necesaria para requerir una presentación biométrica adecuada y para realizar la oportuna validación del 'Template' obtenido con el existente, garantizando así que el 'Template' existente en la estructura **fS=4** corresponde realmente al usuario portador de la **Acreditación**.

A partir de que el programa **OEM** haya realizado los pasos expuestos, la **Acreditación** de tal usuario pasa a disponer de la estructura **fS=4** original (correspondiente al otro **centro operativo**) más la estructura **fS=4** recién generada (correspondiente al **centro operativo** "en curso"), existiendo un único archivo $XX_{DATBIO3}$ y/o $SF_{DATBIO4}$ en la **Acreditación** que está integrado con ambas estructuras **fS=4**, de manera que es directamente utilizable en cualquiera de ellas.
El planteamiento expuesto no hay que entenderlo como limitado a sólo dos **centros operativos**, dado que puede formalizarse también para otros (la única limitación viene impuesta por la memoria disponible en las **Acreditaciones**).

09.3 Procedimientos a seguir ante la pérdida de una Acreditación

Dado que una **Acreditación** siempre puede ser extraviada, los programas **OEM** deben aportar al Operador los procedimientos funcionales adecuados para la generación de una nueva **Acreditación** que substituya a la perdida. Una vez declarada la pérdida de la **Acreditación,** y una vez que el Operador haya cargado (utilizando para ello los recursos aportados por el programa **OEM**) en la **Lista_Negra** de sus Terminales (ver el capítulo 2.2 de la Revisión P2 y superiores del documento BTP027) el **NIS** contenido en la estructura **fS=4** vigente de la **Acreditación** perdida, el Operador utilizará otros procedimientos que tomarán información de la Base de Datos, aplicarán un nuevo **NIS** y culminarán en la **Personalización** de la nueva **Acreditación** (ver los puntos 07.2.2 y 07.3.2 en la Nota de Aplicación QAN-07). En esta situación, el 'Template' será tomado por el programa **OEM** del correspondiente elemento "biodato3"[(3)] y/o "biodato4"[(3)] y grabado en el archivo $XX_{DATBIO3}$ y/o en el archivo $SF_{DATBIO4}$ por la macrofunción *138 Enrolar_fS=4*, quedando por tanto integrado en la estructura **fS=4**. Finalmente, la nueva **Acreditación** será entregada al usuario correspondiente.

Para la mayoría de las situaciones (como ocurre con las Instalaciones que tengan un único **centro operativo** 'primario'), los procedimientos descritos en el párrafo anterior deberían ser suficientes. Sin embargo, en aquellas situaciones en las que exista más de un actor (como ocurre con aquellas Instalaciones que tengan más de un **centro operativo** 'primario' o con aquellas Instalaciones totalmente independientes pero que mantengan el vínculo que representa la utilización de las mismas **Acreditaciones** en ambas Instalaciones), aparece la necesidad de que el Operador del sistema en la Instalación en la cual ha sido declarada la perdida de la **Acreditación** asuma la responsabilidad de dar a conocer tal hecho a todas las demás Instalaciones vinculadas, de manera que también ellas puedan cargar sus **Listas_Negras**. Una última consideración ante esta situación consiste en aclarar que la generación de una nueva **Acreditación** puede ser realizada desde cualquiera de las Instalaciones vinculadas dado que todas ellas disponen de información suficiente sobre el usuario (la cual debe incluir el 'Template'[(3)]), de manera que a medida que el usuario pretenda acceder a otras Instalaciones vinculadas, éstas deberán generar sus propias estructuras **fS=4** y formalizar una integración explícita del 'Template' (ver el punto 09.2).

09.4 Exportación e Importación de un 'Template'

Una de las pretensiones del **sistema CONACC** es la de permitir, en la medida de lo posible y de lo deseable, la compatibilidad biométrica[(4)] entre sistemas y entre Instalaciones. Para ello, el **sistema CONACC** aporta un recurso que permite la desvinculación del 'Template' de la estructura **fS=4** de la que forma parte, así como también aporta un recurso para la vinculación a la estructura **fS=4** de un 'Template' generado externamente.

Si un programa **OEM** pretendiera cargar un 'Template' desvinculado (contenido en un elemento "biodato3x" o "biodato4x") debería utilizar la secuencia normal de llamar a las subfunciones 5 y 3 de la macrofunción *138 Enrolar_fS=4*), aunque el **driver** rechazaría tal pretensión ya en la subfunción 5 (retornando el código de estado 19) al detectar la falta de vinculación inherente a todo elemento "biodato3x" y "biodato4x".

Para este tipo de situación debe existir un acuerdo previo entre los actores sobre cual de ellos es el responsable de aportar físicamente la nueva **Acreditación**, así como también sobre cual de ellos recae la responsabilidad del enrolamiento de los usuarios (fundamentalmente, estamos ante la misma situación que se produce en la primera emisión de **Acreditaciones**).

NOTAS:

(1)

Con la intención de no tener que utilizar más de una **Acreditación** por usuario, podría darse el caso de que, para una misma **Acreditación**, fuera conveniente disponer de dos o más estructuras **fS=4**, las cuales, aún siendo totalmente independientes, estarían, obviamente, referidas al mismo usuario.

(2)

Cada una de tales estructuras define al usuario para su interacción con los Terminales de cada una de las correspondientes Instalaciones, las cuales puede ser que, incluso, no tengan absolutamente ninguna relación entre ellas.

(3)

Para ayudar a superar este tipo de situaciones es por lo que consideramos muy importante que todos los programas **OEM** materialicen un archivo que contenga a todos los elementos “biodato3” y/o “biodato4” a medida que los vaya generando en el proceso de enrolamiento de los usuarios y/o a medida que los puedan obtener en el proceso de integración de ‘Template’. La descripción de los elementos “biodato3” y “biodato4” aparece en el capítulo <Elementos “biodato”> de la Revisión C y superiores del documento BTP036.

(4)

La condición imprescindible para la compatibilidad de la biometría “de dedo” es la de que pueda ser utilizada por sistemas de distintos fabricantes, razón por la que los sistemas de Qontinuum cumplen la norma ISO/IEC 19794-2 dado que los ‘Templates’ que cumplen dicha norma están exentos de las características “propietarias” de cada fabricante, características éstas que hacen incompatibles a tales ‘Templates’ cuando se pretende usarlos en un sistema habiendo sido generados en otro.

La condición imprescindible para la compatibilidad de la biometría “de palma” (sistema de un único fabricante) es la de que todas aquellas Instalaciones que quieran compatibilidad utilicen la misma “application key” suministrada por el fabricante.

ESTA PÁGINA HA SIDO DEJADA EN BLANCO INTENCIONADAMENTE

código	título	relaciones
QAN-10	Consideraciones sobre el **Estado Operativo** de una estructura **fS=4**	- MRT019 : capítulo 3 (*Direcciones 23-24, 35, 91, 95 y 96*) - BTP036 (Revisión C y >>): subcapítulos 4.1 y 5.1

Este nuevo mecanismo lógico (introducido en la Revisión W de las especificaciones del **sistema CONACC**) establece un control estricto sobre el **Estado Operativo** de las **Acreditaciones**, de manera que aquellas en cuya estructura **fS=4** (la que se esté tratando) conste indicado que está 'desactivada', son rechazadas de inmediato con la generación de un **marcaje normal** con CE=24 (este mecanismo afecta a la Versión 8.0 y posteriores de los FW específicos de *Control de Accesos* para tratar estructuras **fS=4** sobre **Acreditaciones** 7816-4, 'MIFARE' y 'DESFire').

10.1 Antecedentes

Una de las posibles vulnerabilidades en la seguridad que se puede producir consiste en el uso de una **Acreditación** por parte de alguien que no sea el usuario legítimo.

En Instalaciones dotadas con sistemas tradicionales (donde cada **Acreditación** se identifica sólo por un código y toda la información radica en los Terminales) este tipo de vulnerabilidad resulta por completo incontrolable, así como también lo es en la utilización de sistemas mucho más evolucionados como los que leen y graban en la memoria de las **Acreditaciones** en tiempo real de acceso (por ejemplo, las estructuras **fS=4** de Qontinuum) puesto que nada impide a una persona utilizar la **Acreditación** de otra. En ambos casos, y para minimizar el adverso impacto de la suplantación, se puede implantar la autenticación mediante **IDEP** por presentación biométrica (el **PIN** no deja de ser, en cierta medida, vulnerable) en cada punto de acceso, aunque ello podría implicar un sobrecoste muy importante para la Instalación.

La solución a este problema consiste en la implementación de un mecanismo lógico que permite establecer y controlar el **Estado Operativo** de las estructuras **fS=4**, de manera que cuando el usuario abandona el recinto protegido, la **Acreditación** utilizada queda 'desactivada' para cualquier nuevo uso, debiendo forzosamente ser 'activada' de nuevo pero pudiendo sólo serlo por el usuario autorizado dado que éste debe ser autenticado mediante **IDEP** por presentación biométrica.

10.2 Procedimientos a seguir por parte del programa OEM

Para que el **Estado Operativo** de la estructura **fS=4** que se esté tratando quede 'desactivado', el programa **OEM** debe activar el bit b3 del parámetro 'MÁSCARA MISCELÁNEA 3' pero sólo en aquellos Terminales que estén situados en los puntos de salida del recinto de la Instalación, de manera que, a partir de ese momento, tal estructura **fS=4** (y por extensión la **Acreditación** que la contiene) dejará de ser operativa en todos los Terminales (de cualquier especialidad) que puedan existir en la Instalación (la **Acreditación** será rechazada con la generación de un **marcaje normal** con CE=24). La única excepción se produce en aquellos Terminales biométricos (también de cualquier especialidad aunque, por razones obvias, deberían ser de C.A.) que estén situados en los puntos de entrada del recinto de la Instalación, los cuales no rechazarán a las **Acreditaciones** con la estructura **fS=4** 'desactivada' siempre que el programa **OEM** haya cargado el valor 7 en el subparámetro **tipo autenticación**'(1), en cuyo caso el FW ignorará tal 'desactivación' y procederá con las validaciones oportunas y, si la autenticación biométrica del usuario resulta correcta, 'activará' el **Estado Operativo** de la estructura **fS=4** y completará el proceso, con lo que la **Acreditación** habrá vuelto al circuito funcional de la Instalación.

Por si se diera el caso de que los Terminales situados en los puntos de entrada del recinto de la Instalación no pudieran ser biométricos, los Terminales instalados deberán admitir **Acreditaciones** cuya estructura **fS=4** presente el **Estado Operativo** como 'desactivado', para lograr lo cual el programa **OEM** deberá activar el bit b1 del parámetro 'MÁSCARA MISCELÁNEA 4'; en consecuencia, y con independencia del tipo real de tales Terminales, el FW tomará como valor 0 cualquier otro valor que pueda constar en el subparámetro **tipo autenticación**.

Si fuera necesario que los Terminales situados en los puntos de salida del recinto de la Instalación permitan el paso a todas las **Acreditaciones**, el programa **OEM** debe activar el bit b1 del parámetro 'MÁSCARA MISCELÁNEA 4' así como el bit b3 del parámetro 'MÁSCARA MISCELÁNEA 3', de manera que tales Terminales, sin negar la salida a ningún usuario, dejarán 'desactivadas' a las estructuras **fS=4** que todavía no lo estuvieran.

Dado un Terminal, también resulta posible que la 'desactivación' se produzca sólo en aquellas estructuras **fS=4** que indiquen su pertenencia a un **grupo Usuario** concreto, para lo cual hay que activar el bit b2 del parámetro 'MÁSCARA MISCELÁNEA 4' además de cargar el número de tal **grupo Usuario** en el parámetro 'GRUPO USUARIO POR DEFECTO'. Tal posibilidad permite que un mismo Terminal 'desactive' sólo las **Acreditaciones** asignadas, por ejemplo, a los Visitantes, de manera que los Usuarios que sean personal de la propia empresa no vean afectado el **Estado Operativo** de la estructura **fS=4** contenida en sus **Acreditaciones**.

Mediante el uso del bit b7 del quinto Byte de la macrofunción *133 Analizar_fS=4*, el programa **OEM** puede conocer el **Estado Operativo** de una estructura **fS=4**, de manera que, si fuera imprescindible hacerlo, puede forzar la 'activación' mediante el uso del bit b7 del quinto Byte de la macrofunción *134 Desbloquear_fS=4*.

También resulta posible forzar la activación desde un Terminal mediante el uso del bit b4 del campo 'Miscelánea' de la Lista_Actualización.

NOTAS:

(1)

Si el bit b7 del parámetro 'IM' (cargado por la macrofunción *129 Instalar_fS=4*) está desactivado, se genera un **marcaje normal** con CE=20.

código	título	relaciones
QAN-11	El subsistema **VirGO** **** Documento obsoleto ****	- MRT019 : capítulo 5 (funciones *0, 19 y 33*) (funciones 'librería' *153*, *156* y *157*) - BTP030 (Revisión R y >>) - BTP037 (Revisión K3) - FW : Versión 08.00.00 y >>) - Q2_DRV32 : Versión 8.0 y >>) - Q2_UTIL : Versión 6.0 y >>

En términos generales, los programas **OEM** que de manera sistemática, y por razones que escapan a este documento, deban estar recogiendo en los Terminales los marcajes a medida que éstos se producen, se enfrentan a la labor de iterar (cambiando el ID cada vez) el uso de la función *16 Leer_RAM* (apuntando a la dirección del parámetro 'PUNTERO_LISTA_MARCAJES' o del parámetro 'PUNTERO_LISTA_MARCAJES_CDP') por cada uno de los Terminales existentes en la Instalación, de manera que, si existen muchos Terminales, el tiempo de "refresco-de-la-información" puede llegar a ser grande dado que una vez comprobado un Terminal no se volverá a hacer hasta haber comprobado a todos los demás.

El escenario anteriormente descrito resultó aliviado, en el factor tiempo, cuando implementamos la Versión 6.0 del **driver**, dado que desde entonces se pudo tratar de manera concurrente, mediante el uso de 'threads' independientes, a los Terminales conectados a cada Bus RS-485. Si bien es cierto que con este método se logra una sustancial mejora en los tiempos globales al actuar tales 'thread' en paralelo, no se evita la erosión sistemática del ancho de banda disponible en las comunicaciones por red basadas en TCP/IP/Ethernet, además de no conseguir, en la mayoría de las ocasiones, el menor tiempo posible entre la generación de una situación en un Terminal (un marcaje, una Alarma, una Advertencia, etc.) y el conocimiento de tal situación por parte del programa **OEM** dado que las comunicaciones siguen siendo **master**-**slave** entre el programa y los Terminales (lo llamamos "primer paradigma").

La actual propuesta consiste en la implementación del subsistema **VirGO**, el cual aporta un cambio sustancial del planteamiento (lo llamamos "segundo paradigma") en las comunicaciones por red, de manera que éstas se agilizan y potencian (una explicación muy amplia se encuentra en el documento BTP037).

Aunque los conceptos marcados en negrita están explicados en el capítulo 8 GLOSARIO DE TÉRMINOS, y para la mejor interpretación de los esquemas que aparecen en los siguientes subcapítulos, es conveniente puntualizar que una **capa VirGO** requiere de la existencia de la **capa Gateway**, la cual, a su vez, sólo puede operar en los **elementos IP** de Qontinuum,

11.1 Configuración del subsistema VirGO usando la API

Para configurar el subsistema **VirGO** utilizando la API de nivel bajo Q2_DRV32.DLL hay que seguir los siguientes pasos:

11.1.1 Activación de las capas VirGO

En cada equipo dotado con **capa VirGO** hay que activar ésta de la manera indicada en los siguientes párrafos.

El Operador del programa debe ejecutar las operaciones que se indican en el subcapítulo 8.3.1 (hasta acabar el paso 9) en la Revisión C y posteriores del documento BTP037.

A continuación, el programa **OEM** debe ejecutar las siguientes funciones de la API:

- *0 Ini_PORT:1:21* (b4 de NR = 0) para abrir un Puerto 'socket' con la dirección IP 192.168.1.1, Puerto TCP 1500.
- *33 Reconfigurar_VirGO* pasando como parámetros la nueva dirección IP de la **capa VirGO**, el puerto TCP, la dirección IP del Servidor **VirGO** y el Puerto en el Servidor **VirGO** (cada **capa VirGO** debe tener un número de Puerto diferente en el Servidor **VirGO**).
- *18 Reset* para que los parámetros configurados con la función *33 Reconfigurar_VirGO* pasen a ser efectivos.
- *0 Ini_PORT:0* para cerrar el Puerto 'socket'.

El Operador del programa debe ejecutar las operaciones que se indican en el subcapítulo 8.3.1 (a partir del paso18) en la Revisión C y posteriores del documento BTP037.

11.1.2 Configuración de los puertos en el PC que comunica con los Terminales

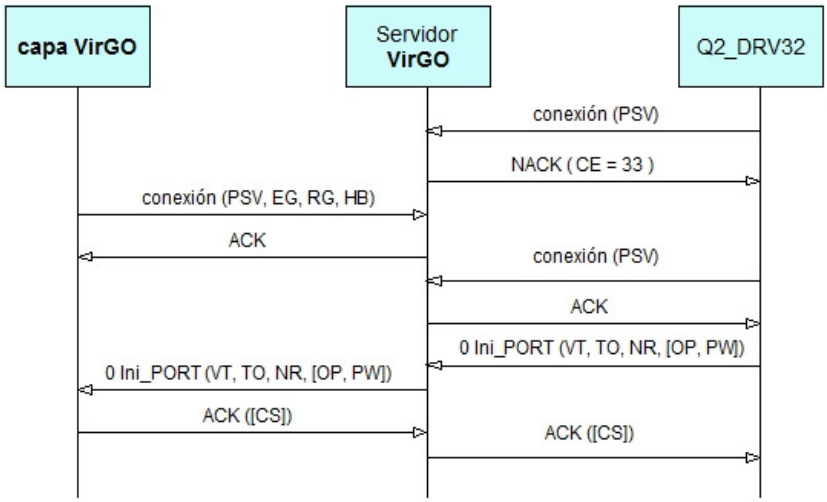
El programa **OEM** debe ejecutar las siguientes funciones de la API:

- *157 Gestión_VirGO* para dar de alta los diferentes Servidores **VirGO** que se vaya a tener.
- *0 Ini_PORT:1:12* (b4 de NR = 1) para 'tomar el uso del Puerto' que permitirá comunicar con cualquier equipo dotado con **capa VirGO** (y por extensión con el/los Terminal(es) dependientes, si los hay).

11.2 Conexión de una capa VirGO al Servicio VirGO

La **capa VirGO** establecerá conexión a nivel TCP/IP y después enviará una trama con los parámetros 'PSV', 'EG', 'RG' y 'HB'. Si el Servicio **VirGO** ya tiene conectado otra **capa VirGO** con el mismo 'PSV' retornará un NACK. La **capa VirGO** cerrará la conexión y volverá a intentar establecerla (esta situación resulta irresoluble mientras no se cambie el valor del parámetro 'PSV' contenido en la estructura **TInGW**).

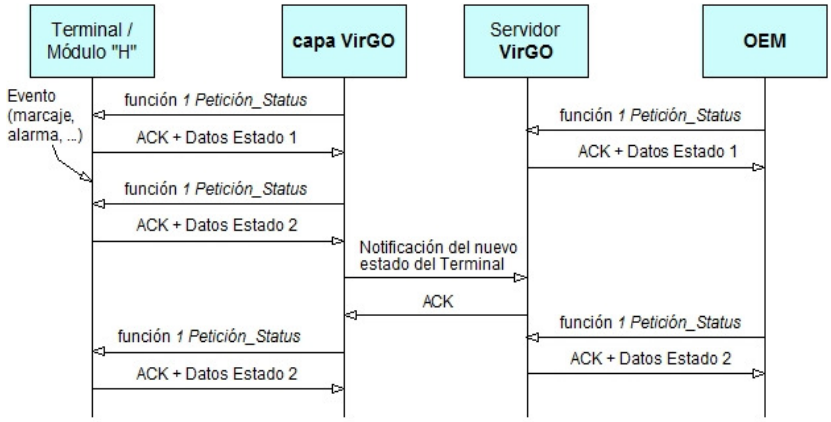
Cuando el programa **OEM** ejecuta la función *0 Ini_PORT* del **driver** Q2_DRV32.DLL (API de nivel bajo), éste intenta conectarse al Servicio **VirGO**, por lo que le envía el 'PSV' de la **capa VirGO** con la que se quiere conectar. Si el Servicio **VirGO** no tiene conectada la **capa VirGO** con el 'PSV' indicado retorna un NACK con CE=33, mientras que si el Servicio **VirGO** tuviera conectada la **capa VirGO** el **driver** enviará la trama de *Inicio de Sesión / Enrolamiento* con los parámetros 'VT', 'TO' y 'NR' (más 'OP' y 'PW' si es enrolamiento) y el Servicio **VirGO** los enviará a la **capa VirGO**, la cual retornará un ACK (y la pertinente Clave de Sesión 'CS' si es enrolamiento) al Servicio **VirGO** y éste lo retornará al **driver** Q2_DRV32.DLL.



11.3 Interrogando a los Terminales

Cada **capa VirGO** interroga sistemáticamente a los Terminales que de ella dependen (son los conectados a su Bus RS-485 o a su Bus **WPAN** en el caso de ser un **Adaptador de protocolos** o son los hasta cuatro Módulos "H" de un subsistema HYDRA o es el propio Terminal *Compacto* o Terminal *Modular* de la Serie 700 o de la Serie 3000) y que consten en la lista interna generada por detección bajo demanda).

Cuando la **capa VirGO** detecte que el estado del Terminal o del Módulo "H" ha cambiado, enviará una trama al Servicio **VirGO** informando del nuevo estado del Terminal.

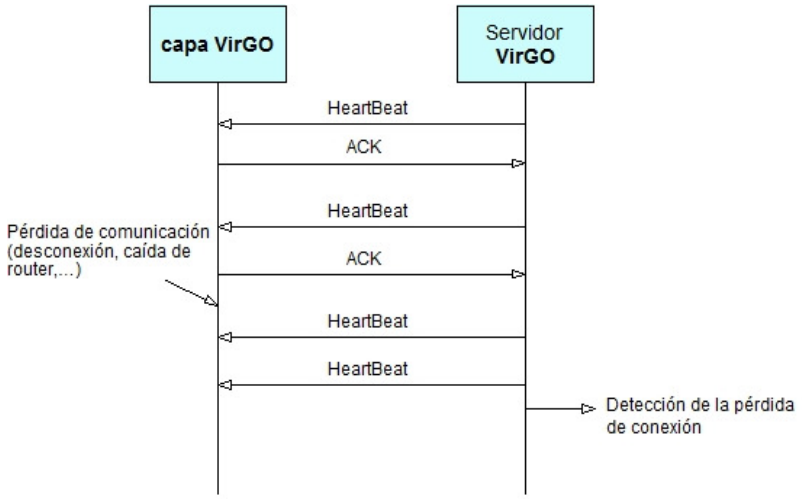


Tal y como puede verse en el esquema anterior, el programa **OEM** no tiene que preocuparse de interrogar a los Terminales para conocer si ha cambiado el 'Puntero_Lista_Marcajes' sino que se limita a ejecutar la función *1 Petición_Status* para obtener la mínima información necesaria para, en consecuencia de tal información, activar los procedimientos adecuados (recoger marcajes, atender Alertas, etc.). Esto resulta posible dado que cuando el Servicio **VirGO** contesta a la función *1 Petición_Status* (enviada al Terminal por el programa **OEM** pero interceptada por el Servicio **VirGO**) responde de inmediato con la última información enviada por la correspondiente **capa VirGO** (la cual ha sido recogida por ésta del Terminal[1] interrogado por el programa **OEM**), de manera que la comunicación entre el programa **OEM** y los Terminales resulta lo más rápida posible dado que, realmente, no hay tráfico sistemático por la red motivado por las interrogaciones del programa **OEM**.

11.4 Detección de pérdida de conexión TCP/IP

La detección de pérdida de conexión TCP/IP se realiza mediante una trama de *Heart Beat* que el Servicio **VirGO** envia a la **capa VirGO** con la latencia definida en el parámetro 'HB'(2) contenido en la estructura **TInGW**, respondiendo la **capa VirGO** a esta trama sólo con un ACK, mientras que en el caso de que la **capa VirGO** no responda en el tiempo indicado en el parámetro 'EGW'(2) contenido en la estructura **TInGW**, el Servicio **VirGO** envía de nuevo la trama.

En caso de que la **capa VirGO** agote los reintentos indicados en el campo HB contenido en la estructura **TInGW**, se consideraría perdida la conexión con la **capa VirGO** .



NOTAS:

(1)

Para que el "segundo paradigma" pueda ser utilizado en su plenitud, el FW de los Terminales tiene que ser de la Versión 08.00.00 (o superior).

(2)

El valor de ciertos parámetros contenidos en la estructura **TInGW** puede ser modificado por medio de la función *33 Reconfigurar_VirGO* de la API de nivel bajo.

ESTA PÁGINA HA SIDO DEJADA EN BLANCO INTENCIONADAMENTE

código	título	relaciones
QAN-12	El **sistema CONACC** y Windows 7	- MRT019 : capítulo 5 (función *0*) - BTP015 (Revisión R y >>) - Q2_DRV32 : Versión 8.0 y >>

Los programas de aplicación y los programas de utilidad desarrollados por Qontinuum pueden, bajo ciertas circunstancias, no ser operativos al ser instalados en PC basados en plataformas Windows 7.

12.1 Antecedentes

Hasta la aparición de la Versión 8.0 del **driver** Q2_DRV32.DLL, toda la información referente al uso de los Puertos de comunicación se guardaba en el Registry de Windows, en una subcarpeta de la rama *HKEY_LOCAL_MACHINE*.

El Sistema Operativo Windows 7 ha modificado el sistema de lectura y escritura de este tipo de carpetas, de manera que, cuando una aplicación quiere escribir en una subcarpeta de *HKEY_LOCAL_MACHINE*, Windows 7 realmente escribe en una carpeta privada del usuario (formalmente, trata a tal carpeta de una manera virtual). Esta sistemática no produce ningún problema mientras sólo un usuario utilice los programas, pero cuando dos o más usuarios deben usar información sobre los Puertos de comunicación aparece el problema dado que el concepto de repositorio general en el Registry ha dejado de ser directamente viable.

Para cubrir documentalmente las diversas circunstancias en las que tales problemas de compatibilidad pueden existir, aparece la Restricción R67 publicada en la Base de Conocimientos de Qontinuum:

http://www.qontinuum-plus.es/esp/KBase/_restricciones_.php#R67

12.2 Nuevo planteamiento

Debido a los antecedentes expuestos hemos cambiado la ubicación de los datos correspondientes a los Puertos de comunicación para separarlos del Registry, para lo cual hemos creado una base de datos de Puertos para uso exclusivo del **driver** (y, en consecuencia, de las APIs). Además, con la aparición de tal base de datos de Puertos, se obtienen las siguientes ventajas:

1ª) Se simplifica la instalación de las aplicaciones al evitar que deba intervenir un Administrador del PC durante la instalación de productos Software de Qontinuum; hasta ahora se necesitaban permisos de escritura en carpetas como *system32* y en una subcarpeta de *HKEY_LOCAL_MACHINE* dentro del Registry, lo cual podía obligar a un Administrador a dar permisos manualmente sobre tales carpetas para que los usuarios pudieran utilizar las aplicaciones.

2ª) Se evitan posibles alertas por parte de programas de protección: algunos antivirus, “anti spyware” y otros sistemas de protección que aíslan al Registry de Windows, de manera especial la rama *HKEY_LOCAL_MACHINE*., lo cual podía provocar falsas alertas o funcionamiento erróneo hasta que no se declarara una excepción expresa en el programa de protección.

3ª) Permite copiar la configuración existente de un equipo a otro de manera fácil: hasta ahora cuando se realizaba un cambio de PC se necesitaba volver a configurar todos los Puertos de comunicación; ahora se puede mover la base de datos de Puertos y, por tanto, ya no es necesario volver a configurar los Puertos de comunicación.

A partir de la Versión 8.0, el **driver** Q2_DRV32.DLL incorpora, en la función *0 Ini_PORT*, nuevos Tipos de Acción (TA = 6 para abrir el Puerto de comunicación sin grabar la información, TA = 7 para añadir un registro para el Puerto de comunicación en la base de datos de Puertos y TA = 8 para eliminar el registro del Puerto de comunicación en la base de datos de Puertos), de manera que el programa **OEM** no deberá preocuparse de donde se guarde la información, ya que las APIs se encargarán de guardar los registros de información donde corresponda, razón por la cual se recomienda el uso de este sistema para garantizar la integridad de los datos y para que, si en el futuro es necesario realizar otro cambio de ubicación de los datos para los Puertos de comunicación, el programa **OEM** no necesite modificaciones, ya que las APIs se encargarán de toda la gestión de los datos referidos a los Puertos de comunicación.

12.4 Cómo quedan afectados los programas de aplicación

Dado que actualmente los programas de aplicación pueden gestionar los Puertos de comunicación de tres maneras, en los siguientes subcapítulos se comenta, brevemente, las maneras actuales de hacerlo y se aclara la posible afectación que el nuevo planteamiento tiene en lo que concierne a tales programas.

12.4.1 Abrir los Puertos pasando todos los parámetros

En esta manera la lógica del programa de aplicación no tiene porqué ser alterada dado que no se guardaba ninguna información sobre los Puertos de comunicación en el Registry ni ahora se guardará en la base de datos de Puertos.
- No es necesario modificar el programa de aplicación.

12.4.2 Configurar los Puertos desde Q2_UTIL y abrirlos sin pasar parámetros

En esta manera el programa de utilidad Q2_UTIL.exe (en las Versiones anteriores a la 6.0) guardaba directamente la información en el Registry y, cuando el programa de aplicación solicitaba abrir el Puerto, el **driver** Q2_DRV32.dll (en las Versiones anteriores a la 8.0) obtenía tal información del Registry.
A partir de la Versión 8.0 y posteriores del **driver** Q2_DRV32.dll, es éste (y no la Versión 6.0. y posteriores de Q2_UTIL.exe) quién graba los parámetros de los Puertos de comunicación en la base de datos de Puertos, pero nada de ello impide que el programa de aplicación pueda seguir solicitando la apertura de los Puertos de comunicación sin pasar parámetros.
- No es necesario modificar el programa de aplicación, dado que el SP (Service Pack) de actualización de Q2_DRV32 a cualquier Versión 8.0 o superior genera automáticamente la base de datos de Puertos y elimina la parte correspondiente del Registry.

12.4.3 Configurar los Puertos en el Registry y abrirlos sin pasar parámetros

En esta manera el programa de aplicación utiliza directamente los recursos Windows para afectar al Registry, de manera que la parametrización de los Puertos de comunicación queda fuera del control del **driver** Q2_DRV32.dll (en las Versiones anteriores a la 8.0), lo cual produce que, al instalar la Versión 8.0 (o superior), el sistema deje de funcionar dado que tal **driver** no busca la información de los Puertos de comunicación en el Registry sino en su propia base de datos de Puertos.

- Es necesario modificar el programa de aplicación para configurar los Puertos de comunicación a través de los nuevos Tipos de Acción (TA) 7 y 8 de la función *0 Ini_PORT* (para una explicación más extensa hay que ver la Revisión R y posteriores del documento BTP015).

ESTA PÁGINA HA SIDO DEJADA EN BLANCO INTENCIONADAMENTE

código	título	relaciones
QAN-13	Usos específicos, usos especiales y señalización con HYDRA	- MRT019 : capítulo 3 (*Dirección 42*) - MRT019 : capítulo 5 (funciones *28, 32 y 129*) - BTP027 (Revisión U y >>) - BTP038 (Revisión E1 y >>) - MIP-HYDRA (Revisión E1 y >>)

Bajo un punto de vista histórico, todos los Terminales fabricados por Qontinuum consisten en una electrónica de control más el correspondiente Cabezal lector o lector-grabador, pudiendo ser dos los Cabezales lectores en los Terminales llamados bicéfalos (modelos XX-507 y XX-907) y pudiendo ser dos Terminales más dos Cabezales lectores o lectores-grabadores en los Terminales dobles (modelos XX-902).

En todos esos casos, los programas **OEM** deben considerar a cada Terminal como un todo, excepto a los Terminales dobles a los que deben considerar como dos todos por completo independientes (físicamente están situados en un mismo contenedor, pero a efectos lógicos se tratan como dos Terminales sin relación alguna entre ellos).

Con la aparición de HYDRA, algunas consideraciones deben ser hechas dado que, aunque cada conjunto formado por un Módulo “H” y el correspondiente Cabezal lector o lector-grabador forma un Terminal y aunque, por lo anteriormente expuesto, cada Terminal debe ser considerado como un todo, existen algunas aplicaciones en las que se produce la cooperación entre dos o más de los Módulos “H” instalados en un mismo subsistema HYDRA. Esta Nota de Aplicación tiene por objetivo ayudar a que los programas **OEM** puedan implementar tales aplicaciones, por lo que este documento debe ser interpretado conjuntamente con el documento BTP038 dado que allí se definen y explican conceptos que aquí se dan por entendidos.

Las prestaciones exclusivas de los subsistema HYDRA se declaran en el código “Control UEES” (Usos Específicos, Especiales y Señalización) del parámetro ‘IM’ de la función *28 Instalar_Terminal* o de la macrofunción *129 Instalar_fS=4*.

El código “Control UEES” puede tomar los valores 0 (ninguna opción seleccionada) o del 1 al 4 y del 8 al 12 (excepto el 11) para seleccionar una de las diferentes opciones posibles descritas a continuación. Cuando la prestación deseada implique a dos Terminales, ambos deberán pertenecer al mismo subsistema HYDRA y ser instalados con la misma opción.

13.1 Utilización con Semáforo virtual

La utilización específica del **Semáforo virtual** debe ser activada indicando el valor 1 en el código "Control UEES" de los dos Terminales involucrados (dos Módulos "H" modelo XX-101 del mismo subsistema HYDRA), así como también debe cargarse en cada Terminal el parámetro 'LATENCIA ENTRADAS' para E1.

Al usar esta prestación, cuando se está realizando un acceso por uno de los dos Terminales, por ejemplo el de ID=3 de la pareja vinculada, se bloquea el intento de uso en el Terminal con ID=4, por lo que el LED rojo del Cabezal lector o lector-grabador del Terminal con ID=4 permanecerá encendido para indicarlo y, a cada intento de acceso, el FW generará un **marcaje normal** con CE=28. En tales circunstancias, también se inhibe en el Terminal con ID=4 la "alarma puerta inmediata" (corresponde a la situación de "puerta forzada") relacionada con el punto de paso abierto, perdurando tal inhibición para este Terminal hasta que se cierre el punto de paso, mientras que en el Terminal con ID=3 el FW controla si se agota el tiempo indicado en su parámetro 'LATENCIA ENTRADAS' para E1 para, de agotarse, activar la "alarma puerta" (corresponde a la situación de "puerta mantenida").

Para dos Terminales (dos Módulos "H" modelo XX-101) de un mismo subsistema HYDRA no es posible definir el uso concurrente de **Semáforo virtual** y de **Semáforo físico**, de manera que, si se intentara hacerlo, el FW del subsistema HYDRA retornaría el código de estado *19 Parámetros erróneos* a la función *28 Instalar_Terminal* o a la macrofunción *129 Instalar_fS=4*.

13.2 Utilización en esclusa

La utilización específica de **esclusa** de tipo 2 (el subsistema HYDRA no admite otro tipo) debe ser activada indicando el valor 2 en el código "Control UEES" de los dos Terminales involucrados (dos Módulos "H" modelo XX-101 del mismo subsistema HYDRA).

Esta prestación implica el control por **Semáforo virtual** añadiendo, a la característica de doble punto de acceso, la más específica de recinto cerrado.

Esta prestación se aplica a los dos Terminales que deban controlar los dos pasos de una **esclusa**. A cada Terminal se le conectará los elementos (Cabezal lector o lector-grabador, "pulsador auxiliar" para el sentido 'Salida', cerradura y sensor de puerta) adecuados para el punto de paso, por lo que los parámetros programados en cada Terminal corresponden a los elementos conectados sólo a él.

Dado que la función básica de una **esclusa** es la de no permitir el acceso por un punto de paso mientras esté abierto el otro, si tal circunstancia se diera, el FW rechaza el intento de acceso y genera un **marcaje normal** (si el intento se realiza por medio de un Cabezal) o un **marcaje especial** (si el intento se realiza por medio del "pulsador auxiliar" para el sentido 'Salida'), en ambos casos con CE=28.

13.3 Utilización en esclusa con control biométrico "de peso"

La utilización específica de **esclusa** de tipo 2 con control biométrico "de peso" debe ser activada indicando el valor 3 en el código "Control UEES" de los dos Terminales involucrados (dos Módulos "H" modelo XX-101 del mismo subsistema HYDRA).

Esta prestación implica el control por **Semáforo virtual** añadiendo a la característica de doble punto de acceso la más específica de recinto cerrado pero con control biométrico "de peso" para constatar la presencia de únicamente el usuario involucrado, por lo cual el subsistema HYDRA debe incorporar también un Módulo "H" modelo GEN-103 para la conexión de la báscula situada dentro de la **esclusa**.

Esta prestación implica las siguientes especificidades:

- la **esclusa** tiene que haber sido debidamente calibrada(1);
- en el interior de la **esclusa** no son necesarios "pulsadores auxiliares" para el sentido 'Salida';
- sólo es aplicable trabajando con Módulos "H" de Familias que traten estructuras **fS=4**;
- permite un control de "aforo" por parte de uno de los dos Terminales involucrados (lógicamente debe ser el que controle al Cabezal situado en el área al que la **esclusa** facilite el acceso).

A continuación aparece un resumen de la secuencia lógica del FW (en el subcapítulo 13.3.1 aparece la secuencia como diagrama de flujo):

1) Una vez que el usuario haya presentado su **Acreditación** y que el FW haya activado la opción **Semáforo virtual** (en el supuesto de que éste estuviera libre en ese momento), la operativa es la habitual en un acceso, de manera que, una vez finalizadas todas las validaciones de manera positiva, se genera un **marcaje normal** con CE=34 y se activa la Salida R1 (del Módulo "H" correspondiente) para abrir la puerta de entrada a la **esclusa**:

- si transcurre el tiempo indicado en el parámetro 'TIEMPOS SALIDA 1 Y SALIDA 2' sin que se haya abierto tal puerta, el FW aborta el proceso(2) con un **marcaje normal** con CE=118;
- una vez abierta tal puerta, si transcurre el tiempo indicado en el parámetro 'LATENCIA ENTRADAS' para la Entrada E1 sin que se haya cerrado, el FW aborta el proceso(2) con un **marcaje normal** con CE=118 seguido de un **marcaje especial** con CE=44 (el cual puede ser seguido de otro **marcaje especial** con CE=97), mientras que si la puerta ha sido cerrada se supone que el usuario a entrado en la **esclusa**.

2) Al ser cerrada la puerta de entrada a la **esclusa**, el Terminal empieza a evaluar la información recibida de la báscula hasta obtener un peso estable o hasta que se agota el tiempo indicado en el subparámetro **latencia Usuario**. Si el peso registrado por la báscula es = 0, indica que el usuario no ha entrado en la **esclusa** (no se ha situado sobre el detector de peso dado que éste debe ocupar toda la superficie de la **esclusa**), por lo que el FW aborta el proceso(2) con un **marcaje normal** con CE=118, mientras que si hay detección de peso el FW lo compara con el indicado en el archivo $XX_{DATBIO5}$ existente en la estructura **fS=4** de la **Acreditación** del usuario (tal archivo fue leído en el paso 1).

3) Peso inestable o incorrecto : si el peso es inestable o es estable pero no corresponde, se aborta el proceso(2) con un **marcaje normal** con CE=120 y el FW abre de nuevo la puerta por la que entró el usuario para que éste pueda salir (realmente deberá salir(2) y reiniciar todo el proceso).

4) Peso correcto : el FW activa la Salida R1 (del Módulo “H” correspondiente) para abrir la puerta de salida de la **esclusa**; si tal puerta no se abre físicamente, el FW genera un **marcaje especial** con CE=121 y activa el zumbador del Módulo “H” modelo GEN-103 y el del Terminal de salida de la **esclusa** para alertar al usuario para que abra la puerta, mientras que si la puerta ha sido abierta se supone que el usuario a salido de la **esclusa, en cuyo momento el FW comprueba que se haya cerrado la puerta (mientras tal cosa no ocurra** genera un único **marcaje normal** con CE=44 y activa el zumbador del Módulo “H” modelo GEN-103 y el del Terminal de salida de la **esclusa** hasta que la puerta es cerrada.

5) Si en estado de reposo (con la puerta cerrada) se detecta un peso superior a la ‘Desviación máxima’(3), el FW genera un **marcaje especial** con CE=121 y activa el zumbador del Módulo “H” modelo GEN-103 para alertar de una situación completamente anómala (o el usuario no ha salido o existe algo o alguien dentro de la **esclusa**), por lo que el FW activa de nuevo la apertura de la puerta de salida de la **esclusa**. Si el peso detectado es superior a la ‘Desviación de base’(3) pero sin alcanzar a la ‘Desviación máxima’(3), el FW, aunque a todos los efectos lo considera como peso = 0, genera un **marcaje especial** con CE=120 (sólo uno por cada día) para indicar que quizá haya que recalibrar la báscula; si esta situación se repite frecuentemente, entonces habría que replantear la configuración de los parámetros lógicos asignados a la báscula.

6) La utilización en **esclusa** con control biométrico “de peso” y control de “aforo” permite, de manera automática, el “armado” o “desarmado” de un **Panel de Alarmas externo** según el contador de “aforo” este o no a 0. El control “de aforo” lo llevará a cabo el Terminal configurado para tal empeño (para lo cual hay que activar el bit b21 del parámetro ‘IM’ mediante la función *28 Instalar_Terminal* o la macrofunción *129 Instalar_fS=4*), de manera que el FW de tal Terminal incrementará el contador a cada acceso completado que se inicie en su cabezal y lo decrementará a cada acceso completado en sentido contrario.

Resumiendo, el subsistema HYDRA sólo considerará acabado el proceso, en cuyo momento desactivará el **Semáforo virtual** y se dará por terminado el acceso, cuando las dos puertas de la **esclusa** estén cerradas y el sensor de peso no indique la existencia de alguien o de algo situado dentro de la **esclusa**.

NOTAS:

(1)

El calibrado es necesario para definir las características operativas de la báscula en relación al subsistema HYDRA al que se conecta (realmente se conecta al Módulo “H” modelo GEN-103, el cual almacena en su memoria los datos de calibración), de manera que si en un subsistema HYDRA hubiera que cambiar, por avería, o bien la báscula o bien el Módulo “H” (o ambos), habría que calibrar de nuevo el conjunto resultante. El proceso de calibración puede efectuarse tanto desde la API de nivel bajo (**driver** Q2_DRV32.DLL) como desde el programa de utilidad Q2_UTIL (Versión 06.01.00 y superiores).

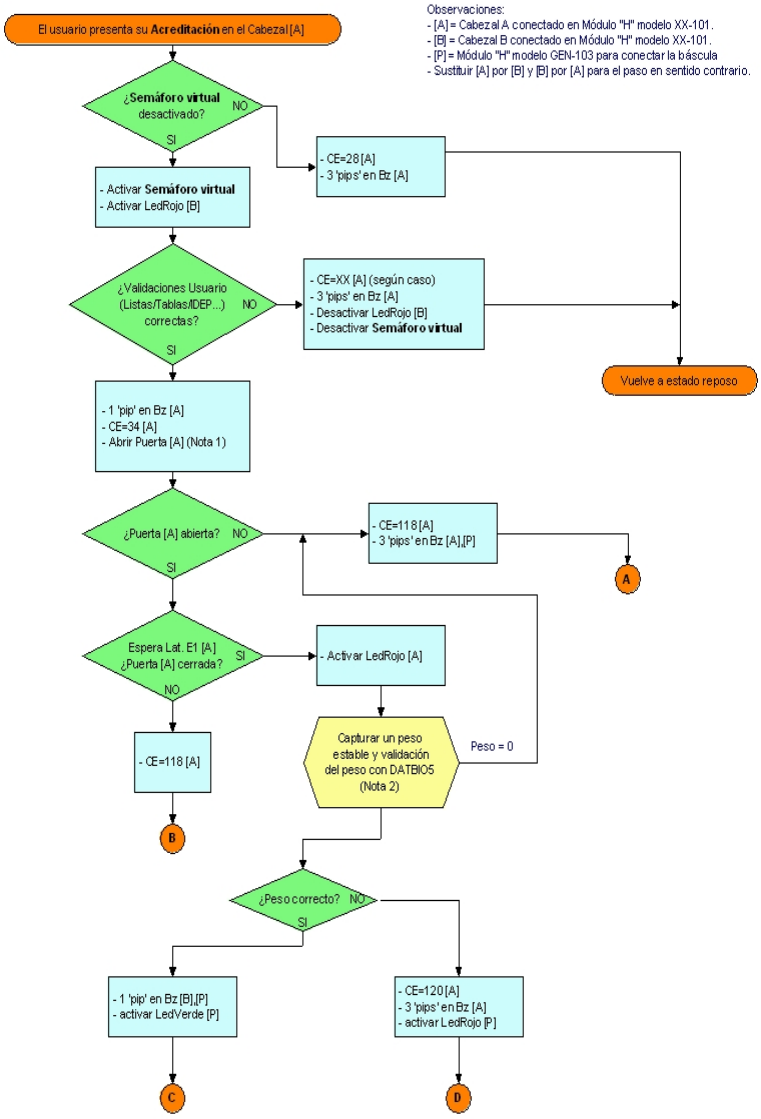
(2)

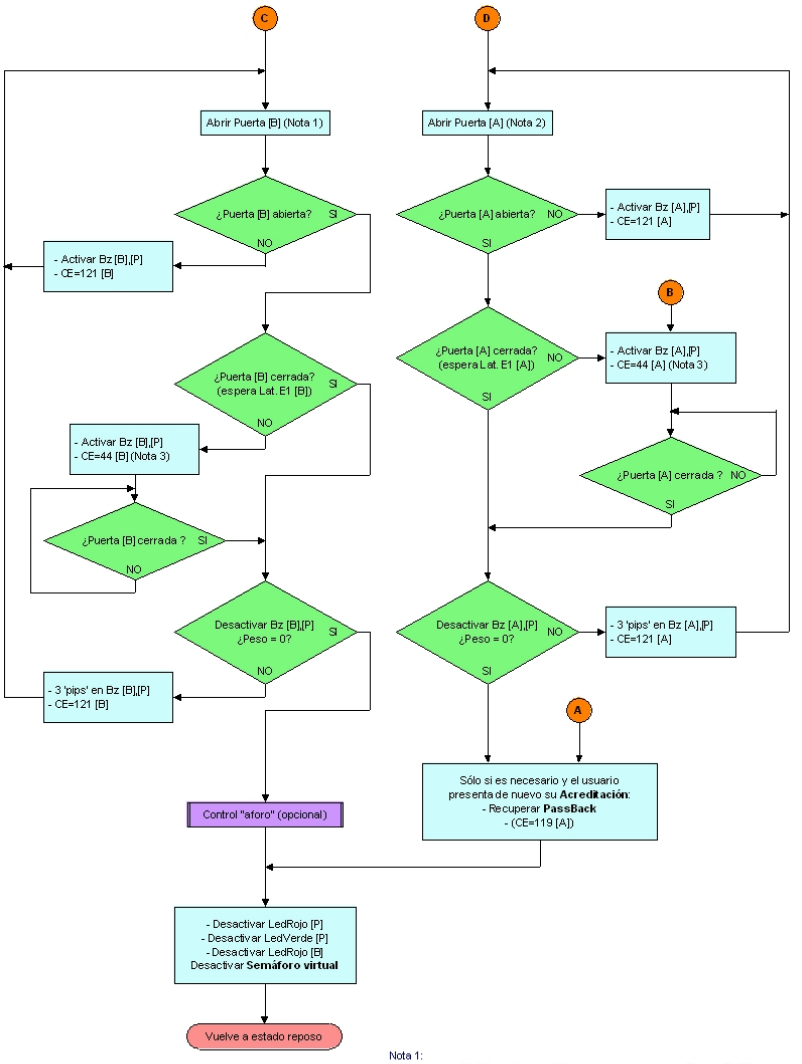
Dado que la Instalación utiliza **Acreditaciones** dotadas con estructura **fS=4**, los usuarios deberán ser advertidos de la conveniencia de que, ante la situación de proceso abortado, presenten de nuevo su **Acreditación** al Cabezal lector-grabador que hubieran acabado de utilizar para que el FW del Terminal correspondiente les restaure el control anti **Pass-Back** (si tal control se utiliza en ese Terminal).

(3)

Este parámetro está explicado en el capítulo 5 de la Revisión E1 (y posteriores) del documento BTP038.

13.3.1 Diagrama de flujo





Nota 1:
Implica activar R1 [B] y LedVerde [B] hasta que transcurra el Tiempo R1 [B] o hasta que la Puerta [B] sea abierta.

Nota 2:
Implica activar R1 [A] y LedVerde [A] hasta que transcurra el Tiempo R1 [A] o hasta que la Puerta [A] sea abierta.

Nota 3:
Al cerrar la puerta, y si el bit b6 del parámetro **máscara Miscelánea** está activado, al **marcaje especial** con CE = 44 se le añadirá otro con CE = 97.

13.4 Utilización en doble intervención simultánea

La utilización especial de la **doble intervención simultánea** debe ser activada mediante el valor 8 en el código “Control UEES” y cargando de contenido el parámetro ‘GRUPO DOBLE INTERVENCIÓN SIMULTÁNEA’ del único Terminal involucrado, el cual estará formado por un Módulo “H” modelo XX-101, con su Cabezal correspondiente, más un Módulo “H” modelo XX-101/DIS para conectar un Cabezal adicional, formando parte ambos Módulos “H” del mismo subsistema HYDRA.

Esta prestación requiere que sean dos los usuarios autorizados y que realicen la presentación de sus respectivas **Acreditaciones** de manera concurrente en el tiempo, por lo que un usuario presentará su **Acreditación** en un Cabezal y el otro usuario presentará la suya en el otro Cabezal con una forzada simultaneidad (el decalaje temporal no puede superar el tiempo indicado en el subparámetro **latencia Usuario**(1)).

Los Cabezales se colocarán físicamente a una distancia suficiente entre ellos para que una sola persona no pueda alcanzar a ambos simultáneamente (por ejemplo, extendiendo los brazos) ni antes de que acabe el tiempo indicado en **latencia Usuario**(1). Una explicación completa de esta prestación puede verse en el subcapítulo 2.4.2 de la Revisión U y posteriores del documento BTP027.

NOTAS:
(1)
Excepcionalmente para este caso, el FW tomará el tiempo indicado en el subparámetro **latencia Usuario** en décimas de segundo.

13.5 Utilización para el control de una Partición en un Panel de Alarmas externo

La utilización específica del control de una Partición en un **Panel de Alarmas externo** debe ser activada indicando el valor 4 en el código "Control UEES" (parámetro 'IM' de la función *28 Instalar_Terminal* o de la macrofunción *129 Instalar_fS=4*) y cargando de contenido el parámetro 'INTERACCIÓN PANEL' de los dos Terminales involucrados. De tales Terminales, el primero (el que tenga el ID inferior) es el que se conectará físicamente con el **Panel de Alarmas externo**, por lo que se le deberá activar el bit b21 (parámetro 'IM' de la función *28 Instalar_Terminal* o de la macrofunción *129 Instalar_fS=4*) y definir el parámetro 'INTERACCIÓN PANEL' al completo, mientras que en el segundo Terminal tal bit b21 deberá estar desactivado y sólo se usará el subparámetro 'Tiempo permanencia' del parámetro 'INTERACCIÓN PANEL'.

Cada uno de los Terminales implicados que tenga activado el bit b3 del parámetro 'MÁSCARA MISCELÁNEA 4' indicará (mediante el LED del Cabezal lector-grabador correspondiente) el estado actual de la 'zona común' del **Panel de Alarmas externo** (rojo = "armado", verde = "desarmado").

Cuando el subsistema HYDRA autorice a un usuario el acceso desde cualquiera de los dos puntos vinculados, "desarmará" la correspondiente Partición en el **Panel de Alarmas externo**, al igual que la "armará" (también desde cualquiera de los dos puntos de acceso) cuando el usuario realice la operativa adecuada. Mientras se realiza una operación en uno de los Terminales se bloqueará la operativa en el otro y viceversa, lo cual queda indicado por el LED rojo encendido.

Cuando el programa **OEM** quiera conocer o modificar en el **Panel de Alarmas externo** el estado de la Partición físicamente vinculada, podrá hacerlo dirigiéndose a cualquiera de los Terminales implicados. El Operador deberá tener en cuenta que la última operación que haga sobre cada Terminal será el estado en el que quede la Partición en el **Panel de Alarmas externo** (por ejemplo, si "arma" desde el ID = 3 y posteriormente "desarma" desde el ID = 4, la Partición en el **Panel de Alarmas externo** quedará "desarmada").

Los **marcajes normales** *55 "desarmado"* y *56 "armado"* generados por el FW debido a la presentación de una **Acreditación** por parte de los usuarios, se grabarán en el Terminal desde el cual se ha ordenado la acción de "desarmar" o de "armar".

Los **marcajes especiales** *55 "desarmado"* y *56 "armado"* generados por el FW debido a las ordenes enviadas por el programa **OEM** directamente a uno de los Terminales vinculados, se grabarán en ese Terminal.

El **marcaje especial** *56 "armado"* generado por el FW debido a las ordenes enviadas por el programa **OEM** directamente al **Panel de Alarmas externo** y comunicado por éste al subsistema HYDRA, se grabará en el primer Terminal (el que tenga el ID inferior) dado que es el que tiene las conexiones físicas con la pertinente Partición en el **Panel de Alarmas externo**.

13.6 Señalización

La arquitectura de los subsistema HYDRA obliga a los Módulos “H” a tomar el ID del conector en el que son colocados de manera física, por lo que los Terminales residentes en un mismo subsistema HYDRA sólo pueden tener los ID del 3 al 6.

Hecha la excepción de los casos descritos en los capítulos anteriores (y en el documento BTP038), la elección del conector físico en el que situar cada Módulo “H” es totalmente libre. Sin embargo, si se quisiera utilizar la posibilidad que ofrecen los subsistema HYDRA de dar a conocer si existe una apertura del contenedor resulta imprescindible la existencia de un Módulo “H” en el conector con el ID = 3 dado que es éste el encargado de generar la señalización global.

Para la señalización de la apertura y cierre del contenedor (lo cual podría significar un acto de **“tamper”**) se generan, respectivamente, los **marcajes especiales** *46 “vandalismo en el Terminal Modular”* y *94 Final “vandalismo en el Terminal Modular”*. Como consideración importante, hay que tener en cuenta que si se desea un aviso acústico de tal situación de alerta, éste sólo se podrá efectuar en el Cabezal conectado al Módulo "H" con el ID=3 (utilizando el correspondiente parámetro ‘MASCARA AVISOS SONOROS’).

La señalización para indicar tanto el inicio de la situación de alimentación desde la batería como el final de tal situación se generan, respectivamente, los **marcajes especiales** *13 “alimentación en precario”* y *12 Final “alimentación en precario”*. Esta señalización se puede obtener de cualquiera de los cuatro posibles Módulos "H", siempre que el escogido haya sido instalado mediante la función *28 Instalar_Terminal* o la macrofunción *129 Instalar_fS=4* con el bit 'b27' del parámetro ‘IM’ activado(1).

NOTAS:

(1)
Existe una Instalación de trato excepcional que plantea parecidas necesidades pero que son resueltas de manera distinta, para lo cual hay que solicitar a Qontinuum el documento correspondiente a tal Instalación.

ESTA PÁGINA HA SIDO DEJADA EN BLANCO INTENCIONADAMENTE

código	título	relaciones
QAN-14	Consideraciones sobre el **NIS**	- MRT019 : completo - BTP036 (Revisión C y >>): capítulo 3

Esta Nota de Aplicación tiene como objetivo clarificar el **NIS** tanto conceptualmente como en la manera de usarlo en los programas **OEM**.

NIS es un acrónimo con dos significados históricos y uno actual:
- en el primero correspondía a Número Identificador Soporte, y fue definido así desde el inicio de las especificaciones para el **sistema CONACC**;
- en el segundo corresponde a Número Identificador del Sujeto, y fue definido así cuando el uso de la biometría quedó incorporado a las especificaciones para el **sistema CONACC**.

Sin embargo, con la publicación de la Revisión X1 del **sistema CONACC** el significado del acrónimo **NIS** cambia a Número Identificador Serializado como única acepción.

Una característica básica del **sistema CONACC** es la de establecer una clara separación conceptual entre la numeración de los Usuarios y la numeración de las **Acreditaciones** que vayan a ser usadas por aquellos para identificarse frente al sistema. El sentido de tal separación radica en el hecho de que muchos tipos de tales **Acreditaciones** implementan tecnologías que no permiten que el **NIS** sea grabado a voluntad de la Instalación(1) sino que, al permitir sólo su lectura, presenta un número fijado en origen, normalmente conocido como **NUFAB**, que es único e irrepetible, de manera que la asignación de tal número a un Usuario establece una relación también única e irrepetible, por lo que si el Usuario pierde la **Acreditación** asignada los programas **OEM** deben preveer que la relación { ID del Usuario <--> **NIS** } deberá ser cambiada imprescindiblemente para hacerla coincidir con la nueva realidad (mismo Usuario pero distinta **Acreditación**).

Tal situación no presenta mayor problema que lo expuesto, pero la cosa cambia si en una misma Instalación han de coexistir **Acreditaciones** de diferentes tecnologías como sería, por ejemplo, el caso de querer utilizar tarjetas de banda magnética para las personas pero también identificadores RFID específicos para la 'identificación automática de vehículos en Tránsito' (iavT). En tales casos (y en otros de circunstancias similares), los programas **OEM** deben aportar soluciones eficaces y fácilmente comprensibles para los Operadores de los programas, por lo que la mejor solución es, sin duda alguna, que se puedan establecer múltiples relaciones { ID del Usuario <--> **NIS** }, siendo también responsabilidad de tales programas la inequívoca selección de los **NIS** a cargar en la **Lista_Blanca** de cada Terminal en función de cual sea la naturaleza de las **Acreditaciones** que deba tratar.

En aquellas Instalaciones que usen Terminales de la Familia BIO (exclusivamente o en combinación con Terminales de otras Familias), la solución más intuitiva para establecer la relación de cada 'Template' con su propietario pasa por asignar a tales 'Templates' el ID del Usuario (no hay que olvidar que estamos tratando con un dato personal), pero por coherencia se debiera hacer asignando un **NIS** a tales 'Templates' y formalizando la relación { ID del Usuario <--> **NIS** } de la manera estándar del **sistema CONACC**.

En aquellas Instalaciones de *Control de Accesos* que quieran combinar identificación mediante **Acreditaciones** con autenticación por biometría (por ejemplo, usando el Cabezal lector modelo SEP-F985), el **NIS** debe ser, lógicamente, único y corresponder al de la **Acreditación** (en este ejemplo sería de la Clase "F" de la Familia SEP). Tales **NIS** serán utilizados para la identificación de las **Acreditaciones** presentadas por los Usuarios, por lo que el programa **OEM** cargará los **NIS** en la memoria del Cabezal lector (mediante la función *17 Grabar_RAM*) formando la **Lista_Blanca**, mientras que la relación de cada **NIS** con los 'Templates' correspondientes para las autenticaciones deberán ser cargadas (mediante la función *75 BioPlex*) en la memoria propia del lector biométrico integrado en el Cabezal lector (el modelo SEP-F985, para seguir con el ejemplo). Hasta este punto no hay mayor problema, pero si que lo hay cuando un Usuario pierde su **Acreditación** y debe serle asignado otra que tendrá un **NIS** diferente del que tenía la **Acreditación** perdida. En consecuencia, el hecho de cambiar el **NIS** en la **Lista_Blanca** es condición necesaria pero no suficiente dado que en una búsqueda 1:1 el **NIS** contenido en la **Lista_Blanca** y el **NIS** contenido en la memoria del lector biométrico, necesariamente deben coincidir. Para restablecer tal igualdad, el programa **OEM** deberá hacer uso de la subfunción 'Actualizar' (parámetro TS = 6) de la función *75 BioPlex*.
Sin embargo, si en el ejemplo anteriormente expuesto se diera el caso de que también debiera existir algún Cabezal lector de la Familia BIO (como el modelo BIO-3140 dotado sólo con lector biométrico), el problema del **NIS** al que se vinculen los 'Templates' toma otra dimensión dado que entonces un mismo 'Template' deberá tener un **NIS** distinto en el Cabezal lector modelo SEP-F985 y en el Cabezal lector modelo BIO-3140. De no hacerlo así, en el caso de que un usuario pierda su **Acreditación** y deba serle entregado otra, el cambio de **NIS** vinculado con el 'Template' debería hacerse no sólo en el Cabezal lector modelo SEP-F985 sino también en el Cabezal lector modelo BIO-3140, con la dificultad que ello conlleva al ser posible que pudieran haber duplicados. Para facilitar que los 'Templates' (en realidad los elementos "biodato") queden referenciados en la Base de Datos por un código único, debería cambiarse el valor del **NIS** original al, por ejemplo, valor 0, de manera que la información contenida en los elementos "biodato" quede aislada de los **NIS** excepto cuando sea necesario cargarla en los Terminales, para lo cual existe (en la Versión 08.09.00 y posteriores del **driver**) la función de 'librería' *158 Gestión de "biodatos"*, la cual permite desvincular y vincular los **NIS** a los elementos "biodato" de manera que, partiendo de un repositorio común (la Base de Datos), se carguen los elementos "biodato" (con su **NIS** correspondiente) en cada tipo de Terminal.

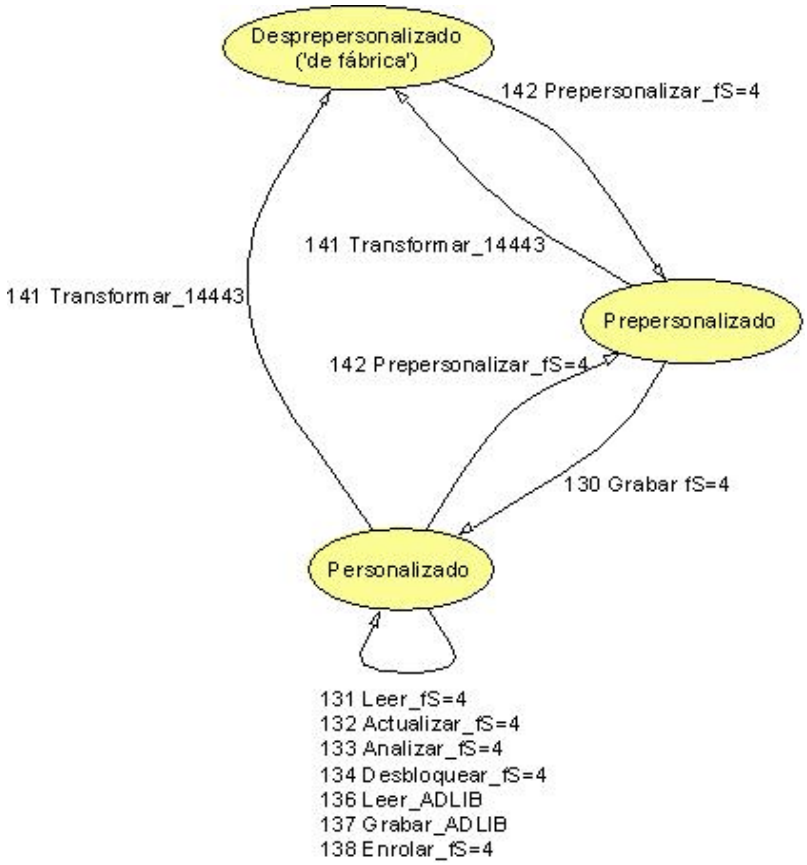
NOTAS:
(1)
Las diferentes tecnologías admitidas en el **sistema CONACC** y el uso que se hace de sus prestaciones aparecen explicadas en el capítulo 4.

código	título	relaciones
QAN-15	- Relación causal entre los códigos de estado retornados y las macrofunciones utilizadas - Las causas del Código de evento 54	- MRT019 : Anexo A, Anexo C y Anexo E

Esta Nota de Aplicación tiene como objetivo (subcapítulo 15.1) clarificar la relación existente entre los códigos de estado (ST) y las macrofunciones que los pueden producir, así como también tiene como objetivo (subcapítulo 15.2) detallar las causas del Código de Evento 54.

15.1

En el siguiente esquema se muestra la relación existente entre los códigos de estado (ST) que el **driver** retorna y las macrofunciones utilizadas por el programa **OEM** teniendo en cuenta la Familia del Terminal, de manera que se indican las posibles causas que generan tales códigos de estado:



ST	macrofunción	Familia	causas
8	130 / 131 / 133 / 136 / 137	LPC / DEF	no existe el Directorio de **fS=4**
80	132 / 134		
8	130 / 131 / 133 / 136 / 137	LPC / MIF / DEF	no coinciden las claves que afectan al archivo XX_{DATCOM}
80	132 / 134		
8	130 / 131 / 133 / 136 / 137	LPC / DEF	no existe el archivo XX_{DATCOM}
80	132 / 134		
8	130 / 131 / 133 / 136 / 137	MIF / DEF	error en la validación de la integridad del archivo XX_{DATCOM}
80	132 / 134		
0	130 (completa)	LPC / MIF / DEF	**NIS** = 0 en XX_{DATCOM}
76	130 (parcial) / 131 / 133 / 136 / 137		
80	132 / 134		
8	130 / 131 (desde el centro primario)	LPC / MIF / DEF	no coinciden las claves que afectan al archivo XX_{DATESP}
80	132 / 134		
00[1]	130	LPC / DEF	no existe el archivo XX_{DATESP}
80	132 / 134		

ST	macrofunción	Familia	causas
00(2)	130	MIF / DEF	error en la validación de la integridad del archivo XX_{DATESP}
80	132 / 134		
55	136	LPC / MIF / DEF	no coinciden las claves que afectan al archivo XX_{ADLIB}
8	137		
55	136	LPC / DEF	no existe el archivo XX_{ADLIB}
55	136	MIF / DEF	error en la validación de la integridad del archivo XX_{ADLIB}

NOTAS:
(1)
El archivo es creado automáticamente por el **driver**, por lo que el código de estado que retorna no establece la ausencia del archivo sino el final correcto de la macrofunción.

(2)
La integridad es restaurada automáticamente por el **driver**, por lo que el código de estado que retorna no establece el error sino el final correcto de la macrofunción.

15.2

El FW del Terminal genera un **marcaje excepcional** con CE=54 cuando detecta incongruencias y/o falta de información en la parametrización inherente a las especificaciones del **sistema CONACC**, y que son fruto de errores de planteamiento del programa **OEM** y/o de un mal uso por parte del Operador del programa de los recursos que éste proporcione.

En los Terminales de las Series 500 / 800 / 900 / 2000 / 3000, el **marcaje excepcional** se produce cuando el FW ...

... necesita usar la Tabla_Grupos y/o la Tabla_Horarios y no están declarados los respectivos punteros.;

... pretende la anotación de **NIS** por teclado habiendo sido el Terminal preconfigurado para operar en formato **fS=4**;

... pretende grabar un registro en la Lista_Marcajes o en la Lista_Marcajes_CDP pero existe incoherencia en los valores indicados por los correspondientes punteros;

... detecta un **tipo autenticación** que requiere pedir **IDEP** pero el Terminal no ha sido preconfigurado para operar en **fS=4** ni con biometría ni tiene configurada **Lista_Blanca** con **PIN**;

... debe utilizar la Tabla_Incidencias con la prestación “SxT”, pero existen incoherencias en la definición de los diversos parámetros (ver el Anexo D);

... debe utilizar una Incidencia_CDP pero el valor contenido está fuera de los límites impuestos, tanto para la Lista_Operaciones_CDP como para la Tabla_Incidencias_CDP;

... realiza una búsqueda en una Lista o Tabla y detecta un puntero con un valor erróneo;

... encuentra declarado el control **IDEP** con datos inválidos o incongruentes;

... el FW no encuentra el **registro EOF** obligatorio en:

- Tabla_Grupos
- Tabla_Horarios
- -- Tabla_Agenda
- Tabla_Excepciones
- Lista_Operaciones_CDP
- Lista_Especial
- Tabla_Incidencias_CDP
- Tabla_Excepción_Biometría
- Lista_Actualización
- Tabla_Mensajes

En los Terminales de las Series 2000 / 3000, el **marcaje excepcional** se produce también cuando el FW ...

... no encuentra el **registro EOF** obligatorio en:

- Lista_Otras_Prestaciones.

código	título	relaciones
QAN-16	Interacción del **sistema CONACC** con un **Panel de Alarmas externo**	- MRT019 : completo - BTP038 (Revisión E2 y >>) - BTP041 (Revisión C y >>) - BTP043 (Revisión C1 y >>)

Esta Nota de Aplicación tiene como objetivo clarificar las peculiaridades de los Terminales de Qontinuum para interaccionar con una Partición de un **Panel de Alarmas externo**, así como facilitar información a los programadores **OEM** para ayudarles a integrar tales Terminales en sus aplicaciones.

Esta prestación sólo es aplicable a los Terminales de las Familias MIF y DEF con un FW de Versión igual o superior a las que se mencione.

Dada la igualdad de diseño de la electrónica y la similitud operativa entre un subsistema HYDRA-II, un Terminal *Modular* modelo DEF-3002 y un Terminal *Modular* modelo DEF-3001 (todos ellos corresponden a la Serie 3000), toda referencia en esta Nota de Aplicación a los subsistema HYDRA-II hay que entenderla aplicable también a los modelos DEF-3002 y a los modelos DEF-3001.

16.1 Versión de FW 08.00.00 y >>

(para Terminales *Modulares* de la Serie 500 y de la Serie 900)

(primera Versión oficial de FW con la nueva prestación para "desarmar" / "armar" una Partición de un **Panel de Alarma externo** desde Terminales de C.A. de la Familia MIF)

Si en el momento de instalar el Terminal mediante la función *28 Instalar_Terminal* o la macrofunción *129 Instalar_fS=4* se activa el bit 'b21' del parámetro 'IM', el FW podrá "desarmar" / "armar" mediante una Salida (indicada en 'Sad') parametrizable (R2, S3 o S4) conectada a una 'Zona llave' del Panel (la cual deberá estar adecuadamente programada).

El FW del Terminal, para "desarmar", activa la Salida (indicada en 'Sad') y genera un **marcaje normal** con CE=55, mientras que, para "armar", desactiva tal Salida y genera un **marcaje normal** con CE=56.

Para indicar al FW que ejecute una de estas dos acciones hay tres posibilidades:

1) Mediante la presentación de una **Acreditación**:
   - si se realiza un acceso autorizado, el FW "desarma" automáticamente al retirar la **Acreditación** al mismo tiempo que permite el acceso.
   - si se presenta una **Acreditación** y (antes de retirarla) se espera un tiempo igual o superior al indicado en 'Tp', entonces el FW "arma" en vez de dar paso, aunque la **Acreditación** debe superar todas las validaciones como si de un intento de acceso se tratara.
2) Mediante un mecanismo de seguridad para un "rearmado" automático controlado por la superación del tiempo indicado en 'Taa' desde el último "desarmado" (excepto en 'Modo : Supervisado') o mediante una señal exterior aplicada a una Entrada (indicada en 'Taa').

3) Vía comunicaciones:

- mediante las funciones *16 Leer_RAM* y *17 Grabar_RAM* se puede consultar/modificar este nuevo estado ubicado en el Nibble alto del parámetro 'SITUACIÓN TERMINAL':
  Nibble bajo : 'Situación' Terminal (0,1,2 : como hasta ahora);
  Nibble alto : 'SubSituación' (0="armado", 1="desarmado").

Para que no se produzcan problemas de sincronización entre los diferentes elementos, hace falta que el programa **OEM** haga uso de estos recursos en los siguientes casos:

- cada vez que la aplicación quiera alterar este estado en el **Panel de Alarmas externo**;
- cuando la aplicación detecte un cambio de este estado en el **Panel de Alarmas externo** (producido, por ejemplo, por una operativa de teclado e informado por el Software que se utilice para comunicar con el Panel).

A cada cambio de estado el FW genera un **marcaje normal** (posibilidad 1) o un **marcaje especial** (posibilidad 2 y 3):

CE=55 : "desarmado"
CE=56 : "armado"

Para poder definir los valores 'Tp', 'Sad' y 'Taa' existe el parámetro 'INTERACCIÓN_PANEL' en el mapa de memoria del Terminal:

b8-b7	b6-b5	b4-b1
'Tp'	'Sad'	'Taa'

'Taa' : Tiempo "armado" automático :

- 0 = no control
- 1..12 = controlado por el FW al cabo de nx10 minutos (10 a 120 minutos)
- 13 = controlado externamente a través de la Entrada E2(1)
- 14 = controlado externamente a través de la Entrada E5(1)
- 15 = controlado externamente a través de la Entrada E6(1)

'Sad' : Salida para "armado" / "desarmado" :

- 0 = R2
- 1 = S3
- 2 = S4
- 3 = (reservado)

'Tp' : Tiempo permanencia :

- 0 = sin posibilidad de "armar" presentando una **Acreditación**
- 1 = 3 segundos,
- 2 = 5 segundos,
- 3 = 7 segundos.

Si el bit 'b3' del parámetro 'MASCARA MISCELÁNEA 4' está activado, los LED del Cabezal indicaran el estado virtual de "armado" / "desarmado":

LED verde = "desarmado"
LED rojo = "armado"

En el siguiente cuadro se combinan las diferentes posibilidades de coexistencia de la 'Situación : Bloqueado' o 'Situación : Inhibido' con la 'SubSituación : "desarmado"'(2):

SubSituación :	Bloqueado	Inhibido	LED verde	LED rojo
"armado"	No	No	apagado	encendido
"desarmado"	No	No	encendido	apagado
"armado"	Si	No	apagado	intermitente
"desarmado"	Si	No	encendido	intermitente
"armado"	No	Si	encendido	encendido
"desarmado"	Si	No	encendido	apagado

(En los Cabezales dotados con un solo LED, si el verde y el rojo están encendidos resulta color naranja).

OBSERVACIONES:
- No es compatible con la prestación anti **Pass-Back** en Instalaciones que usen estructuras **fS=4**.
- No es compatible con el bit 'b5[a]' de 'MASCARA MISCELÁNEA 3' (excepto si 'Tp' = 0).

NOTAS:
(1)
Mediante un pulso (contacto cerrado) generado por el **Panel de Alarmas externo** (el pulso tiene que ser >= 1 segundo, aunque se recomienda que sea, como mínimo, de 2 segundos).

(2)
La combinación de 'Situación : Inhibido' y 'SubSituación : "armado"' no tiene ningún sentido práctico.

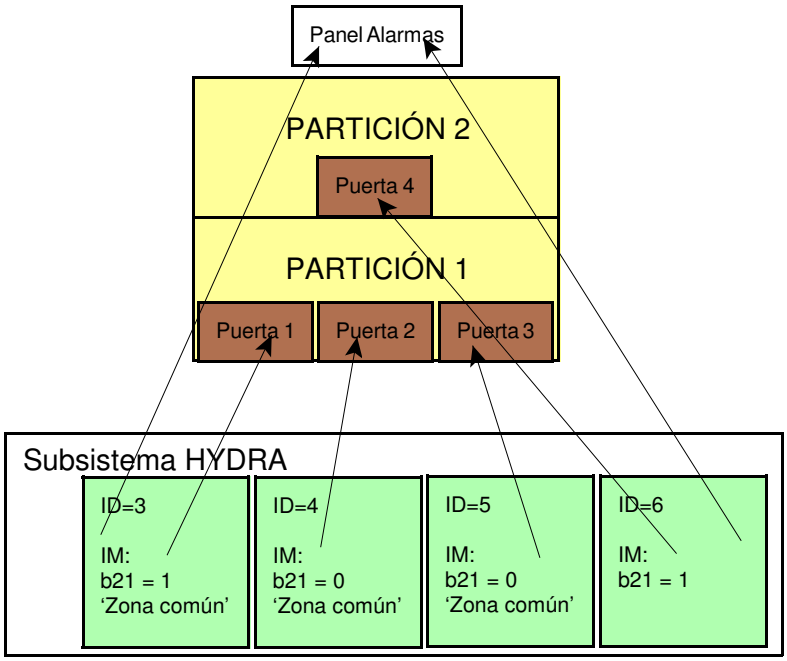
16.2 Versión de FW 08.02.00 y >> (para subsistema HYDRA)
Versión de FW 09.04.00 (para subsistema HYDRA-II)
Versión de FW 09.04.00 (para DEF-3002)

A partir de tales Versiones, a las prestaciones ya mencionadas en este documento se añadió la posibilidad de uso en 'zona común', la cual es exclusiva de los subsistema HYDRA (ver la Revisión E1 o posterior del documento BTP038) y de los subsistema HYDRA-II y de los Terminales *Modulares* modelo DEF-3002 (ver el documento BTP041).

A parte de algunas prestaciones estándar tales como el **Semáforo virtual** o el control de **esclusa** (sólo presentes en los equipos antedichos), existe una prestación de gran utilidad para el control del "Armado"/"Desarmado" con posibilidad de agrupar en una misma Partición del **Panel de Alarmas externo** a diferentes Terminales de un mismo subsistema HYDRA o a los dos Terminales de un mismo subsistema HYDRA-II o de un mismo equipo modelo DEF-3002. Para ello, todos los Terminales que formen parte de dicho grupo se deberán instalar, con la opción 4: uso en 'zona común' en el código "Control UEES" (bits b22, b23, b24 y b25 del parámetro 'IM' de la función *28 Instalar_Terminal* o la macrofunción *129 Instalar_fS=4*).

El Terminal del grupo con ID inferior (en el subsistema HYDRA) o el Terminal que se forme con el Cabezal #1 (en el subsistema HYDRA-II) se tiene que instalar también con el valor 4 cargado en el código "Control PANEL" por ser tal Terminal el que controlará las conexiones físicas con el **Panel de Alarmas externo** (para el subsistema HYDRA existe más información en el apartado 13.5 de la Nota de Aplicación QAN-13, mientras que para el subsistema HYDRA-II y para el Terminal *Modular* modelo DEF-3002 existe más información en el apartado 21.3 de la Nota de Aplicación QAN-21).

EJEMPLO (basado en un subsistema HYDRA)
Tenemos dos recintos con una Partición aplicada a cada uno de ellos; al primer recinto se accede desde tres puntos de paso diferentes; al segundo recinto se accede desde el primero mediante un único punto de paso.



A cada Módulo "H" se conecta un Cabezal lector-grabador, un contacto magnético y una cerradura de cada una de las puertas. Además, el primero (ID=3) y el último (ID=6) se conectan al **Panel de Alarmas externo**.

16.3 Versión de FW 08.03.00 y >> (para subsistema HYDRA)
Versión de FW 09.04.00 (para subsistema HYDRA-II)
Versión de FW 09.04.00 (para DEF-3001 y para DEF-3002)

A partir de tales Versiones el tipo de señal que el Terminal recibe del **Panel de Alarmas externo** puede ser por nivel, en vez de por pulso, indicando así el estado real del Panel (si la señal está en reposo indica "armado" y si está activada indica "desarmado"). Por lo tanto, el Panel puede forzar el cambio de 'Subsituación' a "armado", como hasta ahora, pero también puede forzarla a "desarmado". Además, el Panel puede informar al Terminal de si el cambio pretendido mediante la Salida 'Sad' se ha efectuado o no dentro del tiempo parametrizado. Mediante esta retroalimentación, la 'Subsituación' en la que se encuentra un Terminal con respecto al **Panel de Alarmas externo** conectado pasa a ser real y no virtual como en versiones de FW anteriores.

En el mapa de memoria de los Terminales se modificaron las direcciones 32 y 76 y se añadió la dirección 73. También fueron añadidos los códigos de evento:

CE=76: Iniciado el intento de "desarmado" (**marcaje normal** o **marcaje especial**)
CE=77: Iniciado el intento de "armado" (**marcaje normal** o **marcaje especial**)
CE=78: Fracasado el intento de "armado" / "Desarmado" (**marcaje especial**)

En el punto 16.3.1 se describe la operativa del FW cuando se trabaje con la Entrada indicada en 'Ead' por nivel. En este caso será dicha Entrada quien dictamine el estado final ("armado" / "desarmado") que tomará en consideración el Terminal.

16.3.1 "desarmado" mediante Acreditación

El usuario presenta su **Acreditación** en el Cabezal lector-grabador (éste tendrá el LED rojo encendido para indicar que la Partición del Panel está "armada"), y al retirar la **Acreditación** ocurre lo indicado a continuación (dependiendo del tiempo 'Td' definido en el parámetro 'LATENCIA ARMADO/DESARMADO'):

- Si 'Td' > 0 el FW genera un **marcaje normal** con CE=76, pone DIRECCIÓN 32 = 20h, activa la Salida indicada en 'Sad' para el "desarmado" y empieza un periodo de espera hasta que la Entrada indicada en 'Ead' confirme el cambio de estado en el Panel. Durante este periodo el Cabezal enciende y apaga el LED verde a razón de una vez cada 2 segundos para indicar dicha espera (cualquier **Acreditación** presentada durante este periodo será rechazada). Si se agota el tiempo 'Td', el FW genera un **marcaje especial** CE=78, regresa a la situación inicial (DIRECCIÓN 32 = 00h, activa el LED en rojo permanente, desactiva la Salida indicada en 'Sad' y realiza 2 pitidos (o un 'pirrip', según el modelo de Cabezal). En caso contrario, el FW genera un **marcaje especial** con CE=55, pone DIRECCIÓN 32 = 10h, mantiene activada la Salida indicada en 'Sad' para el "desarmado", enciende el LED verde de manera permanente y realiza un pitido para indicar que se ha "desarmado" correctamente. Para realizar un acceso, una vez la Partición está "desarmada", el usuario deberá presentar de nuevo su **Acreditación** (1).
- Si 'Td' = 0 (por ser la respuesta del Panel casi inmediata) el FW no realiza espera alguna y genera directamente el **marcaje normal** CE=55, pone DIRECCIÓN 32 = 10h, activa la Salida de "desarmado" ('Sad') y el LED verde de manera permanente. Sin embargo se ignora el estado actual de la Entrada 'Ead' durante un máximo de 5 segundos para dar tiempo al Panel a cambiar su estado. En caso afirmativo también se dará paso al usuario en la misma operativa (se genera un **marcaje normal** CE=34).

16.3.2 “armado” mediante Acreditación

El usuario presenta su **Acreditación** en el Cabezal lector-grabador (éste tendrá el LED verde encendido por estar la Partición "desarmada"). Al retirar la **Acreditación** pasado el tiempo definido en ‘Tp’, el FW genera un **marcaje normal** con CE=77, pone DIRECCIÓN 32 = 30h, desactiva la Salida ‘Sad’ para indicar "desarmado" y empieza un periodo de espera hasta que la Entrada ‘Ead’ confirme el cambio de estado en el Panel. Durante este periodo el Cabezal enciende y apaga el LED rojo y realiza un pitido a razón de una vez cada 2 segundos para indicar dicha espera (cualquier **Acreditación** presentada durante este periodo será rechazada). Si se agota el tiempo ‘Ta’ definido en el parámetro ‘LATENCIA ARMADO/DESARMADO’, el FW genera un **marcaje especial** con CE=78 y se vuelve a la situación inicial (DIRECCIÓN 32 = 10h, LED en verde permanente y Salida ‘Sad’ activada) y realiza 2 pitidos (o un 'pirrip', según el modelo de Cabezal). En caso contrario, el FW genera un **marcaje especial** con CE=56, pone DIRECCIÓN 32 = 10h, mantiene desactivada la Salida de “desarmado” (‘Sad’), enciende el LED rojo de manera permanente y realiza un tren de 6 pitidos para alertar que ya se ha “armado” correctamente.
Si se define ‘Td’ = 0, por ser la respuesta del Panel casi inmediata (menos probable en la maniobra de “armar”), el FW no realiza dicha espera y genera directamente el **marcaje normal** CE=56, pone DIRECCIÓN 32 = 00h, desactiva la Salida de “desarmado” (‘Sad’) y activa el LED rojo de manera permanente. Sin embargo, ignora el estado actual de la Entrada ‘Ead’ durante un máximo de 5 segundos para dar tiempo al Panel a cambiar su estado.

16.3.3 “armado” / “desarmado” por comunicaciones

Esta operativa del programa de aplicación queda simplificada a dar la orden al Panel dado que será éste el que se encargue de sincronizar al Terminal a través de ‘Ead’. Sin embargo, se mantiene esta prestación aunque sólo será efectiva si al campo 'SubSituación' se envía el valor 2 (intentando “desarmar”) pero sólo si previamente estaba “armado”, o el valor 3 (intentando “armar”) pero sólo si previamente estaba “desarmado”. En cualquier otra circunstancia sólo tendrá efecto el otro campo 'Situación' integrado en el mismo Byte de la DIRECCIÓN 32, facilitando así su gestión por parte de las aplicaciones **OEM**.
En ambas operativas, de “armado” y “desarmado”, el FW se comporta de manera similar a las operativas mediante **Acreditación** anteriormente descritas, aunque en este caso todo son **marcajes especiales**.

Cuando se trabaja por pulsos, el FW se comporta de manera similar a como lo hacía en las Versiones anteriores, excepto:
- En la operativa de “desarmado” el orden de los marcajes con CE=34 y CE=55 se invierte.
- Ahora también se permite definir ‘Ta’. Si ‘Ta’ > 0 el FW espera a que el Panel le envíe un pulso por la Entrada indicada en ‘Ead’ (todo se produce de manera similar a cuando la señal ‘Ead’ es por nivel).
- Para las maniobras vía comunicaciones de cambio “armado” / “desarmado” hay que enviar el valor 2 o el valor 3 en el campo 'SubSituación' en lugar del valor 1 o del valor 0, respectivamente. En el caso de querer “desarmar” el FW convertirá el 2 en 1 inmediatamente. En el caso de pretender “armar” el FW convertirá el 3 en 0 inmediatamente (Ta = 0) o cuando reciba un pulso por ‘Ead’ (Ta > 0).

NOTAS:
(1)
No es conveniente hacerlo de manera automática pues desde la maniobra de intento de “desarmado” hasta que ha “desarmado” podría llegar a transcurrir un tiempo considerable (hasta 1 minuto según la parametrización del **Panel de Alarmas externo**), por lo que el usuario podría ya no estar presente cuando el Terminal permitiera abrir la puerta, lo cual no es razonable.

16.4 Versión de FW 09.00.00 y >> (para subsistema HYDRA)
Versión de FW 09.04.00 (para subsistema HYDRA-II)
Versión de FW 09.04.00 (para DEF-3001 y para DEF-3002)

A partir de tales Versiones, la metodología descrita en el punto 16.3.1 queda adaptada a la posible activación del bit b6 del parámetro 'MÁSCARA MISCELÁNEA 4', de manera que si se presenta una **Acreditación** cuando la Partición del Panel esté "armada", aquella será rechazada con un marcaje normal con CE=87 excepto que tal **Acreditación** esté declarada en la Lista_Especial, en cuyo caso el FW "desarmará" la Partición.

Una explicación pormenorizada de la metodología funcional aplicada puede verse en el capítulo 2.7 de la Versión W (o posterior) del documento BTP027.

16.5 Versión de FW 09.13.00 (para DEF-3001)

A partir de tal Versión, los Terminales *Modulares* modelo DEF-3001 pueden ser usados en combinación con la prestación de **esclusa** de tipo 3 (extendida), de manera que en este caso la acción de "desarmado" y de "armado" no se ejecuta por la simple presentación de la **Acreditación** sino que el FW utiliza el contenido del parámetro 'CONTADOR AFORO' para decidir cuando debe hacerlo:

- si el contenido del subcampo 'CA' del parámetro 'CONTADOR AFORO' = 0 se "arma" la Partición del **Panel de Alarmas externo**, mientras que si el valor no es = 0 se "desarma" tal Partición.

Dado que se trata de un recinto cerrado, el montaje de la **esclus**a implica un doble sentido de paso, por lo que son necesarios dos Terminales *Modulares* modelo DEF-3001, debiendo cargar, en ambos Terminales, el valor 4 en el código "Control LOP" así como el valor 1 en el bit b8 (subcampo 'AS') del parámetro 'CONTADOR AFORO', aunque sólo uno de tales dos Terminales (el situado en el sentido de entrada al recinto y al que llamamos "Terminal-Panel") debe ser interconectado con el **Panel de Alarmas externo**, siendo en éste Terminal en el cual el programa **OEM** debe cargar el valor 4 en el código "Control Panel". El FW del Terminal situado en el sentido de salida se encarga de informar (para lo cual utiliza su Salida S5(1)) del paso de cada usuario al "Terminal-Panel" (el cual recibe la señal por su Entrada E9(1)) para que éste decremente en una unidad el subcampo 'CA' de su parámetro 'CONTADOR AFORO'.

En el caso de querer utilizar una segunda **esclusa** de tipo 3 (extendida) en el mismo recinto, hay que utilizar la Entrada E10(1) del "Terminal-Panel" (a la cual se conectará la señal proveniente de la Salida S5(1) del Terminal situado en el sentido de salida de la segunda **esclusa**) para hacer que el FW decremente en una unidad el subcampo 'CA', y hay que utilizar la Entrada E11(1) del "Terminal-Panel" (a la cual se conectará la señal proveniente de la Salida S5(1) del Terminal situado en el sentido de entrada de la segunda **esclusa**) para hacer que el FW incremente en una unidad el subcampo 'CA'.

Para impedir que se supere el aforo máximo del recinto, debe conectarse la Salida S5 del "Terminal-Panel" a la entrada del **Semáforo físico** (E6) del Terminal situado en el sentido de entrada de la segunda esclusa, por lo que quedará conectado en paralelo con la señal para el control del **Semáforo físico** proveniente del Terminal situado en el sentido de Salida de la segunda **esclusa**.

Una explicación pormenorizada de la metodología funcional aplicada puede verse en el capítulo 3.2 de la Versión C1 (o posterior) del documento BTP043.

NOTAS:
(1)
Dada la utilización atípica de estas Salidas y Entradas, en el siguiente cuadro se establece la relación entre la funcionalidad del FW y el necesario cableado físico en las placas:

funcionalidad	serigrafía en la placa	bornas
Salida S5	OUT1 (en conector CN13)	38 y 39
Entrada E9	IN1 (en conector CN9)	30 y 31
Entrada E10	IN2 (en conector CN9)	32 y 33
Entrada E11	IN5 (en conector CN9)	34 y 35

Para una mayor información hay que ver el Manual Informativo del Producto MIP-3001.

ESTA PÁGINA HA SIDO DEJADA EN BLANCO INTENCIONADAMENTE

código	título	relaciones
QAN-17	Inclusión en el **sistema CONACC** de un **Panel tipo mixto**	- MRT019 : completo

Esta Nota de Aplicación tiene como objetivo clarificar las peculiaridades de aquellos Terminales de Qontinuum que disponen de la capacidad de actuar como **Panel tipo mixto**, así como facilitar información a los programadores **OEM** para ayudarles a integrar tales Terminales en sus aplicaciones. Esta capacidad sólo es aplicable a los Terminales *Modulares* modelo MIF-709[(1)] (FW de Versión 8.5 y posterior) y a los Terminales *Modulares* modelo DEF-3001[(2)] (FW de Versión 9.0 y posterior), pudiendo actuar como *Control de Accesos* físicos y/o 'Zona llave' virtual por **Acreditación**, siendo una condición imperiosa para su uso el que no se requiera de conectividad a una receptora pública dado que no se utilizan protocolos estándar de mercado (como "CONTACT ID" o "SIA 2000").

La modalidad de **Panel tipo mixto** se diferencia de la de **Panel tipo interno** por tener algunas restricciones para asimilarlo al control del **Panel de Alarmas externo** y facilitar así a los programadores **OEM** la migración de aplicaciones que estén haciendo uso de éste último. Así pues los parámetros 'Sad', 'Tp', 'Taa'/'MEad', 'Ta', 'Td' (aunque éste último con significado diferente) y los estados "armado" / "desarmado" son tratados de igual manera en esta modalidad (ver QAN-16 para más detalles). De todos modos, los programas **OEM** deberán implementar la función FU=72 (para poder definir el resto de parámetros del Panel) y la función FU=71 (para interactuar con él), así como gestionar el **marcaje normal** con CE=79 y los **marcajes Panel** (CE=113).

Se activa con la opción 6: **Panel tipo mixto** en el código "Control Panel" del parámetro 'IM' de la función *28 Instalar_Terminal* o la macrofunción *129 Instalar_fS=4*. Con ella se permite que una o varias Entradas (cada Entrada corresponde, normalmente, a un sensor) conjuntamente con una o varias Salidas (cada Salida corresponde a un relé) sean vinculados en hasta un máximo de 8 agrupaciones de Entradas y Salidas, agrupaciones a las que se denomina Particiones.

Tales Particiones pueden ser de dos tipos:

- de 'operativa **local**' : es aquella que puede interrumpir temporalmente el control de sus Entradas para permitir el acceso de personal autorizado, dentro de su área de supervisión, sin generar alarma aún cuando detecte actividad en sus Entradas; para ello debe permitir ser "desarmada", y posteriormente "armada", mediante una 'operativa local', siendo posible definir una serie de tiempos para que el usuario pueda realizar tales operativas sin causar alarmas (un ejemplo de Partición de 'operativa local' seria la que controla Entradas tales como el contacto magnético de la puerta de acceso, un volumétrico en el área de paso, etc.).
  Cuando en este documento se haga referencia al "armado" o "desarmado" del Panel hay que entenderlo como referido a la Partición #1.

- de ‘24H’ : son las que controlan sus Entradas de manera continua; pueden generar alarma, por actividad en sus Entradas, a cualquier hora del día (por ejemplo, las Particiones con Entradas para detectores de incendio, pulsadores de emergencia, etc.).

Todas las Particiones pueden ser “armadas” (generan alarma cuando detectan una Entrada activa) o “desarmadas” (no generan alarma) vía comunicaciones, pero sólo en la Partición de ‘operativa local’ puede realizarse el “armado” / “desarmado” por otros medios (como el uso de **Acreditaciones** en un Cabezal de lectura-escritura).

La ‘operativa local’ puede realizarse por dos vías: con la presentación de una **Acreditación** en el Cabezal lector-grabador (‘Zona llave’ virtual) o a través de una Entrada declarada como ‘Zona llave’; el propio FW también podrá, de manera automática, “re-armar” una Partición que haya sido “desarmada”, pasado un tiempo determinado de inactividad en sus Entradas. Si se utiliza el Cabezal lector-grabador como ‘Zona llave’ virtual es necesario presentar una **Acreditación** que supere todas las validaciones del sistema: formato correcto, **Lista_Blanca** o **Lista_Negra**, horario, etc. Si se utiliza una Entrada declarada como ‘Zona llave’, ésta puede configurarse para ser activada por pulso (sólo permite “armar”) o por nivel (permite “armar” y “desarmar”) desde un pulsador, un contacto de llave, un sistema externo, etc. Además de los **marcajes Panel** con CE=113 pertinentes para indicar cada una de las acciones en el Panel, cuando éstas sean causa de la presentación de una **Acreditación**, se generará previamente un **marcaje normal** con CE=79 para registrar el **NIS** implicado.

NOTAS:
(1)
A partir de los FW de Versión 8.6 existe compatibilidad funcional con los Terminales *Especiales* modelos DEF-PCTn (ver el Anexo H del documento MRT019.

(2)
A partir de los FW de Versión 9.5 existe compatibilidad funcional con los Terminales *Especiales* modelos DEF-PCTn (ver el Anexo H del documento MRT019.

17.1 Características de las Entradas

Todas las Entradas pueden programarse para que sean de efecto inmediato o temporizado con tiempos individualizados. A las que son temporizadas también se les pueden indicar el tipo de activación para que la Entrada correspondiente, para ser efectiva, tenga que estar activa (por nivel) o no estarlo (por pulso) durante todo el tiempo de temporización. Este último caso es especialmente útil, en la Partición de 'operativa local', para Entradas con una posible activación de corta duración, como, por ejemplo, una barrera de rayos infrarrojos; aunque ello implica tener que definir un tiempo 'Td' suficientemente grande para poder salir del recinto sin generar alarma al "Armar" la Partición en modo local.

Cada Entrada temporizada puede asociarse a un Horario (parámetro 'TABLA_GRUPOS') distinto para alterar, mediante un factor multiplicador, el tiempo de temporización según un horario (parámetro 'TABLA_HORARIOS') de una o dos franjas para cada día de la semana (alterable temporalmente según el parámetro 'TABLA_AGENDA'); tal factor también pude ser 0, en cuyo caso la Entrada queda anulada durante esos períodos.

Las temporizaciones también permiten dar tiempo al usuario para que éste realice un "desarmado" local cuando el Cabezal lector-grabador esté dentro del área de supervisión de las Entradas implicadas.

Cada Entrada se asocia a una Partición (de la #1 a la #8) y a cada Partición se le asigna una o varias Salidas de activación. La relación puede ser directa (alarma activada hasta que se restablece el estado de la Entrada causante), o de enclavamiento (alarma activada, aún cuando el estado de la Entrada causante se restablezca, hasta que se desactive vía comunicaciones o presentando una **Acreditación** válida). Independientemente de si la relación es directa como si es de enclavamiento, es posible definir, de manera individual, un tiempo mínimo de activación por alarma para cada Salida (excepto para la Salida R1). Es recomendable definir como enclavables las Particiones con Entradas temporizadas activadas por pulso.

En el parámetro 'INTERACCIÓN PANEL' se puede definir una salida en 'Sad' (S2..S4) para indicar "armado" (desactivada) o "desarmado" (activada) que puede ser utilizada para una señalización de la Partición de 'operativa local'. El LED propio del Cabezal lector-grabador también puede usarse para dicha señalización (luz roja para indicar "armado" y luz verde para indicar "desarmado") si se activa el bit b3 del parámetro 'MÁSCARA MISCELÁNEA 4'.

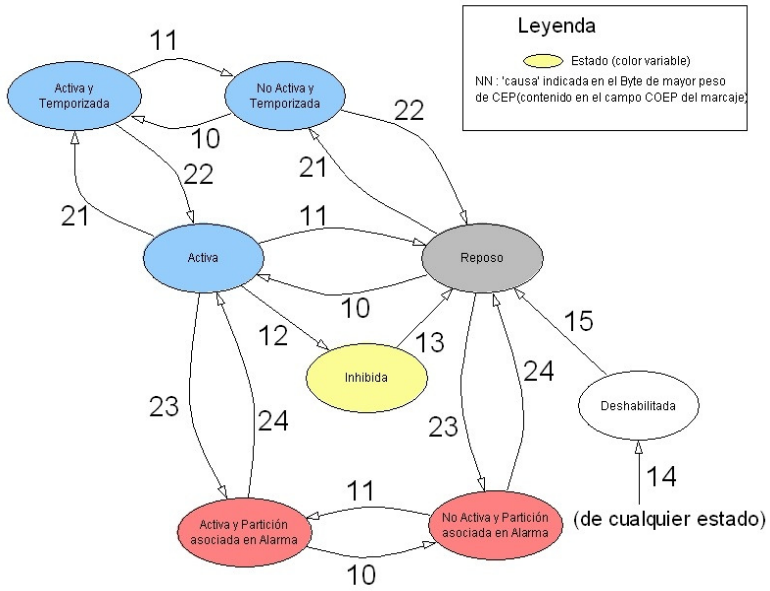
Para los Terminales *Modulares* modelo MIF-709, el número de Entradas y Salidas disponibles dependerá del número de módulos de E/S utilizados:

ASSY100 :	ninguno	un módulo	dos módulos
Configuración 'IM' (bit b15, b16 y b17) :	4	5	6
Salidas :	**4** (R1,R2,S3,S4)	**8** (R1,R2,S3..S8)	**12** (R1,R2,S3..S12)
Entradas :	**4** (E1,E2,E5,E6)	**8** (E1,E2,E5,E6, E9..E12)	**12** (E1,E2,E5,E6, E9..E16)
Entradas (virtuales) :	**1** (E4)	**2** (E4 y E8)	**2** (E4 y E8)
	E4 : **"tamper"** en Cabezal: no hay comunicación con el Cabezal E8 : 'error de Bus interno' (comunicaciones) con el/los módulo(s) de E/S		

Para los Terminales *Modulares* modelo DEF-3001, el número de Entradas y Salidas disponibles dependerá del número de módulos de E/S utilizados:

ASSY100 :	ninguno	un módulo
Configuración 'IM' (bit b15, b16 y b17) :	5	6
Salidas :	**8** (R1,R2,S3..S8)	**12** (R1,R2,S3..S12)
Entradas :	**8** (E1,E2,E5,E6, E9..E12)	**12** (E1,E2,E5,E6, E9..E16)
Entradas (virtuales) :	**1** (E4)	**2** (E4 y E8)
	E4 : **"tamper"** en Cabezal: no hay comunicación con el Cabezal E8 : 'error de Bus interno' (comunicaciones) con el módulo de E/S	

Para los marcajes relacionados con las Entradas y los posibles estados de éstas se puede seguir el siguiente diagrama:



Los colores de los estados son los utilizados por el programa de aplicación WinAcces y, por tanto, son sólo orientativos. Dado que el FW sólo puede grabar un código de 'causa' en cada marcaje, para indicar que una Entrada pasa de un estado a otro pueden ser necesarios dos marcajes (con una separación entre ellos de hasta 1 segundo).

A continuación se explican los estados indicados en el diagrama anterior:

Activa: el estado físico de la Entrada más la máscara NO/NC indica "Entrada activa" y no ha iniciado su temporizador. Este estado es transitivo(1), y sólo puede ser permanente(1) si la Partición a la que está vinculada la Entrada está "desarmada" o "intentado armar".

Activa y Temporizada: el estado físico de la Entrada más la máscara NO/NC indica "Entrada activa" y ha iniciado su temporizador. Este estado sólo se puede dar si la Partición a la que está vinculada la Entrada está "armada".

No Activa y Temporizada: la Entrada ha iniciado su temporizador y físicamente está en reposo. Este estado sólo se puede dar si la Entrada ha sido configurada por pulso y la Partición a la que está asignada está "armada".

Activa y en Alarma: la Entrada ha agotado su temporizador (si el temporizador es 0 se pasa directamente a este estado sin pasar antes por el estado de Temporizada). Indica que esta Entrada ha hecho que la Partición a la que está asignada pase a estado de alarma. Este estado sólo se puede dar si la Partición está "armada". También indica que la Entrada está físicamente activa.

No Activa y en Alarma: la Entrada ha agotado su temporizador (si el temporizador es 0 se pasa directamente a este estado sin pasar antes por el estado de Temporizada). Indica que esta Entrada ha hecho que la Partición a la que está vinculada pase a estado de alarma. Este estado sólo se puede dar si la Partición está "armada". Este estado será transitivo(1) si la Entrada está configurada por pulso. También indica que la Entrada está físicamente en reposo.

Reposo: la Entrada está en reposo, lo que quiere decir que no está Activa ni Temporizada ni en Alarma. Físicamente está en reposo.

Inhibida: el FW ha inhibido la Entrada para poder armar. El FW ignorará el estado de esta Entrada, por lo tanto tal Entrada no hará que la Partición pase a estado de alarma. Indica que la Entrada está físicamente activa. Cuando la Entrada cambie y esté físicamente en reposo se pasará a estado "Reposo".

Deshabilitada: la Entrada ha sido deshabilitada a través de comunicaciones. La Entrada sólo puede habilitarse a través de comunicaciones. El FW ignorará el estado de la Entrada, por lo tanto tal Entrada no hará que la Partición pase a estado de alarma. Además, el FW no generará ningún marcaje para indicar el estado físico de la Entrada, por lo tanto el estado físico de la Entrada es desconocido.

NOTAS:
(1) Se considera estado transitivo el estado intermedio que el FW usa para pasar de un estado a otro, y estado permanente el estado en el que la Entrada puede permanecer durante más de un segundo.

17.2 Operativas

17.2.1 "desarmado"

La operativa de "desarmado" siempre será de ejecución inmediata sea cual sea la Partición o el medio de actuación.

Peculiaridades de la 'operativa local' a través del Cabezal lector-grabador:

- La **Acreditación** válida debe presentarse sólo durante el tiempo mínimo para la lectura y (sólo en formato **fS=4**) su posible grabación; al hacerlo se oye un pitido y se apaga momentáneamente el LED rojo para indicarlo, debiendo ser retirada antes de que se supere el tiempo definido en el campo 'Tp' del parámetro 'INTERACCIÓN_PANEL'.
- Es posible indicar al Panel que, una vez "desarmado", facilite el acceso activando la Salida R1 si se ha definido un tiempo superior a 0 para esta Salida. Para ello, el Cabezal lector-grabador debería ser instalado en la parte exterior del área controlada por la Partición, y la Salida R1 debería ser conectada a la cerradura eléctrica de la puerta de acceso. En este caso, y estando "desarmada" la Partición, cualquier presentación (durante un tiempo < 'Tp') de una **Acreditación** válida seguirá el tratamiento normal dado a los intentos de acceso, por lo que, si resulta correcto, el FW generará un **marcaje normal** con CE=34.

A partir de la Versión de FW 09.00.00, la metodología descrita queda adaptada a la posible activación del bit b6 del parámetro 'MÁSCARA MISCELÁNEA 4', de manera que si se presenta una **Acreditación** cuando la Partición de 'operativa local' del Panel esté "armada", aquella será rechazada con un **marcaje normal** con CE=87 excepto que tal **Acreditación** esté declarada en la Lista_Especial, en cuyo caso el FW "desarmará" la Partición de 'operativa local'.

El FW realiza esta operativa considerando que el valor contenido en el campo 'Td' del parámetro 'LATENCIA ARMADO' es diferente de 0 aunque realmente fuera = 0, de manera que el usuario que haya "desarmado" a la Partición deberá presentar de nuevo su **Acreditación** para intentar el acceso.

17.2.2 “armado”

La operativa de “armado” para las Particiones de ‘24H’ siempre será de ejecución inmediata.

Para la Partición de ‘operativa local’ dependerá del medio de actuación (el “re-armado”, por ejemplo, siempre será inmediato) o de la parametrización. A excepción de los casos mencionados, cuya respuesta es inmediata, para el resto de casos el **Panel tipo mixto** sólo considerará la Partición “armada” si todas sus Entradas vinculadas están en reposo antes de transcurrir el tiempo definido en el campo ‘Ta’ (parámetro ‘LATENCIA ARMADO/DESARMADO’).

De todas las Entradas de la Partición se puede indicar cuales deben estar inactivas para permitir al Panel “armar”, y, de entre tal grupo, a cuales se les permite eximirse de dicha responsabilidad si pasado el tiempo ‘Ta’ existen otras Entradas operativas de la Partición que sí estén en situación de inactividad, exceptuando las que no tengan la obligación de estarlo. Si es así, el Panel las inhibe temporalmente hasta que se restablezca su estado de reposo o hasta que se inicie otro intento de “armado” (excepto en el re-armado” automático).

Para la ‘operativa local’ (no aplicable vía comunicaciones) también es posible definir en el campo ‘Td’ (parámetro ‘LATENCIA ARMADO/DESARMADO’) un tiempo previo y fijo de demora para que el Panel, una vez recibida la orden, espere a intentar “armar” la Partición y así dar tiempo al personal para salir de donde corresponda.

Cuando ‘Ta’ y ‘Td’ se definan con valor 0, la respuesta también será inmediata, en caso contrario ambas esperas serán indicadas por el Panel con un pitido y un destello del LED rojo cada 2 segundos.

17.2.3 Peculiaridades de la ‘operativa local’ a través del Cabezal lector-grabador

- La **Acreditación** válida debe presentarse el tiempo mínimo para la lectura y, sólo para el formato **fS=4**, su posible grabación (se oye un pitido y se apaga durante un segundo el LED rojo para indicarlo) más el tiempo definido en ‘Tp’ de 3, 5 ó 7 segundos (el LED rojo vuelve a apagase cuando ha transcurrido dicho tiempo) antes de que la **Acreditación** deba ser retirada.

17.2.4 Resumen

En el siguiente cuadro se resume las diferentes posibilidades de “armar” y “desarmar” los dos tipos de Particiones:

<table>
<tr><td rowspan="3">Partición ...</td><td rowspan="3">por medio de ...</td><td colspan="4">efecto ...</td></tr>
<tr><td colspan="2">‘Ta’ = 0</td><td colspan="2">‘Ta’ > 0</td></tr>
<tr><td>‘Td’ = 0</td><td>‘Td’ > 0</td><td>‘Td’ = 0</td><td>‘Td’ > 0</td></tr>
<tr><td colspan="6">“desarmado”</td></tr>
<tr><td>... de ‘24H’</td><td>... comunicación</td><td colspan="4" rowspan="4">... inmediato</td></tr>
<tr><td rowspan="3">... de ‘operativa local’</td><td>... comunicación</td></tr>
<tr><td>... Cabezal</td></tr>
<tr><td>... Entrada (por nivel)</td></tr>
<tr><td colspan="6">“armado”</td></tr>
<tr><td>... de ‘24H’</td><td>... comunicación</td><td colspan="4">... inmediato</td></tr>
<tr><td rowspan="4">... de ‘operativa local’</td><td>... comunicación</td><td colspan="2">Inmediato</td><td colspan="2">Espera (máx. ‘Ta’) Entradas en reposo</td></tr>
<tr><td>... Cabezal</td><td rowspan="2">Inmediato</td><td rowspan="2">Espera fija (‘Td’)</td><td rowspan="2">Espera (máx. ‘Ta’) Entradas en reposo</td><td rowspan="2">Espera fija (‘Td’) + Espera (máx. ‘Ta’) Entradas en reposo</td></tr>
<tr><td>... Entrada (por pulso o por nivel)</td></tr>
<tr><td>... “re-armado”</td><td colspan="4">... inmediato</td></tr>
</table>

En el siguiente cuadro se resumen los marcajes relacionados con la operativa de “armar” o “desarmar” una Partición de ‘operativa local’, donde entre paréntesis aparece, según el caso, el **NIS** o el **COEP** (con sus 4 campos: origen/destino, causa, causante y tipo causante):

Nomenclatura utilizada en el siguiente cuadro (ver también el Anexo D):
LA = Latencia “armado” (implica ‘Ta’ + ‘Td’) P = Partición (el número) E = Entrada (el número) Op = Operador (la identificación)

OPERATIVAS	**SECUENCIA DE CÓDIGOS DE EVENTO**
Operativas por automatismo:	
“re-armado”	CE=113 (P, 5, 0, 0)
Operativas por **Acreditación**:	
Condición: Partición de ‘operativa local’ “armada”	
“desarmado”	CE=79 (NIS) + CE=113 (P, 6, 0, 1) + [CE=34 (NIS)](*)
intento “armado” ignorado	CE=79 (NIS)
Condición: Partición de ‘operativa local’ “desarmada”	
Acceso/desactivar alarma	CE=79 (NIS) + [CE=113 (P, 8, 0, 1)](**) + [CE=34 (NIS)](*)
“armado” (LA=0)	CE=79 (NIS) + CE=113 (P, 5, 0, 1)
“armado” correcto (LA>0)	CE=79 (NIS) + CE=113 (P, 3, 0, 1) ... CE=113 (P, 5, 0, 1)
“armado” fallido (LA>0)	CE=79 (NIS) + CE=113 (P, 3, 0, 1) ... CE=113 (P, 4, 0, 1)
Operativa local rechazada por intento de “armado” en curso	CE=79 (NIS) + CE=113 (P, 20, 0, 1)
(*) sólo cuando haya acceso (tiempo Salida R1 > 0) (**) sólo cuando esté activa una alarma desactivable	
Operativas por ‘Zona llave’:	
“desarmado”	CE=113 (P, 6, E, 2)
“armado” (LA=0)	CE=113 (P, 5, E, 2)
“armado” correcto (LA>0)	CE=113 (P, 3, E, 2) ... CE=113 (P, 5, E, 2)
“armado” fallido (LA>0)	CE=113 (P, 3, E, 2) ... CE=113 (P, 4, E, 2)
Operativa local rechazada por intento de “armado” en curso	CE=113 (P, 20, E, 2)
Nota: cuando la Entrada implicada indica el uso por pulsos y la Partición está “armada”, se ignora cualquier intento de “armado” y no se generan marcajes..	

Operativas por comunicación:	
“desarmado”	CE=113 (P, 6, Op, 3)
“armado” (LA=0)	CE=113 (P, 5, Op, 3)
“armado” correcto (LA>0)	CE=113 (P, 3, Op, 3) ... CE=113 (P, 5, Op, 3)
“armado” fallido (LA>0)	CE=113 (P, 3, Op, 3) ... CE=113 (P, 4, Op, 3)
Nota: el rechazo de la orden de “armado” por ya estarlo o por intento de “armado” en curso no genera marcaje y se indica con un ST=69 en el momento de recibir la orden.	

17.3 Ejemplos aplicativos

17.3.1

Parametrización para un pequeño recinto (tipo faro, aerogenerador, garita, subestación, etc) con los siguientes elementos:
- un contacto magnético en la puerta de entrada;
- un sensor volumétrico en el exterior del recinto;
- un sensor volumétrico en la planta baja del interior del recinto;
- un Cabezal lector-grabador en la planta baja del interior del recinto (uso como 'Zona llave' virtual);
- un pulsador de emergencia en la planta baja del interior del recinto;
- un detector de incendios en la planta baja del interior del recinto;
- un pulsador de emergencia en la planta superior del interior del recinto;
- un detector de incendios en la planta superior del interior del recinto:

DEFINICIÓN DE ENTRADAS					
Entrada	Función	Tipo vinculación "armado"	Temporización [factor horario] (tipo activación)	Grupo horario	Partición
E1	Contacto magnético	3(1)	T1=15" [x4](3)	1 (de 7 a 19h)	#1
E2	Volumétrico IR 2 exterior	1(2)	T2=30" [x4](4)	1 (de 7 a 19h)	#1
E4	Fallo/vandalismo Cabezal	-	inmediata	-	#4
E5	Fallo Alimentación(5)	-	inmediata	-	#4
E6	Volumétrico IR 1 interior	3(1)	T6=10" [x4](4)	1 (de 7 a 19h)	#1
E8	Fallo/vandalismo módulo maniobras	-	inmediata	-	#4
E9	Detector Incendio abajo	-	inmediata	-	#3
E10	Pulsador emergencia abajo	-	T10=2"(4)	-	#2
E11	Detector Incendio arriba	-	inmediata	-	#3
E12	Pulsador emergencia arriba	-	T12=2"(4)	-	#2

DEFINICIÓN DE SALIDAS		
Salida	TSn	Descripción
S3	0	Señalización sistema "armado" / "desarmado" (desactivada / activada)
S5	4	Sirena
S6	8	Luces sorpresivas
S7	0	Opcional
TSn = Tiempo excitación Salida Sn (en segundos)		

DEFINICIÓN DE PARTICIONES				
Partición	Función	Tipo	Enclavable	Salidas
#1	Intrusión	de 'operativa local'	Si	S5 y S6
#2	Emergencias	de '24H'	No	S6
#3	Incendios	de '24H'	No	S5 y S6
#4	Vandalismo/Averías	de '24H'	No	S7

OTROS
Sad' = Salida S3 Tp' = 5 seg. Td' = 30 seg. Ta' = 1 minuto.

Con el sistema "armado", si el volumétrico exterior (Entrada E2) detecta presencia por más tiempo de 30 segundos (T2) o de 2 minutos (T2x4) en horario de trabajo sin que se haya efectuado una operativa de "desarmado", se dispara la Alarma de la Partición #1 activando la sirena (Salida S5) y las luces sorpresivas (Salida S6) hasta que se "desarme" la Partición #1 (mediante **Acreditación** o vía comunicaciones). A cada activación de la Entrada E2 se genera el **marcaje Panel** correspondiente, y se genera otro al desactivarse la Entrada E2 incluso si la Alarma de la Partición #1 ya estuviese disparada.

Si, con la Partición #1 "armada", el contacto magnético (Entrada E1) indica puerta abierta, aunque sea un instante, y antes de 15 segundos (T1) o de 1 minuto (T1x4) en horario de trabajo no se "desarma" la Partición, se dispara la Alarma de la Partición #1 activando la sirena (Salida S5) y las luces sorpresivas (Salida S6) hasta que se desarme la Partición #1 (mediante una **Acreditación** o vía comunicaciones). En la primera activación de la Entrada E1 se genera un **marcaje Panel** para indicar estado de pre-alarma, y se genera otro al finalizar dicho estado. Independientemente de estos marcajes, se generaran otros dos para indicar el estado real de la Entrada tantas veces como cambie de estado dicha Entrada.

Si, con la Partición #1 "armada", el volumétrico interior (Entrada E6) indica presencia durante más de 10 segundos (T6) o de 40 segundos (T6x4) en horario de trabajo, se dispara la Alarma de la Partición #1 activando la sirena (Salida S5) y las luces sorpresivas (Salida S6) hasta que se desarme la Partición #1 (mediante una **Acreditación** o mediante la función *71 Control_Panel*). A cada activación de la Entrada E6 se genera el **marcaje Panel** correspondiente, y se genera otro al desactivarse incluso si la Alarma de la Partición #1 ya estuviese disparada.

La primera vez que una Entrada activa la alarma de la Partición #1 también se genera el **marcaje Panel** correspondiente, y se genera otro cuando esta alarma es desactivada.

Para "desarmar" el sistema es suficiente con presentar en el Cabezal lector-grabador una **Acreditación** válida, aunque también es posible realizar el "desarmado" mediante la función *71 Control_Panel*.

Para iniciar el proceso de “armado” de la Partición #1 es necesario presentar en el Cabezal lector-grabador una **Acreditación** válida y mantenerla durante un tiempo mínimo de 5 segundos (‘Tp’). A partir de ahí el FW espera un mínimo de 30 segundos (‘Td’) ignorando las Entradas E1 y E6. Agotado dicho tiempo, el FW espera a que las Entradas E1 y E6 estén en estado inactivo para poder “armar”. Si transcurrido 1 minuto (‘Ta’) ambas Entradas están en estado activo, se aborta el intento de “armar”. Si al menos una de ellas está en estado inactivo, se inhibe la otra y se “arma” la Partición #1. También es posible iniciar el proceso de “armado” de la Partición #1 mediante la función *71 Control_Panel*. En este caso el Panel actúa de la misma manera pero sin realizar la primera espera de 30 segundos.

Resumen de las situaciones, en cada momento, del proceso de “armado”:

CONDICIÓN:	SITUACIÓN:
t < ‘Td’	Partición #1 “desarmada” a la espera de “armar”
‘Td’ > t < ‘Ta’ y E1 inactiva y E6 inactiva	Partición #1 “armada”
t = ‘Ta’ y E1 activa y E6 activa	Partición #1 “desarmada” (intento “armar” abortado)
t = ‘Ta’ y E1 activa y E6 inactiva	Partición #1 “armada” (E1 Inhibida)
t = ‘Ta’ y E1 activa y E6 activa	Partición #1 “armada” (E6 Inhibida)

Las Entradas tipo ‘24H’ actúan independientemente de si el Panel está “armado” o “desarmado” (Partición #1). Si se activa una de dichas Entradas (de inmediato para la E9 y la E10 o si se mantiene durante un mínimo de 2 segundos para la E11 y la E12) se genera el **marcaje Panel** pertinente (con causa tipo 9, 10 ,11 ó 12 según la Entrada implicada) y se dispara la Alarma de la Partición #3, activando la sirena (Salida S5) y las luces sorpresivas (Salida S6), para los detectores de incendio (Entradas E9 y E11) o la Alarma de la Partición #2, activando sólo las luces sorpresivas, para los pulsadores de emergencia (Entradas E10 y E12). Al restablecerse la Entrada en cuestión a su estado de reposo se genera el **marcaje Panel** correspondiente y se desactiva/n la/s Salida/s mencionada/s. En estos casos, si la Alarma en cuestión no estaba previamente activada, se genera también un **marcaje Panel** indicándolo, al igual que se genera otro al desactivarse.

Como las alarmas de la Partición #2 y de la Partición #3 pueden ser de corta duración se ha definido un tiempo mínimo de 4 y 8 segundos para la activación de las Salidas S5 y S6 respectivamente. Este tiempo no afecta cuando estas Salidas se activen por una alarma en la Partición #1 ya que ésta es del tipo enclavable.

NOTAS:
(1)
Indica que se tiene en cuenta en la operativa local de “armar”, pero puede ser inhibida por el FW.

(2)
Indica que no se contempla en la operativa local de “armar”.

(3)
Activación por pulso (sólo requiere un cambio de ‘estado de reposo’ a ‘estado activo’).

(4)
Activación por nivel (la Entrada debe mantenerse activa el tiempo definido para ser efectiva).

(5)
Se podrá hacer uso de la Entrada E5 si el SAI (Sistema de Alimentación Ininterrumpida) utilizado dispone de una salida para indicar fallo de red eléctrica

17.3.2

Como variante del ejemplo anterior (17.3.1) se podría considerar el mismo escenario, pero con el Cabezal lector-grabador situado en la parte exterior del recinto, actuando como 'Zona llave' virtual y como *Control de Accesos* físico (para la apertura de la puerta). En este caso se debería definir un tiempo de RELE1 para la excitación de la cerradura eléctrica, y también se cambiaria el contenido de algunos de los parámetros:

DEFINICIÓN DE ENTRADAS					
Entrada	Función	Tipo vinculación "armado"	Temporización [factor horario] (tipo activación)	Grupo horario	Partición
E1	Contacto magnético	3(1)	inmediata	-	#1
E6	Volumétrico IR 1 interior	3(1)	inmediata	-	#1

OTROS
Td' = 0 seg.

DEFINICIÓN DE SALIDAS		
Salida	TSn	Descripción
R1	5	Cerradura eléctrica para la puerta de acceso.
TSn = Tiempo excitación Salida Sn (en segundos)		

Con ello, a cada presentación de una **Acreditación** válida en el Cabezal por un tiempo que sea inferior a 'Tp', se activara la Salida R1 durante un tiempo de 5 segundos, para permitir el acceso.

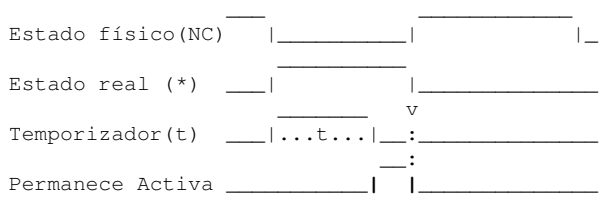
NOTAS:

(1)

Indica que se tiene en cuenta en la operativa de "armar" localmente, pero puede ser inhibida por el FW.

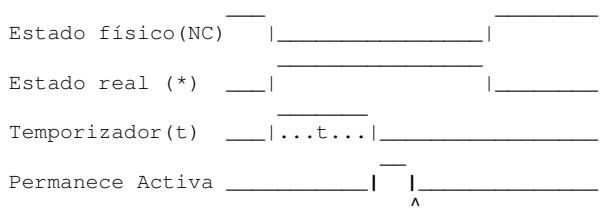
17.4 Ejemplos lógicos

17.4.1
Entrada activada por nivel con final por cambio de estado:



(*) Según Selector NC/NO

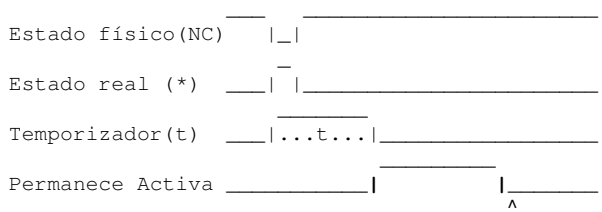
17.4.2
Entrada activada por nivel con final por desarmado:



"desarmado"

(*) Según Selector NC/NO

17.4.3
Entrada activada por pulso (flanco):



"desarmado" o Alarma desactivada

(*) Según Selector NC/NO

ESTA PÁGINA HA SIDO DEJADA EN BLANCO INTENCIONADAMENTE

código	título	relaciones
QAN-18	Interacción con el sistema Kone	- MRT019 : capítulo 3 (*Dirección 57*) (*Direcciones 83-84* y *85-86*) (*Dirección 91*) - MRT019 : capítulo 5 (función *20*) (función *28*, código "Control LOP") - MRT019 : Anexo B.1 - MRT019 : Anexo G - BTP027 (Revisión W y >>): capítulo 2.14

Esta Nota de Aplicación debe ser tomada como guía para la correcta integración en el **sistema CONACC** del sistema Kone de gestión de ascensores, para lo cual se ha escrito la **capa Kone** como elemento de intercomunicación con el sistema Kone. La **capa Kone** utiliza un protocolo específico de Kone en combinación con la Lista_Otras_Prestaciones (ver el capítulo 3 del documento MRT019), y es exclusiva de los Terminales *Modulares* modelo DEF-3001(4).

La interacción de la **capa Kone** con el sistema Kone tiene por objetivo comunicar a éste cual es la planta de destino de los usuarios y sus requerimientos específicos de transporte (si los hay) a medida que éstos son identificados por el Terminal (normalmente situado en un torno de paso, pero no exclusivamente) y su acceso es admitido, por lo que cualquier imposibilidad de comunicación entre la **capa Kone** y el sistema Kone no afectará en ningún sentido a tales accesos. Por tal razón, si el sistema de Kone no estuviera operativo, el *Control de Accesos* seguirá funcionando normalmente, aunque los usuarios perderán la indicación del ascensor que deben tomar para acceder a su planta de trabajo.

El programa **OEM** es responsable de preparar y cargar en los Terminales adecuados la Lista_Otras_Prestaciones, así como de haber establecido previamente su uso mediante el código "Control LOP" (al instalar el Terminal mediante la función *28 Instalar_Terminal* o la macrofunción *129 Instalar_fS=4*).

Dado que los Terminales *Modulares* modelo DEF-3001(4) utilizan un elemento **TInGW**, es en éste donde la **capa Kone** encuentra la información necesaria para establecer y para mantener la intercomunicación con el sistema Kone, de manera que el Administrador del sistema deberá aportar la información necesaria para ello mediante el uso del programa de utilidad Q2_UTIL (Versión 7.0 o posterior).

Cuando el código “Control LOP” contiene el valor 1, la Lista_Otras_Prestaciones (sólo si está declarada) permite que el FW del Terminal, una vez validada por completo la **Acreditación** presentada, utilice la **capa Kone** para comunicar al sistema Kone el dato ‘planta destino’ y el dato ‘puerta salida’ indicado en el elemento ‘Cápsula_1' de tal Lista correspondiente al **NIS** del usuario al que se ha concedido el acceso, de manera que el sistema Kone sepa la planta de destino del usuario y la puerta de salida del ascensor (de las dos posibles) que deberá abrir y, en consecuencia, informe al usuario (por medio de un visualizador de Kone o de un Cabezal de Qontinuum con pantalla(4)) de cual es el ascensor que deberá tomar y de cual es el tiempo estimado de llegada para que el usuario pueda tomarlo.

La adaptación de valores para el sistema Kone la realiza la **capa Kone** del Terminal, lo cual libera de tal trabajo al programa **OEM**.

18.1 Casuísticas

18.1.1

Dependiendo de la afluencia sistemática de usuarios tanto en ciertos momentos del día como por eventos especiales, es razonable pensar que pueda existir la necesidad de agilizar el proceso de acceso en los puntos de paso que interaccionen con el sistema Kone, por lo cual, y con la intención de facilitar al operador del programa **OEM** el uso discrecional de tal interacción, tal programa debería implementar el uso del bit b3[a] del parámetro ‘MÁSCARA MISCELÁNEA 5', por el cual el FW del Terminal desactiva (y activa de nuevo) tal interacción sin necesidad de otras operativas sobre la memoria del Terminal, propiciando así el mejor uso posible de este recurso.

18.1.2

Aunque el sistema Kone informa a los usuarios de cual será el ascensor que deberá tomar para acceder a su planta de destino mediante una pantalla de visualización de la propia Kone, y de manera complementaria (que podría ser suplementaria si no se instalara tal visualizador de Kone), si está definido un texto para el mensaje establecido para la situación [x : TIEMPO_ASCENSOR] (ver la dirección 560 en el capítulo B.1 en el Anexo B), el FW de los Terminales *Modulares* modelos DEF-3001(4) mostrará tal texto en la primera línea de la pantalla(1) tan pronto como reciba la información desde el sistema Kone (en la segunda línea de la pantalla estará visible el mensaje establecido para la situación ACCESO : PERMITIDO).
Como resumen, y una vez validada la posibilidad de paso del usuario, el funcionamiento es el siguiente (la situación de partida es la de paso bloqueado):

- con mensaje definido:
  - petición de servicio al sistema Kone;
  - la respuesta a la petición de servicio se muestra en la pantalla del Terminal (con total independencia de la posible pantalla de Kone);
  - desbloqueo del punto de paso.
- sin mensaje definido:
  - desbloqueo del punto de paso;
  - petición de servicio al sistema Kone;
  - la respuesta a la petición de servicio se muestra en la pantalla de Kone.

18.1.3

Podría darse el caso de que en una misma Instalación se utilizaran **Acreditaciones** dotadas con estructura **fS=4** para la identificación y validación de los usuarios, pero también que se utilizara para ello directamente biometría de Clase "3" en la modalidad 1:N, de manera que fueran los propios usuarios quienes decidieran si presentar su **Acreditación** o si presentar su dedo.

Los terminales modelo DEF-3001(4) (y también los Terminales modelo DEF-3002) permiten tal cosa de manera concurrente, pero hay que tener en cuenta que, normalmente, el trabajar con estructuras f**S=4** implica que los Terminales utilicen **Lista_Negra**, mientras que al trabajar con biometría implica que los Terminales utilicen **Lista_Blanca**(2), lo cual plantea un problema que debe ser resuelto (hay que recordar que un mismo Terminal no puede admitir los dos tipos de Lista).

Para operar admitiendo ambos métodos, la solución puede ser configurar tales Terminales con **Lista_Blanca** de identificación y de validación o con **Lista_Negra**, pero en este caso aceptando que cada **Acreditación** sería validada en base al contenido de la pertinente estructura **fS=4** y cada identificación por biometría sería aceptada sin validación posible (ni Horarios, ni Agenda, etc.), por lo que cierta información necesaria para la interacción con el sistema Kone (como el **tipo Usuario** para saber si se trata de un usuario VIP) se podría obtener de la estructura **fS=4** pero no cuando se utilice biometría.

La solución propuesta es la de que el programa **OEM** cargue la indicación del tipo de usuario en el Nibble de mayor peso del Byte bajo de cada elemento 'Cápsula_1' en la Lista_Otras_Prestaciones.

18.2 Parámetros

Para facilitar tanto la instalación original como posibles modificaciones posteriores, algunos de los parámetros necesarios para el funcionamiento del sistema son accesibles para el programa **OEM** mediante el uso de la función *33 Reconfigurar_capaKone*, quedando tales parámetros almacenados dentro de la estructura proporcionada por los elementos **TInGW** (existe uno en cada Terminal *Modular* del modelo DEF-3001(4)).

De todos modos, el programa de utilidad Q2_UTIL (Versión 7 y posteriores) aporta una opción para la administración de tales parámetros.

El parámetro 'CPB' (contenido en la estructura **TInGW**) debe contener el valor que indica el número relativo que corresponde a la planta baja del edificio, de manera que las equivalencias en la numeración cardinal secuencial utilizada por el sistema Kone puedan ser calculadas.

Por ejemplo, si los ascensores de un edificio pueden acceder a tres plantas subterráneas, a la planta baja y a 15 plantas elevadas, la numeración que se permite indicar a nivel de los programas (tanto para el parámetro 'Planta de origen' como para el campo 'planta_destino' en los elementos 'Capsula_1' situados en la Lista_Otras_Prestaciones) es numérica con signo (-3, -2, -1, 0, +1, ..., +15), mientras que para el sistema Kone la numeración debe ser secuencial sin signo (1 a 19 en este ejemplo), de manera que este parámetro debería indicar 4 como valor para la planta baja con lo cual, al sumarlo algebraicamente al valor numérico con signo se obtiene el correspondiente valor en el sistema Kone.

18.3 LOG para auditorias

Este LOG tiene por objetivo recoger todos los mensajes que se transmitan entre la **capa Kone** y el sistema Kone, por lo que cada Terminal involucrado[4] los graba en su EEPROM en base al flujo producido y respetando la secuencia real de envío/recepción.

Aunque los mensajes recibidos de los Servidores del sistema Kone incorporan el "momento" en el que han sido generados, y para evitar dudas en el análisis de diferenciales de tiempo entre los mensajes enviados y los recibidos, la **capa Kone** añade un campo con su propio **crono** (el diferencial entre los **cronos** de los mensajes enviados y de los correspondientes recibidos permite establecer un cálculo realista de demoras en el proceso 'petición de la *capa Kone* –> cómputo –> respuesta del sistema Kone).

Fundamentalmente se trata de una herramienta para auditoría de rendimiento (con la clara intención de evitar controversias entre fabricantes), por lo que la generación del LOG es exclusiva de la **capa Kone** mientras que su lectura puede realizarse mediante la función *20 Leer_EEPROM* o mediante el recurso expreso aportado por la Versión 7.8 (y posteriores) del programa de utilidad Q2_UTIL.

Cada registro ocupa 19 Bytes, y dada su complejidad no se publica su estructura sino que se propone que, en caso de haberse activado la generación de tal LOG[3], el contenido sea enviado a Qontinuum para su análisis.

NOTAS:

(1)

La pantalla puede ser la propia del Cabezal “en Kit” modelo DEF-KC097 o modelo DEF-KC097B o modelo DEF-KC097BO o modelo DEF-KC097BO2 conectado a un Terminal *Modular* modelo DEF-3001 o puede ser la pantalla propia de los Terminales *Compactos* de la Serie 4000[(4)].

(2)

Aunque se podría configurar un Terminal para que trabajara con **Lista_Negra** y con identificación por biometría, la fase de validación no se podría llevar a cabo dado que no existiría la información necesaria para ello, puesto que es en la **Lista_Blanca** y/o en las estructuras **fS=4** donde reside tal información.

(3)

La activación sólo puede conseguirse marcando la oportuna casilla en la opción {SAT : Control elementos IP : Configurar parámetros ‘capa Kone’} del programa de utilidad Q2_UTIL (Versión 7.8 y posteriores).

(4)

Todo el potencial de la **capa Kone** también está presente en algunos modelos de Terminales *Compactos* de la Serie 4000, los cuales utilizan una estructura **TInGW** virtual.

ESTA PÁGINA HA SIDO DEJADA EN BLANCO INTENCIONADAMENTE

código	título	relaciones
QAN-19	Generación desasistida de la estructura **fS=4** (para ISO/IEC 14443)	- MRT019 : capítulo 5 (funciones *1*, *2* y *4*) (macrofunción *129*, bit b34) - QAN-07 - BTP037

En circunstancias normales, en aquellas Instalaciones que, por sus necesidades, hayan decidido implementar el uso de **Acreditaciones** conformes con la norma ISO/IEC 14443 ('MIFARE' o 'DESFire') dotadas con formato **fS=4**, hay que seguir, para cada **Acreditación**, un proceso de generación asistida que consiste en la intervención expresa del Operador del programa **OEM** para, utilizando un Terminal *de Sobremesa* y los recursos apropiados de la API del **driver** Q2_DRV32.DLL (las macrofunciones *142 Prepersonalizar_fS=4* y *130 Grabar_fS=4*) conseguir efectuar el proceso de **Prepersonalización** y el de **Personalización (ver la Nota de Aplicación QAN-07)**.

Cuando la intención es implementar el formato f**S=4** en una Instalación que ya disponga de **Acreditaciones** 'MIFARE' o 'DESFire' que, probablemente, habían sido o son usadas en otras aplicaciones, y siendo el caso de que existan en gran cantidad y que sea muy laboriosa y compleja su recolección para poder prepararlas siguiendo los procesos (típicos en el **sistema CONACC**) de **Prepersonalización** y de **Personalización**, la generación en tales **Acreditaciones** de la estructura **fS=4** se convierte en un objetivo que sería imposible de realizar si no fuera por la alternativa de generación desasistida que ofrece la activación del bit b34 del parámetro 'IM' de la macrofunción *129 Instalar_fS=4*(1), lo cual proporciona (pero sólo a los Terminales de la Familia DEF de la Serie 3000) la capacidad de generar la estructura **fS=4** en aquellas **Acreditaciones** presentadas por los usuarios directamente en cualquier Terminal de tal Serie que haya sido parametrizado para ello.

Esta Nota de Aplicación contempla la generación desasistida de la estructura **fS=4**, de manera que los programas **OEM** que deban enfrentarse a ella puedan resolverla con éxito si tienen en cuenta ciertas condiciones, siendo la primera de ellas que los Terminales involucrados en este tipo de proceso deben estar operando en Modo: Autónomo y la segunda que debe existir y estar operativo el subsistema **VirGO**(2) si son varios los Terminales en los que se pretenda facilitar la generación desasistida y pueda existir afluencia notable de usuarios.

19.1 Funcionamiento

El FW del Terminal comprueba que en la **Acreditación** presentada exista la estructura **fS=4** y que sea válida(3); si todas las comprobaciones resultan correctas, el FW procede normalmente como en cualquier otro tipo de Instalación, mientras que si tal estructura **fS=4** no existe o existiendo no presenta integridad lógica pero está activado el bit b34 del parámetro 'IM', no se rechaza a la **Acreditación** con el típico "pirripip" sino que el FW se encarga de los pasos necesarios para generar la oportuna estructura **fS=4** en tiempo real y sin que el usuario tome conciencia de ello más que por el mayor tiempo necesario (exclusivamente en esta ocasión) para concederle el acceso.

19.1.1 paso 1

El FW comprueba la posibilidad de operar en la **Acreditación** usando las Claves de Transporte o la CMGD (Clave Maestra Generación Desasistida) para al Sector previsto en 'MIFARE' o usando la PMK ('Picc Master Key') para 'DESFire'), y si no le resulta posible operar aborta el proceso generando un **marcaje especial** con CE=08.

19.1.2 paso 2

Si el FW puede operar, coloca al Terminal en "Modo: Supervisado" (de manera efímera por el tiempo que dure el proceso) y activa el bit b14 en el mapa de bits de respuesta a la función *1 Petición_Status* que debe recibir, sistemáticamente, del programa **OEM**,

19.1.3 paso 3

El programa **OEM** analiza la respuesta del FW a cada función *1 Petición _Status* enviada, y en esta ocasión averigua por el código de estado *11 Acreditación detectada* (además de por el contenido del mapa de bits) que el FW ha iniciado un proceso de generación desasistida, por lo que el programa **OEM** deberá ejecutar de inmediato la función *2 Leer_Acreditación* con la parametrización oportuna(4) para obtener el **NUFAB** de la **Acreditación** que está siendo presentada por un usuario.

19.1.4 paso 4

El FW contesta a la función *2 Leer_Acreditación* comunicando el tipo de **Acreditación** presentada ('MIFARE' o 'DESFire') y el correspondiente **NUFAB**, por lo que el programa **OEM** debe encargarse de acceder, por el valor recibido, a su Base de Datos con la mayor rapidez posible, y de preparar toda la información(5) adecuada y de ejecutar la función *4 Grabar_Acreditación*.

19.1.5 paso 5

Al recibir el FW tal información genera la estructura **fS=4** y la graba en la **Acreditación**, por lo que ésta queda en situación de **Prepersonalizada** y de **Personalizada** (todo a la vez); como consecuencia, el FW regresa al "Modo: Autónomo", genera un **marcaje normal** con CE=05 y comienza el proceso normal que hubiera seguido de haber existido previamente la estructura f**S=4**.

19.2 Situaciones de excepción

Son aquellos casos en los que el proceso de generación desasistida resulta inviable.

19.2.1

Si el FW, antes de prepararse para informar al programa **OEM** (en respuesta a la última función *1 Petición_Status* recibida), comprueba que no resultan válidas ni las Claves de Transporte, ni la CMGD (para 'MIFARE') o la PMK (para 'DESFire'), aborta el proceso generando un **marcaje especial** con CE=08; el problema puede estar en que o la CMGD o la PMK (cargadas en **TInACC**) no es la adecuada o que el esquema de seguridad del Sector (en 'MIFARE') cuya clave se quiera transformar no permite cambiarla; todos estos problemas son, por tanto, irresolubles hasta hacer los cambios oportunos en **TInACC** o hasta comprobar que la **Acreditación** presentada no sea de las previstas, por lo que podría no resultar posible su tratamiento.

19.2.2

Si el programa **OEM** no atiende (quizá no esté funcionando) a la indicación del Terminal para reclamar que se proceda a la generación desasistida, el FW, transcurridos el tiempo declarado en el Nibble de mayor peso del parámetro 'DURACIÓN MENSOP', rechaza a la **Acreditación** con el típico "pirripip" y regresa al "Modo: Autónomo".

19.2.3

Si el programa **OEM** no encuentra en su Base de Datos el **NUFAB** recibido, debe ejecutar la función *8 Terminar_Mal* con ADDR a ceros (por lo que el Terminal rechaza a la **Acreditación** pitando tres veces) y el FW regresa al "Modo: Autónomo".

19.2.4

Si el FW no logra una grabación correcta de la estructura **fS=4** en la **Acreditación**, regresa al "Modo: Autónomo" y genera un **marcaje normal** con CE=06.

NOTAS:

(1)

La capacidad de generación desasistida de una estructura **fS=4** en **Acreditaciones** 'MIFARE' está limitada a la correspondiente al **centro operativo** 'primario', de manera que es el **driver** el que comprueba que el archivo de **datos comunes** y el archivo de **datos específico** vayan a residir en el mismo Sector, por lo que si la información contenida en **TInACC** o en **TInACC/2** no respeta tal coincidencia retorna un código de estado 19.

(2)

El recurso llamado **capa VirGO** (ver la Revisión H o posterior del documento BTP037) hace que sea el FW el que informe al Servidor **VirGO** de la situación en la que se encuentra el Terminal, y es el Servidor **VirGO** el que contesta realmente al programa **OEM** cuando éste ejecuta la función *1 Petición_Status*.

(3)

Se comprueba la validez del **CODSE** y la integridad de los archivos en base a la información que consta en la memoria reservada del Terminal (provenientes del **TInACC** o **TInACC/2**).

(4)

El FW retornará el **NUFAB** en la forma por defecto (NUID en orden LH para 'MIFARE' y CT + UID en orden LH para 'DESFire'), por lo que el programa **OEM** debe tener en cuenta que quizá tal información deba ser adaptada para hacerla coherente con la forma en la que conste grabada en la Base de Datos (posiblemente tal dato haya sido importado desde un sistema externo que ya estuviera tratando las **Acreditaciones** por su **NUFAB**, por lo que hay que adaptarse a la forma que éstos presenten).

(5)

Tal información constituye la esencia del formato **fS=4**, por lo que se trata de la misma información que se utiliza en la macrofunción *130 Grabar_fS=4* para la creación del archivo de **datos comunes** y del archivo de **datos específicos**.

ESTA PÁGINA HA SIDO DEJADA EN BLANCO INTENCIONADAMENTE

código	título	relaciones
QAN-20	Inclusión en el **sistema CONACC** de un **Panel de Intrusión** y/o de un **Panel tipo interno**	- MRT019 : capítulo 3 (*Direcciones 81-82, 83-84* y *85-86*) - MRT019 : capítulo 5 (función *28* / macrofunción *129*, código “Control PANEL") (función *28* / macrofunción *129*, código “Control LOP") - MRT019 : capítulo 6 (Nota de Aplicación QAN-02) - MRT019 : Anexos D y F - BTP027 (Revisión W y >>): capítulo 2.14

Esta Nota de Aplicación tiene como objetivo clarificar las peculiaridades de los **Paneles de Intrusión** de Qontinuum y/o de aquellos Terminales de Qontinuum que disponen de la capacidad de actuar como **Panel tipo interno**, así como facilitar información a los programadores **OEM** para ayudarles a integrar tales equipos en sus aplicaciones. Esta capacidad sólo es aplicable a los **Paneles de Intrusión** modelo DEF-3003[(1)] y modelo DEF-3003/L[(1)] (FW de Versión 10.0 y posterior) y a los Terminales *Modulares* modelo DEF-3001[(1)] (FW de Versión 9.0 y posterior), pudiendo actuar como *Control de Accesos* físicos y/o ‘Zona llave’ virtual por **Acreditación**, siendo una condición imperiosa para su uso el que no se requiera de conectividad a una receptora pública dado que no se utilizan protocolos estándar de mercado (como “CONTACT ID” o “SIA 2000").

La modalidad de actuación como **Panel tipo interno** se diferencia de la de **Panel de Alarmas externo** y del **Panel tipo mixto** en que aquella incorpora las prestaciones de éstas y añade la prestación de “armar” / “desarmar” hasta a ocho Particiones en ‘operativa local’, así como la prestación para controlar a más de un punto de acceso, en ambos casos al actuar como una única “consola”[(2)] (el propio Terminal). Para ambas prestaciones añadidas, las diferentes acciones se ejecutan de manera individual, siendo para el "armado" / "desarmado" no concurrentes, es decir, que no se podrá "armar" o "desarmar" ninguna Partición hasta que la última operativa de "armado" o "desarmado" hay concluido. De todos modos, los programas **OEM** deberán implementar la función FU=72 (para poder definir el resto de parámetros del Panel) y la función FU=71 (para interactuar con él), así como gestionar el **marcaje normal** con CE=79 y los **marcajes Panel** (CE=113).

En los **Paneles de Intrusión** modelo DEF-3003 y modelo DEF-3003/L y en los Terminales *Modulares* modelo DEF-3001, la actuación como **Panel tipo interno** se activa mediante la opción 2: **Panel tipo interno** en el código "Control Panel" del parámetro ‘IM’ de la función *28 Instalar_Terminal* o la macrofunción *129 Instalar_fS=4*. Con ella se permite que una o varias Entradas (cada Entrada corresponde, normalmente, a un sensor) conjuntamente con una o varias Salidas (cada Salida corresponde a un relé) sean vinculados en agrupaciones de Entradas y Salidas, agrupaciones a las que se denomina Particiones.

En los **Paneles de Intrusión** modelo DEF-3003 y modelo DEF-3003/L es posible la conexión de un lector de elementos **TInKey**, de manera que se facilite el “predesarmado” en aquellas Instalaciones que pudieran requerirlo (ver la Revisión D y posteriores del documento BTP040).

Panel / Terminal modelo :	Particiones disponibles	Particiones que admiten 'operativa local' :	
		siempre	sólo usando la prestación "SxT"
DEF-3003	12	#1	#1 a #8
DEF-3003/L	4	#1	-
DEF-3001	8	#1	#1 a #8

Las Particiones pueden ser de dos tipos:

- de 'operativa local' : son las que pueden interrumpir temporalmente el control de sus Entradas para permitir el acceso de personal autorizado, dentro de su área de supervisión, sin generar alarma aún cuando detecte actividad en sus Entradas; para ello deben permitir ser "desarmadas", y posteriormente "armadas", mediante una 'operativa local', siendo posible definir una serie de tiempos para que el usuario pueda realizar tales operativas sin causar alarmas (un ejemplo de Partición de 'operativa local' seria la que controla Entradas tales como el contacto magnético de la puerta de acceso, un volumétrico en el área de paso, etc.).
- de '24H'' : son las que controlan sus Entradas de manera continua; pueden generar alarma, por actividad en sus Entradas, a cualquier hora del día (por ejemplo, las Particiones con Entradas detectoras de incendio, pulsadores de emergencia, etc.).

Todas las Particiones pueden ser "armadas" (generan alarma cuando detectan una Entrada activa) o "desarmadas" (no generan alarma) vía comunicaciones, pero sólo en las Particiones de 'operativa local' puede realizarse el "armado" / "desarmado" por otros medios (como el uso de **Acreditaciones** en un Cabezal de lectura-escritura).

La 'operativa local' puede realizarse por dos vías: interactuando con la "consola"(2) ('Zona llave virtual') o a través de una Entrada declarada como 'Zona llave'; el propio FW también podrá, de manera automática, "re-armar" una Partición que haya sido "desarmada", pasado un tiempo determinado de inactividad en sus Entradas. Si se utiliza la "consola"(2) como 'Zona llave virtual', es posible que se requiera presentar (en el Cabezal lector-grabador) una **Acreditación** que supere todas las validaciones del sistema: formato correcto, **Lista_Blanca** o **Lista_Negra**, horario, etc. Si se utiliza una Entrada declarada como 'Zona llave', ésta puede configurarse para ser activada por pulso (sólo permite "armar") o por nivel (permite "armar" y "desarmar") desde un pulsador, un contacto de llave, un sistema externo, etc. Además de los **marcajes Panel** con CE=113 que son pertinentes para indicar cada una de las acciones en el Panel, cuando éstas sean causa de la presentación de una **Acreditación**, se generará previamente un **marcaje normal** con CE=79 para registrar el **NIS** implicado. Si el usuario indica situación de **coacción**, se genera un **marcaje normal** con CE=88.

NOTAS:
(1)
Para los **Paneles de Intrusión** modelo DEF-3003 y modelo DEF-3003/L (a partir del FW de Versión 10.0) y para los Terminales *Modulares* modelo DEF-3001 (a partir del FW de Versión 9.5) existe compatibilidad funcional con los Terminales *Especiales* modelos DEF-PCTn (ver el Anexo H del documento MRT019).

(2)
El concepto "consola" hace referencia a la combinación de una pantalla y un teclado con un elemento lector o lector-grabador de **Acreditaciones**, de manera que los usuarios pueden seleccionar opciones para el control del **Panel tipo interno** y/o puedan anotar un **PIN**.
Pueden actuar como "consolas":

- los **Paneles de Intrusión** modelo DEF-3003 y los Terminales *Modulares* modelo DEF-3001 cuando se les conecta un Cabezal "en Kit" modelo DEF-KC097 o modelo DEF-KC097B (complementados con un teclado).

No pueden actuar como "consolas":

- los **Paneles de Intrusión** modelo DEF-3003/L.

Para que la "consola" resulte operativa debe habilitarse la prestación "SxT" en el código "Control LOP".

20.1 Características de las Entradas, Particiones y Salidas

Todas las Entradas pueden programarse para que sean de efecto inmediato o temporizado con tiempos individualizados. A las que son temporizadas también se les pueden indicar el tipo de activación para que la Entrada, para ser efectiva, tenga que estar activa (por nivel) o no estarlo (por pulso) durante todo el tiempo de temporización. Este último caso es especialmente útil, en la Partición de 'operativa local', para Entradas con una posible activación de corta duración, como, por ejemplo, una barrera de rayos infrarrojos; aunque ello implica tener que definir un tiempo 'Td' suficientemente grande para poder salir del recinto sin generar alarma al "Armar" la Partición en modo local.

Cada Entrada temporizada puede asociarse a un Horario (parámetro 'TABLA_GRUPOS') distinto para alterar, mediante un factor multiplicador, el tiempo de temporización según un horario (parámetro 'TABLA_HORARIOS') de una o dos franjas para cada día de la semana (alterable temporalmente según el parámetro 'TABLA_AGENDA'); tal factor también puede ser 0, en cuyo caso la Entrada queda anulada durante esos períodos.

Las temporizaciones también permiten dar tiempo al usuario para que éste realice un "desarmado" local cuando el Cabezal lector-grabador esté dentro del área de supervisión de las Entradas implicadas.

Cada Entrada se asocia a una Partición (de 1 a 12) y a cada Partición se le asigna una o varias Salidas a ser activadas en caso de alarma. La relación puede ser directa (alarma activada hasta que se restablece el estado de la Entrada causante), o de enclavamiento (alarma activada, aún cuando el estado de la Entrada causante se restablezca, hasta que se desactive presentando una **Acreditación** válida o vía comunicaciones). Independientemente de si la relación es directa como si es de enclavamiento, es posible definir, de manera individual, un tiempo mínimo de activación por alarma para cada Salida (excepto para la Salida R1). Es recomendable definir como enclavables las Particiones con Entradas temporizadas activadas por pulso.

Cada Partición de 'operativa local' puede ser programada para actuar en combinación con las prestaciones de tales Terminales para el *Control de Accesos*. En tal caso, la Salida N quedará vinculada a la Partición N (N = 1 a 12), quedando reservada para la activación de la cerradura dispuesta para controlar el acceso, pudiendo tal control ser complementado asociando a la Partición N una Entrada que actúe como sensor de situación de puerta.

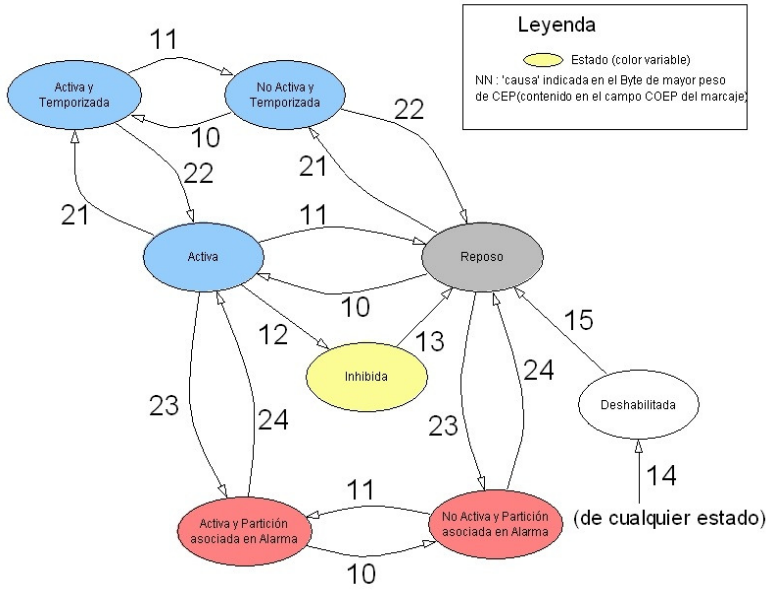
Para cada Partición se puede definir una Salida (R2..S15) en el campo 'Sad' del registro pertinente en la 'TABLA PARTICIONES' (ver en el Anexo D.2.1 del documento MRT019) para indicar "armado" (desactivada) o "desarmado" (activada) que puede ser utilizada para una señalización de la Partición de 'operativa local'. Los LED propios del Cabezal lector-grabador también pueden usarse para dicha señalización si se activa el bit b3 del parámetro 'MÁSCARA MISCELÁNEA 4'. En tal caso, el LED rojo indica que hay una o más Particiones de 'operativa local' en estado "armado" mientras que el LED verde indica que hay una o más Particiones de 'operativa local' en estado "desarmado" (en los Cabezales con un único LED bicolor, cuando se activen ambos colores se verá de color naranja).

Aún trabajando como **Panel tipo interno** es posible forzar que una o más Particiones de 'operativa local' interaccionen con un **Panel de Alarmas externo** activando el bit b32 = 1 en el registro pertinente en la 'TABLA PARTICIONES' (ver en el Anexo D.2.1 del documento MRT019), para lo cual la definición del campo 'Sad' en dicha 'TABLA PARTICIONES' tiene especial relevancia; además, la asociación a tal Partición de una 'Zona llave' definida en TABLA ENTRADAS (ver en el Anexo D.3.1 del documento MRT019) implica el uso de ésta como señal 'Ead' tal y como se hace en el subparámetro 'Ead'' del parámetro 'INTERACCIÓN_PANEL' (ver la Nota de Aplicación QAN-16).

El número de Entradas y Salidas disponibles dependerá del número de módulos de E/S que se usen:

módulo de E/S :	no se usa módulo	con un módulo	con dos módulos
Configuración 'IM' (bit b15, b16 y b17) :	5	6	7
Salidas :	**8** (R1,R2,S3..S8)	**12** (R1,R2,S3..S12)	**16** (R1,R2,S3..S16)
Entradas :	**8** (E1,E2,E5,E6, E9..E12)	**12** (E1,E2,E5,E6, E9..E16)	**16** (E1,E2,E5,E6, E9..E20)
Entradas (virtuales) :	**1** (E4)	**2** (E4 y E8)	**2** (E4 y E8)
	E4 : **"tamper"** en Cabezal: no hay comunicación con el Cabezal E8 : 'error de Bus interno' (comunicaciones) con el/los módulo(s) de E/S		

Para los marcajes relacionados con las Entradas y los posibles estados de éstas se puede seguir el siguiente diagrama:



Los colores de los estados son los utilizados por el programa de aplicación WinAcces y, por tanto, son sólo orientativos. Dado que el FW sólo puede grabar un código de 'causa' en cada marcaje, para indicar que una Entrada pasa de un estado a otro pueden ser necesarios dos marcajes (con una separación entre ellos de hasta 1 segundo).

A continuación se explican los estados indicados en el diagrama anterior:

Activa: el estado físico de la Entrada más la máscara NO/NC indica “Entrada activa” y no ha iniciado su temporizador. Este estado es transitivo(1), y sólo puede ser permanente(1) si la Partición a la que está vinculada la Entrada está “desarmada” o “intentado armar”.

Activa y Temporizada: el estado físico de la Entrada más la máscara NO/NC indica “Entrada activa” y ha iniciado su temporizador. Este estado sólo se puede dar si la Partición a la que está vinculada la Entrada está “armada”.

No Activa y Temporizada: la Entrada ha iniciado su temporizador y físicamente está en reposo. Este estado sólo se puede dar si la Entrada ha sido configurada por pulso y la Partición a la que está asignada está “armada”.

Activa y en Alarma: la Entrada ha agotado su temporizador (si el temporizador es 0 se pasa directamente a este estado sin pasar antes por el estado de Temporizada). Indica que esta Entrada ha hecho que la Partición a la que está asignada pase a estado de alarma. Este estado sólo se puede dar si la Partición está “armada”. También indica que la Entrada está físicamente activa.

No Activa y en Alarma: la Entrada ha agotado su temporizador (si el temporizador es 0 se pasa directamente a este estado sin pasar antes por el estado de Temporizada). Indica que esta Entrada ha hecho que la Partición a la que está vinculada pase a estado de alarma. Este estado sólo se puede dar si la Partición está “armada”. Este estado será transitivo(1) si la Entrada está configurada por pulso. También indica que la Entrada está físicamente en reposo.

Reposo: la Entrada está en reposo, lo que quiere decir que no está Activa ni Temporizada ni en Alarma. Físicamente está en reposo.

Inhibida: el FW ha inhibido la Entrada para poder armar. El FW ignorará el estado de esta Entrada, por lo tanto tal Entrada no hará que la Partición pase a estado de alarma. Indica que la Entrada está físicamente activa. Cuando la Entrada cambie y esté físicamente en reposo se pasará a estado “Reposo”.

Deshabilitada: la Entrada ha sido deshabilitada a través de comunicaciones. La Entrada sólo puede habilitarse a través de comunicaciones. El FW ignorará el estado de la Entrada, por lo tanto tal Entrada no hará que la Partición pase a estado de alarma. Además, el FW no generará ningún marcaje para indicar el estado físico de la Entrada, por lo tanto el estado físico de la Entrada es desconocido.

NOTAS:
(1)
Se considera estado transitivo el estado intermedio que el FW usa para pasar de un estado a otro, y estado permanente el estado en el que la Entrada puede permanecer durante más de un segundo.

20.2 Operativas

20.2.1 "desarmado"

La operativa de "desarmado" siempre será de ejecución inmediata sea cual sea la Partición o el medio de actuación, con una excepción(1).

20.2.1.1 Peculiaridades de la 'operativa local' usando la "consola"

El hecho de disponer de "consola" implica que se pretende utilizar la prestación "SxT"(2):

- El usuario debe seleccionar una Incidencia de las declaradas con parámetro 'AR' = FDh, FCh(3) o FBh(3), pulsar la tecla Intro y presentar su **Acreditación**(7) y cumplimentar el **IDEP** (**PIN** o biometría) si tal Incidencia "SxT" lo requiere.
- Si la incidencia anotada tiene un código AR = 0xFF (situación de coacción) genera un **marcaje normal** con CE=88 (si se ha usado una **Acreditación**) o un **marcaje especial** con CE=88.
- Si el **NIS** de la **Acreditación** presentada existe en la Lista_Otras_Prestaciones (ver el capítulo 3 en el documento MRT019) se comprueba los permisos disponibles, mientras que si no existe o no dispone del permiso pertinente se aborta la operativa con un **marcaje Panel** con **COEP** (CEP) = 2100h apareciendo en pantalla el mensaje declarado para la situación de ACCESO : DENEGADO (ver en el Anexo B del documento MRT019).
- Si se superan las validaciones el FW genera un **marcaje normal** con CE=79 (si se ha usado una **Acreditación**) seguido por ...
  - ... un **marcaje Panel** con **COEP** (CEP) = 0601h a 0608h:
    - se indica con un pitido y con el mensaje declarado para la situación de OPERATIVA : CORRECTA (ver en el Anexo B del documento MRT019) o para la situación de ACCESO : PERMITIDO (ver en el Anexo B del documento MRT019) si se concede el acceso (sólo con el parámetro 'AR' = FCh o FBh), con lo que también se genera un **marcaje Panel** con **COEP** (CEP) = 2001h a 2008h y se activa la Salida pertinente.
  - ... excepcionalmente(1), un **marcaje Panel** con **COEP** (CEP) = 1E01h a 1E08h (sólo si el parámetro 'AR' = FDh):
    - se indica con el mensaje 'Intentando Desarmar' (ver en el Anexo D.4.1 del documento MRT019) y un destello del LED verde cada 2 segundos hasta completar la operación, en cuyo caso se indica con un pitido y con el mensaje declarado para la situación de OPERATIVA : CORRECTA (ver en el Anexo B del documento MRT019), además de generar un **marcaje Panel** con **COEP** (CEP) = 0601h a 0608h, mientras que si la operación no se completa porque se agota el tiempo definido en el campo 'Td' (ver en el Anexo D.2.1 del documento MRT019) se indica con tres pitidos y reaparece el mensaje que indica la situación real de la Partición además de generar un **marcaje Panel** con **COEP** (CEP) = 1F01h a 1F08h.
- Finalmente, y al quedar el Terminal en estado de reposo, si el bit b2 del parámetro 'CONTROL MISCELÁNEA DEL PANEL' (ver en el Anexo D.1.2 del documento MRT019) está activado en la 2ª línea de la pantalla aparece el mensaje pertinente a la situación.

20.2.1.2 Peculiaridades de la 'operativa local' usando un Cabezal lector-grabador

En tal situación no se puede utilizar la prestación "SxT" y sólo la Partición #1 puede ser de 'operativa local':

- La **Acreditación** válida debe presentarse sólo durante el tiempo mínimo para la lectura y (sólo en formato **fS=4**) su posible grabación; al hacerlo se oye un pitido y se apaga momentáneamente el LED rojo para indicarlo, debiendo ser retirada antes de que se supere el tiempo definido en el campo 'Tp' del parámetro 'CONTROL MISCELÁNEA DEL PANEL' (ver en el Anexo D.1.2 del documento MRT019)
- Es posible indicar al Panel que, una vez "desarmado", facilite el acceso activando la Salida R1 si se ha definido un tiempo superior a 0 para esta Salida. Para ello, el Cabezal lector-grabador debería ser instalado en la parte exterior del área controlada por la Partición, y la Salida R1 debería ser conectada a la cerradura eléctrica de la puerta de acceso. En este caso, y estando "desarmada" la Partición, cualquier presentación (durante un tiempo < 'Tp') de una **Acreditación** válida seguirá el tratamiento normal dado a los intentos de acceso, por lo que, si resulta correcto, el FW generará un **marcaje normal** con CE=34.
- Si el bit b6 del parámetro 'MÁSCARA MISCELÁNEA 4' está activado y se presenta una **Acreditación** cuando la Partición (declarada de 'operativa local') esté "armada", aquella será rechazada con un **marcaje normal** con CE=87 excepto que tal **Acreditación** esté declarada en la Lista_Especial, en cuyo caso el FW "desarmará" la Partición de 'operativa local'.

20.2.2 "armado"

La operativa de "armado" para las Particiones de '24H' siempre será de ejecución inmediata.

Para las Particiones de 'operativa local' dependerá del medio de actuación (el "re-armado", por ejemplo, siempre será inmediato con una excepción[4]) o dependerá de la parametrización. A excepción de los casos mencionados, cuya respuesta es inmediata, para el resto de casos el **Panel tipo interno** sólo considerará la Partición "armada" si todas sus Entradas vinculadas están en reposo antes de transcurrir el tiempo definido en el campo 'Ta' para tal Partición (ver en el Anexo D.2.1 del documento MRT019).

De todas las Entradas de la Partición se puede indicar cuales deben estar inactivas para permitir al Panel "armar", y, de entre tal grupo, a cuales se les permite eximirse de dicha responsabilidad si pasado el tiempo 'Ta' existen otras Entradas operativas de la Partición que sí estén en situación de inactividad, exceptuando las que no tengan la obligación de estarlo. Si es así, el Panel las inhibe temporalmente hasta que se restablezca su estado de reposo o hasta que se inicie otro intento de "armado" (excepto en el re-armado" automático).

Para la 'operativa local' (no aplicable vía comunicaciones ni a Particiones que tengan activada la interacción con un **Panel de Alarmas externo**) también es posible definir en el campo 'Td' pertinente (ver en el Anexo D.2.1 del documento MRT019) un tiempo previo y fijo de demora para que el Panel, una vez recibida la orden, espere a intentar "armar" tal Partición y así dar tiempo al personal para salir del recinto controlado.

Cuando 'Ta' y 'Td' (si la Partición no tiene activada la interacción con un **Panel de Alarmas externo**) se definan con valor 0, la respuesta también será inmediata, en caso contrario ambas esperas serán indicadas por el Panel con un pitido y un destello del LED rojo cada 2 segundos.

20.2.2.1 Peculiaridades de la 'operativa local' usando la "consola"

El hecho de disponer de "consola" implica que se pretende utilizar la prestación "SxT"[2]:

- El usuario debe seleccionar una Incidencia con el parámetro 'AR' = FEh y presentar su **Acreditación** y cumplimentar el **IDEP** (**PIN** o biometría) si tal Incidencia "SxT" lo requiere.
- Si la incidencia anotada tiene un código AR = 0xFF (situación de coacción) genera un **marcaje normal** con CE=88 (si se ha usado una **Acreditación**) o un **marcaje especial** con CE=88.
- Si el **NIS** de la **Acreditación** presentada existe en la Lista_Otras_Prestaciones se comprueba los permisos disponibles, mientras que si no existe o no dispone del permiso pertinente se aborta la operativa con un **marcaje normal** con CE=79 seguido de un **marcaje Panel** con **COEP** (CEP) = 2100h apareciendo en pantalla el mensaje declarado para la situación de ACCESO : DENEGADO (ver en el Anexo B del documento MRT019).
- Si se superan las validaciones el FW genera un **marcaje normal** con CE=79 (si se ha usado una **Acreditación**) seguido por ...

... si el campo 'Ta' = 0 (ver en el Anexo D.2.1 del documento MRT019) un **marcaje Panel** con **COEP** (CEP) = 0501h a 0508h:

se indica con un pitido y con el mensaje declarado para la situación de OPERATIVA : CORRECTA (ver en el Anexo B del documento MRT019).

... si el campo 'Ta' > 0 (ver en el Anexo D.2.1 del documento MRT019) un **marcaje Panel** con **COEP** (CEP) = 0301h a 0308h:

se indica con el mensaje 'Intentando Armar' (ver en el Anexo D.4.1 del documento MRT019) y un destello del LED rojo cada 2 segundos hasta completar la operación, en cuyo caso se indica con seis pitidos y con el mensaje declarado para la situación de OPERATIVA : CORRECTA (ver en el Anexo B del documento MRT019), además de generar un **marcaje Panel** con **COEP** (CEP) = 0501h a 0508h, mientras que si la operación no se completa porque se agota el tiempo definido en el campo 'Ta' (ver en el Anexo D.2.1 del documento MRT019) se indica con tres pitidos y reaparece el mensaje que indica la situación real de la Partición además de generar un **marcaje Panel** con **COEP** (CEP) = 0401h a 0408h.

- Finalmente, y al quedar el Terminal en estado de reposo, si el bit b2 del parámetro 'CONTROL MISCELÁNEA DEL PANEL' (ver en el Anexo D.1.2 del documento MRT019) está activado en la 2ª línea de la pantalla aparece el mensaje pertinente a la situación.

20.2.2.2 Peculiaridades de la 'operativa local' usando un Cabezal lector-grabador

En tal situación no se puede utilizar la prestación "SxT":

- La **Acreditación** válida debe presentarse el tiempo mínimo para la lectura y, sólo para el formato **fS=4**, su posible grabación (se oye un pitido y se apaga durante un segundo el LED rojo para indicarlo) más el tiempo definido en el subparámetro 'Tp' del parámetro 'CONTROL MISCELÁNEA DEL PANEL' (ver en el Anexo D.1.2 del documento MRT019), de manera que el LED rojo vuelve a apagase cuando ha transcurrido dicho tiempo antes de que la **Acreditación** deba ser retirada.

20.2.3 Marcajes normales de Control de Presencia

Existen varias diferencias de comportamiento si el Terminal ha sido instalado indicando o no el uso de la prestación "SxT".

Sólo se generan **marcajes normales** de Control de Presencia cuando se selecciona una Incidencia CP.

Un Terminal instalado sin el uso de la prestación "SxT" genera un **marcaje normal** de Control de Presencia en cada acceso correcto.

Nunca se generan **marcajes normales** de Control de Presencia sin Incidencia.

Al hacer un marcaje con Incidencia CP:

- el FW no concede acceso (por lo cual no genera ningún **marcaje normal** de Control de Accesos) pero genera el **marcaje normal** de Control de Presencia;
- el FW ignora el valor del parámetro 'TRATAMIENTO IDEP' y no pedirá al Usuario que se autentique;
- al realizar un marcaje correcto, el FW muestra por pantalla el mensaje declarado para la situación de OPERATIVA : CORRECTA en vez del declarado para la situación de ACCESO : PERMITIDO (ver en el Anexo B del documento MRT019).

20.2.4 Resumen

En los siguientes dos cuadros se resumen las diferentes posibilidades de “armar” y “desarmar” los tres tipos de Particiones:

<table>
<tr><td rowspan="3">Partición ...</td><td rowspan="3">por medio de ...</td><td colspan="4">efecto ...</td></tr>
<tr><td colspan="2">‘Ta’ = 0</td><td colspan="2">‘Ta’ > 0</td></tr>
<tr><td>‘Td’ = 0</td><td>‘Td’ > 0</td><td>‘Td’ = 0</td><td>‘Td’ > 0</td></tr>
<tr><td colspan="6">“desarmado”</td></tr>
<tr><td>... de ‘24H’</td><td>... comunicación</td><td colspan="4" rowspan="4">... inmediato</td></tr>
<tr><td rowspan="3">... de ‘operativa local’</td><td>... comunicación</td></tr>
<tr><td>... “consola”</td></tr>
<tr><td>... Entrada (por nivel)</td></tr>
<tr><td rowspan="3">... de ‘operativa local’ (interacción con un Panel de Alarmas externo</td><td>... comunicación</td><td rowspan="3">Inmediato</td><td rowspan="3">Esperar OK (máx. ‘Td’) del Panel en ‘Ead’</td><td rowspan="3">Inmediato</td><td rowspan="3">Esperar OK (máx. ‘Td’) del Panel en ‘Ead’</td></tr>
<tr><td>... “consola”</td></tr>
<tr><td>... Entrada (por nivel)</td></tr>
</table>

<table>
<tr><td rowspan="3">Partición ...</td><td rowspan="3">por medio de ...</td><td colspan="4">efecto ...</td></tr>
<tr><td colspan="2">‘Ta’ = 0</td><td colspan="2">‘Ta’ > 0</td></tr>
<tr><td>‘Td’ = 0</td><td>‘Td’ > 0</td><td>‘Td’ = 0</td><td>‘Td’ > 0</td></tr>
<tr><td colspan="6">“armado”</td></tr>
<tr><td>... de ‘24H’</td><td>... comunicación</td><td colspan="4">... inmediato</td></tr>
<tr><td rowspan="4">... de ‘operativa local’</td><td>... comunicación</td><td colspan="2">Inmediato</td><td colspan="2">Espera (máx. ‘Ta’) Entradas en reposo</td></tr>
<tr><td>... “consola”</td><td rowspan="2">Inmediato</td><td rowspan="2">Espera fija (‘Td’)</td><td rowspan="2">Espera (máx. ‘Ta’) Entradas en reposo</td><td rowspan="2">Espera fija (‘Td’) + Espera (máx. ‘Ta’) Entradas en reposo</td></tr>
<tr><td>... Entrada (por pulso o por nivel)</td></tr>
<tr><td>... “re-armado”</td><td colspan="4">... inmediato</td></tr>
<tr><td rowspan="4">... de ‘operativa local’ (interacción con un Panel de Alarmas externo</td><td>... comunicación</td><td colspan="2" rowspan="4">Inmediato</td><td colspan="2" rowspan="4">Espera (máx. ‘Ta’) OK del Panel en ‘Ead’</td></tr>
<tr><td>... “consola”</td></tr>
<tr><td>... Entrada (por pulso o por nivel)</td></tr>
<tr><td>... “re-armado”</td></tr>
</table>

En los siguientes cuadros se resumen los marcajes relacionados con la operativa de “armar” o “desarmar” una Partición de ‘operativa local’, donde entre paréntesis aparece el valor abstracto de **COEP** (ver el Anexo F del documento MRT019), estando sus 4 campos: “origen/destino, causa, causante y tipo causante” separados por una coma):

Nomenclatura utilizada en los siguientes cuadros (ver también el Anexo D del documento MRT019):	
I =	parámetros de la Incidencia “SxT” (ver el subcampo ‘AR’ en el capítulo D.7.1 del Anexo D del documento MRT019).
LA =	Latencia “armado” (implica ‘Ta’ + ‘Td’ o sólo ‘Ta’ en Particiones que operen en interacción con un **Panel de Alarmas externo**).
Op =	Operador (la identificación).
P =	Partición (queda substituido por el número correspondiente).
E =	Entrada (queda substituido por el número correspondiente).

OPERATIVAS	SECUENCIA DE MARCAJES
Operativas por automatismo :	
“re-armado”	**marcaje Panel** con **COEP** = (P, 5, 0, 0)

OPERATIVAS	SECUENCIA DE MARCAJES
Sin prestación “SxT” : Operativas por **Acreditación** :	
Condición: Partición de ‘operativa local’ “armada”	
“desarmado”	**marcaje normal** con CE=79 + **marcaje Panel** con **COEP** = (P, 6, 0, 1) + [**marcaje normal** con CE=34](*)
intento “armado” ignorado	**marcaje normal** con CE=79
“desarmado” correcto (Partición en interacción con **Panel de Alarmas externo** y ‘Td’ > 0)	**marcaje normal** con CE=79 + **marcaje Panel** con **COEP** = (P, 30, 0, 1) ... **marcaje Panel** con **COEP** = (P, 6, 0, 1)
“desarmado” fallido (Partición en interacción con **Panel de Alarmas externo** y ‘Td’ > 0)	**marcaje normal** con CE=79 + **marcaje Panel** con **COEP** = (P, 30, 0, 1) ... **marcaje Panel** con **COEP** = (P, 31, 0, 1)
Condición: Partición de ‘operativa local’ “desarmada”	
Acceso/desactivar alarma	**marcaje normal** con CE=79 + [**marcaje Panel** con **COEP** = (P, 8, 0, 1)](**) + [**marcaje normal** con CE=34](*)
“armado” (LA = 0)	**marcaje normal** con CE=79 + **marcaje Panel** con **COEP** = (P, 5, 0, 1)
“armado” correcto (LA > 0)	**marcaje normal** con CE=79 + **marcaje Panel** con **COEP** = (P, 3, 0, 1) ... **marcaje Panel** con **COEP** = (P, 5, 0, 1)
“armado” fallido (LA > 0)	**marcaje normal** con CE=79 + **marcaje Panel** con **COEP** = (P, 3, 0, 1) ... **marcaje Panel** con **COEP** = (P, 4, 0, 1)
Operativa local rechazada por intento de “armado” en curso	**marcaje normal** con CE=79 + **marcaje Panel** con **COEP** = (P, 20, 0, 1)
(*) Sólo cuando haya acceso (tiempo Salida Rn > 0). (**) Sólo cuando esté activa una alarma desactivable.	

OPERATIVAS	SECUENCIA DE MARCAJES
Con prestación “SxT” : Operativas por “consola” (teclado + **Acreditación**) :	
Condición: Partición de ‘operativa local’ “armada”	
“desarmado”	**marcaje normal** con CE=79 + **marcaje Panel** con **COEP** = (P, 6, I, 1) + [**marcaje Panel** con **COEP** = (P, 32, I, 1)](*)
intento “armado” ignorado	**marcaje normal** con CE=79 + **marcaje Panel** con **COEP** = (P, 20, I, 1)
“desarmado” correcto (Partición en interacción con **Panel de Alarmas externo** y ‘Td’ > 0)	**marcaje normal** con CE=79 + **marcaje Panel** con **COEP** = (P, 30, I, 1) ... **marcaje Panel** con **COEP** = (P, 6, I, 1)
“desarmado” fallido (Partición en interacción con **Panel de Alarmas externo** y ‘Td’ > 0)	**marcaje normal** con CE=79 + **marcaje Panel** con **COEP** = (P, 30, I, 1) ... **marcaje Panel** con **COEP** = (P, 31, I, 1)
Condición: Partición de ‘operativa local’ “desarmada”	
Acceso/desactivar alarma	**marcaje normal** con CE=79 + [**marcaje Panel** con **COEP** = (P, 8, I, 1)]Ç(**) ... [**marcaje Panel** con **COEP** = (P, 32, I, 1)](*)
“armado” (LA = 0)	**marcaje normal** con CE=79 + **marcaje Panel** con **COEP** = (P, 5, I, 1)
“armado” correcto (LA > 0)	**marcaje normal** con CE=79 + **marcaje Panel** con **COEP** = (P, 3, I, 1) ... **marcaje Panel** con **COEP** = (P, 5, I, 1)
“armado” fallido (LA > 0)	**marcaje normal** con CE=79 + **marcaje Panel** con **COEP** = (P, 3, I, 1) ... **marcaje Panel** con **COEP** = (P, 4, I, 1)
Operativa local rechazada por intento de “armado” en curso	**marcaje normal** con CE=79 + **marcaje Panel** con **COEP** = (P, 20, I, 1)
(*) Sólo cuando haya acceso (tiempo Salida Rn > 0). (**) Sólo cuando esté activa una alarma desactivable.	

OPERATIVAS	SECUENCIA DE MARCAJES
Operativas por “consola” (sólo teclado) :	
Condición: Partición de ‘operativa local’ “armada”	
“desarmado”	**marcaje Panel** con **COEP** = (P, 6, I, 4) + [**marcaje Panel** con **COEP** = (P, 32, I, 4)](*)
intento “armado” ignorado	**marcaje normal** con CE=79 + **marcaje Panel** con **COEP** = (P, 20, I, 4)
“desarmado” correcto (Partición en interacción con **Panel de Alarmas externo** y ‘Td’ > 0)	**marcaje Panel** con **COEP** = (P, 30, I, 4) ... **marcaje Panel** con **COEP** = (P, 6, I, 4)
“desarmado” fallido (Partición en interacción con **Panel de Alarmas externo** y ‘Td’ > 0)	**marcaje Panel** con **COEP** = (P, 30, I, 4) ... **marcaje Panel** con **COEP** = (P, 31, I, 4)
Condición: Partición de ‘operativa local’ “desarmada”	
Acceso/desactivar alarma	[**marcaje Panel** con **COEP** = (P, 8, I, 4)](**) + [**marcaje Panel** con **COEP** = (P, 32, I, 4)](*)
“armado” (LA = 0)	**marcaje Panel** con **COEP** = (P, 5, I, 4)
“armado” correcto (LA > 0)	**marcaje Panel** con **COEP** = (P, 3, I, 4) ... **marcaje Panel** con **COEP** = (P, 5, I, 4)
“armado” fallido (LA > 0)	**marcaje Panel** con **COEP** = (P, 3, I, 4) ... **marcaje Panel** con **COEP** = (P, 4, I, 4)
Operativa local rechazada por intento de “armado” en curso	**marcaje Panel** con **COEP** = (P, 20, I, 4)
(*) Sólo cuando haya acceso (tiempo Salida Rn > 0). (**) Sólo cuando esté activa una alarma desactivable.	

OPERATIVAS	SECUENCIA DE MARCAJES
Operativas por 'Zona llave' :	
"desarmado"	**marcaje Panel** con **COEP** = (P, 6, E, 2)
"armado" (LA = 0)[5]	**marcaje Panel** con **COEP** = (P, 5, E, 2)
"armado" correcto (LA > 0)[5]	CE=113 (P, 3, E, 2) ... CE=113 (P, 5, E, 2) **marcaje Panel** con **COEP** = (P, 3, E, 2) ... **marcaje Panel** con **COEP** = (P, 5, E, 2)
"armado" fallido (LA > 0)[5]	**marcaje Panel** con **COEP** = (P, 3, E, 2) ... **marcaje Panel** con **COEP** = (P, 4, E, 2)
Operativa local rechazada por intento de "armado" en curso	**marcaje Panel** con **COEP** = (P, 20, E, 2)

OPERATIVAS	SECUENCIA DE MARCAJES
Operativas por comunicación :	
"desarmado"	**marcaje Panel** con **COEP** = (P, 6, Op, 3)
"armado" (LA = 0)[6]	**marcaje Panel** con **COEP** = (P, 5, Op, 3)
"armado" correcto (LA > 0)[6]	**marcaje Panel** con **COEP** = (P, 3, Op, 3) ... **marcaje Panel** con **COEP** = (P, 5, Op, 3)
"armado" fallido (LA > 0)[6]	**marcaje Panel** con **COEP** = (P, 3, Op, 3) ... **marcaje Panel** con **COEP** = (P, 4, Op, 3)

NOTAS:

(1)
La excepción se produce cuando una Partición de 'operativa local' tiene activado el uso como **Panel de Alarmas externo** y el campo 'Td' (ver en el Anexo D.2.1 del documento MRT019) es mayor que 0.

(2)
El Terminal debe haber sido preconfigurado (desde Q2_UTIL o desde el propio programa **OEM**) indicando el valor 2 en el código "Control LOP" mediante la función *28 Instalar_Terminal* o la macrofunción *129 Instalar_fS=4*), y debe haber sido configurado desde el programa **OEM** cargando la Tabla de Incidencias con las Incidencias "SxT" adecuadas (ver en el Anexo D.7.1 del documento MRT019). Hay que tener en cuenta que la prestación "SxT" sólo permite que un usuario, en un mismo proceso, pueda seleccionar una operación cada vez, por lo que si pretende ejecutar más de una deberá repetir el proceso de anotación en cada ocasión. Cuando la prestación "SxT" está definida queda inhabilitado cualquier otro uso de los permitidos por el **sistema CONACC** para las Salidas que estén involucradas en la definición.

(3)
La Partición afectada debe tener declarada la funcionalidad C.A. (ver el bit b33 en el Anexo D.2.1 del documento MRT019), y la "consola" debe ser accesible a los usuarios.

(4)
La excepción se produce cuando una Partición de 'operativa local' tiene activado el uso como **Panel de Alarmas externo** y el campo 'Ta' (ver en el Anexo D.2.1 del documento MRT019) es mayor que 0.

(5)
Cuando la Entrada implicada indica el uso por pulsos y la Partición está "armada", se ignora cualquier intento de "armado" y no se generan marcajes.

(6)
El rechazo de la orden de "armado" se puede producir por ya estar "armado" o por haber un intento de "armado" en curso; no se genera marcaje y se indica con un ST=69 en el momento de recibir la orden.

(7)
En las Instalaciones que no utilicen formato **fS=4** es posible indicar (mediante el bit b1[a] del parámetro 'MÁSCARA MISCELANEA 2') que la identificación del usuario puede formalizarse mediante anotación del **NIS** por teclado.

20.3 Ejemplos aplicativos

20.3.1 Introducción

En circunstancias normales de uso de un Terminal para el *Control de Accesos*, el mecanismo de apertura de la puerta de acceso está conectado a la Salida R1 del Terminal, pero en aquellas Instalaciones atípicas en las que exista un solo Terminal pero varias puertas (como sería el caso de una pequeña instalación técnica, etc.), se hace necesario que el usuario, antes de ser autorizado, decida por cual de tales puertas quiere acceder, para lo cual deberá usar el teclado del Terminal pulsando la(s) tecla(s) adecuada(s) para la puerta deseada.

La prestación "SxT" requiere el uso de teclado, por lo que sólo está implementada en los Terminales *Modulares* modelo DEF-3001 y en los **Paneles de Intrusión** modelo DEF-3003 cuando utilizan un Cabezal "en Kit" modelo DEF-KC097 o modelo DEF-KC097B si a éste se conecta un teclado no integrado; esta prestación sólo resulta operativa cuando el código "Control PANEL" contiene el valor 2 (para indicar **Panel tipo interno**) y el código "Control LOP" contiene el valor 2 (para indicar 'Cápsula_2'), cargados ambos mediante la función *28 Instalar_Terminal* o la macrofunción *129 Instalar_fS=4*.

La prestación "SxT" permite que, antes de que el FW haya validado la **Acreditación** presentada por el usuario (y le haya autenticado si el Terminal está parametrizado para ello), sea el usuario y no el propio FW el que defina por cual puerta debería serle permitido el acceso. Con la intención de simplificar tanto el FW como el programa **OEM**, esta prestación utiliza la Tabla_Incidencias, por lo que es allí donde habrá que definir cuales Incidencias serán las que hagan referencia a las Salidas activables (las conectadas desde el Terminal).

El FW busca en la Tabla_Incidencias el elemento cuyo campo 'NI' coincide con el número de Incidencia tecleado por el usuario, de manera que si el campo 'Texto' del elemento correspondiente existe un texto presentable al completo en la pantalla del Terminal considera que se trata de una Incidencia que deberá ser informada para ser tratada en *Control de Presencia*, por lo que el FW, una vez validada la **Acreditación**, genera los oportunos marcajes (ver la Nota de Aplicación QAN-02); en caso contrario, es decir, si en tal elemento no existe un texto presentable al completo sino una secuencia de control (formada por los dos primeros Bytes aunque después pueda existir un texto presentable), el FW considera que se trata de una operativa "SxT", por lo que, una vez validada la **Acreditación** del usuario, el FW comprobará en la Lista_Otras_Prestaciones (accediendo por el **NIS**) si el correspondiente elemento 'Cápsula_2' para tal usuario existe y si está admitida la operativa solicitada.

Todo lo expuesto hasta llegar aquí es extensible a otras acciones (aparte de la del acceso) tales como las propias de un Panel de Alarmas (como son "armar" y "desarmar" Particiones, etc.).

20.3.2 Casuística

Se trata de una instalación compuesta por un recinto de tres armarios técnicos (tipo estación de tranvía, aerogenerador, subestación eléctrica, etc) a cada uno de los cuales se accede mediante una puerta

Para efectuar el control de tal recinto se dispone de los siguientes elementos:
- un sensor sísmico general (engloba a todo el recinto);
- un sensor sísmico en el armario #1;
- una cerradura eléctrica y un contacto magnético en la puerta #1;
- una cerradura eléctrica y un contacto magnético en la puerta #2;
- una cerradura eléctrica y un contacto magnético en la puerta #3;
- un contacto magnético en el interior de la puerta #1;
- un contacto para control de **"tamper"** en el contenedor de la "consola" (formada por un Cabezal lector-grabador, una pantalla OLED, varios LED indicativos y un teclado)

Se pretende que los usuarios indiquen, mediante el teclado, una Incidencia, la cual puede ser tanto del tipo *Control de Presencia* (por lo que sólo afectará al control horario) como de tipo operativo (selección de la puerta, tipo de acción, etc.), debiendo el usuario, en ambos casos, identificarse mediante su **Acreditación** y, dependiendo de la operación seleccionada, autenticarse mediante la anotación de un **PIN**.

Para satisfacer tales necesidades deberá instalarse en cada recinto un Terminal *Modular* modelo DEF-3001 que tenga conectado un Cabezal "en Kit" modelo DEF-KC097 (incluye una pantalla OLED) al cual se debe conectar el teclado no integrado. Además, y dado que los usuarios son, mayoritariamente, personal de mantenimiento, también es necesario que puedan indicar hasta cinco Incidencias de tipo laboral (inicio de trabajo global, inicio de descanso, final de descanso, final de trabajo global y ronda de vigilancia) sin que la anotación de tales Incidencias deba facilitar acceso alguno.

Para, en la medida de lo posible evitar errores, se facilita las acciones de los usuarios en base a que éstos indiquen (pulsando las teclas 1, 2 ó 3) sobre cual de las tres puertas quieren operar (con "desarmado" si se requiere) o sobre cual se pretende el "armado" (pulsando las teclas 1+1, 1+2 ó 1+3), al igual que indiquen (pulsando las teclas 4, 5, 6, 7 ó 9) la Incidencia que se corresponde con la situación laboral, quedando el uso de la tecla 8 para declarar una situación de **coacción**.

Dado que todas las Incidencias pueden tener un texto explicativo (de hasta 16 caracteres las Incidencias CP y de hasta 14 caracteres las Incidencias "SxT"), el programa **OEM** debe facilitar al Operador la introducción de los textos oportunos para que aparezcan posteriormente en la pantalla de los Terminales. Sin embargo, para las Incidencias 1 a 3, en el campo 'Texto' debe haber, como mínimo, la secuencia de control adecuada (ver el Anexo D del documento MRT019); el FW valida tal secuencia de control con la información contenida en el elemento 'Cápsula_2'correspondiente al **NIS** del usuario (ver la Lista_Otras_Prestaciones en el capítulo 3 del documento MRT019).

Una vez que el usuario haya anotado la Incidencia oportuna (para indicar la operativa que pretende iniciar o la Incidencia CP que pretende declarar) se identificará normalmente mediante su **Acreditación** y se autenticará anotando el **PIN** que le hayan asignado (en este ejemplo se trata a las **Acreditaciones** en formato **fS=3**, pero también podrían serlo en formato **fS=4**).

Una última consideración atañe a la necesidad de controlar la posible situación de **coacción**, en cuyo caso se vincula a la apertura de la puerta #1.

20.3.2.1 Ejemplo en conexión con un Panel de Alarmas externo

El Terminal *Modular* modelo DEF-3001 se conecta con un **Panel de Alarmas externo** previamente existente en la Instalación:

DEFINICIÓN DE ENTRADAS					
Entrada lógica	Entrada física (clema)	Función	Tipo vinculación "armado"	Temporización	Partición
E1	#1 IN1 (10+11)	'Ead' #1(1)	0	inmediata	#1
E2	#1 IN2 (12+13)	'Ead' #2(1)	0	inmediata	#2
E5	#1 IN3 (14+15)	'Ead' #3(1)	0	inmediata	#3
E6	#1 IN4 (16+17)	(disponible)	-	inmediata	-
E9	#2 IN1 (30+31)	(disponible)	-	inmediata	-
E10	#2 IN2 (32+33)	(disponible)	-	inmediata	-
E11	#2 IN3 (34+35)	(disponible)	-	inmediata	-
E12	#2 IN4 (36+37)	(disponible)	-	inmediata	-

DEFINICIÓN DE SALIDAS		
Salida lógica	Salida física (clema)	Función
S1 (R1)	#1 OUT1 (18+19)	cerradero puerta #1(2)
S2 (R2)	#1 OUT2 (20+21)	cerradero puerta #2(2)
S3	#1 OUT3 (22+23)	cerradero puerta #3(2)
S4	#1 OUT4 (24+25)	(disponible)
S5	#2 OUT1 (38+39)	'Sad' #1(1)
S6	#2 OUT2 (40+41)	'Sad' #2(1)
S7	#2 OUT3 (42+43)	'Sad' #3(1)
S8	#2 OUT4 (44+45)	Alarma por **coacción**(1)

DEFINICIÓN DE PARTICIONES					
Partición	Función	Tipo	b32 (Anexo D.2.1)	Salidas	
				Alarma	'Sad'
#1	armario técnico #1	de 'operativa local'	control externo	-	S5
#2	armario técnico #2	de 'operativa local'	control externo	-	S6
#3	armario técnico #3	de 'operativa local'	control externo	-	S7
#4	Fallo/vandalismo Cabezal	de '24H'	-	-	-

DEFINICIÓN DE INCIDENCIAS[3]					
'NI'	tipo	'AR'	'PAR'		Mensaje en pantalla
			'SP'	'RS'	
1	"SxT"	FBh	1	3	"DESAR.+Abrir 1"
2	"SxT"	FBh	2	3	"DESAR.+Abrir 2"
3	"SxT"	FBh	3	3	"DESAR.+Abrir 3"
4	CP	-	-	-	"ENTRADA JORNADA "
5	CP	-	-	-	" SALIDA JORNADA "
6	CP	-	-	-	" RONDAS "
7	CP	-	-	-	"INICIO DESCANSO "
8	"SxT"	FFh[4]	'NI' = 1		"Abrir Puerta 1"[5]
9	CP	-	-	-	" FIN DESCANSO "
11	"SxT"	FEh	1	1[6]	"ARMAR PUERTA 1"
12	"SxT"	FEh	2	1[6]	"ARMAR PUERTA 2"
13	"SxT"	FEh	3	1[6]	"ARMAR PUERTA 3"

NOTAS:
(1)
La Salida física debe conectarse a una entrada del **Panel de Alarmas externo**.

(2)
Hay que indicar los tiempos de excitación de la Salida en el parámetro 'TIEMPOS SALIDA 1 Y SALIDA 2' y 'TIEMPOS SALIDA S3 Y SALIDA S4' del mapa estándar del **sistema CONACC** (capítulo 3).

(3)
La explicación de los parámetros (los acrónimos inscritos entre apóstrofes) hay que verla en el capítulo D.7.1 en el Anexo D del documento MRT019.

(4)
Para controlar la situación de **coacción** hay que activar los bits b7 y b8 en el parámetro 'ASIGNACIÓN SALIDAS' del mapa estándar del **sistema CONACC** (capítulo 3), mientras que en los bits b13 a b16 del parámetro 'ASIGNACIÓN SALIDAS 2' (ver el capítulo D.1.12 en el Anexo D del documento MRT019) hay que indicar que la Salida que se quiere utilizar es la S8 y, por consiguiente, hay que indicar el tiempo de excitación deseado en el parámetro 'TIEMPOS SALIDAS S7 Y S8' (ver el capítulo D.1.6 en el Anexo D del documento MRT019).

(5)
Como sugerencia, el texto que aparezca en una anotación por **coacción** puede estar en minúsculas para diferenciarlo del texto de anotación normal (mismo texto pero en mayúsculas).

(6)
Si se pretende que se pueda "armar" sin necesidad de presentar una **Acreditación** y simplificar así la operativa, habría que poner el valor 2 en 'RS' para que el FW pida el **PIN** asignado al Terminal, para lo cual el programa **OEM** lo habrá cargado mediante la función *27 Crear_PIN*.

20.3.2.2 Ejemplo en funcionamiento autónomo

El Terminal *Modular* modelo DEF-3001 actúa como **Panel tipo interno**:

DEFINICIÓN DE ENTRADAS					
Entrada lógica	Entrada física (clema)	Función	Tipo vinculación "armado"	Temporización de la Entrada	Partición
E1	#1 IN1 (10+11)	contacto magnético puerta #1	2	inmediata	#1
E2	#1 IN2 (12+13)	contacto magnético puerta #2	2	inmediata	#2
E4	-	contacto para el control de **"tamper"**	-	inmediata	#5
E5	#1 IN3 (14+15)	contacto magnético puerta #3	2	inmediata	#3
E6	#1 IN4 (16+17)	sísmico general	1	5(1)	#4
E9	#2 IN1 (30+31)	contacto magnético interior puerta #1	3	5(1)	#1
E10	#2 IN2 (32+33)	sísmico armario #1	3	5(1)	#1
E11	#2 IN3 (34+35)	fallo alimentación (SAI)	-	5(1)	#6
E12	#2 IN4 (36+37)	'Zona llave' (señalización interna)(2)	0	5(1)	#4

DEFINICIÓN DE SALIDAS		
Salida lógica	Salida física (clema)	Función
S1 (R1)	#1 OUT1 (18+19)	cerradero puerta #1(3)
S2 (R2)	#1 OUT2 (20+21)	cerradero puerta #2(3)
S3	#1 OUT3 (22+23)	cerradero puerta #3(3)
S4	#1 OUT4 (24+25)	señalización interna 'Sad' #1, 'Sad' #2 y 'Sad' #3(2)
S5	#2 OUT1 (38+39)	Salida Alarma (sirena, etc.)
S6	#2 OUT2 (40+41)	(disponible)
S7	#2 OUT3 (42+43)	(disponible)
S8	#2 OUT4 (44+45)	activación cámara, etc.

DEFINICIÓN DE PARTICIONES							
Partición	Función	Tipo	b32 (Anexo D.2.1)	Enclavable	Salidas		C.A,
					Alarma	'Sad'	
#1	intrusión armario técnico #1	de 'operativa local'	control interno	si	S5 y S8	S4	si
#2	intrusión armario técnico #2	de 'operativa local'	control interno	si	S5 y S8	S4	si
#3	intrusión armario técnico #3	de 'operativa local'	control interno	si	S5 y S8	S4	si
#4	Alarma sísmico general	de 'operativa local'	control interno	si	S5 y S8	-	no
#5	**"tamper"** en "consola"	de '24H'	-	si	S5 y S8	-	no
#6	fallo alimentación	de '24H'	-	no	S5	-	no

DEFINICIÓN DE INCIDENCIAS[4]					
'NI'	tipo	'AR'	'PAR'		Mensaje en pantalla
			'SP'	'RS'	
1	"SxT"	FBh	1	3	"DESAR.+Abrir 1"
2	"SxT"	FBh	2	3	"DESAR.+Abrir 2"
3	"SxT"	FBh	3	3	"DESAR.+Abrir 3"
4	CP	-	-	-	"ENTRADA JORNADA "
5	CP	-	-	-	" SALIDA JORNADA "
6	CP	-	-	-	" RONDAS "
7	CP	-	-	-	"INICIO DESCANSO "
8	"SxT"	FFh[5]	'NI' = 1		"Abrir Puerta 1"[6]
9	CP	-	-	-	" FIN DESCANSO "
11	"SxT"	FEh	1	1[7]	"ARMAR PUERTA 1"
12	"SxT"	FEh	2	1[7]	"ARMAR PUERTA 2"
13	"SxT"	FEh	3	1[7]	"ARMAR PUERTA 3"

NOTAS:

(1)
Este tiempo (en segundos) está definido en los bits b17 a b22 del registro correspondiente a la Entrada, el cual forma parte de la TABLA ENTRADAS (ver el capítulo D.3.1 en el Anexo D del documento MRT019).

(2)
Hay que interconectar físicamente la Entrada E12. y la Salida S4.

(3)
Hay que indicar los tiempos de excitación de la Salida en el parámetro 'TIEMPOS SALIDA 1 Y SALIDA 2' y 'TIEMPOS SALIDA S3 Y SALIDA S4' del mapa estándar del **sistema CONACC** (capítulo 3).

(4)
La explicación de los parámetros (los acrónimos inscritos entre apóstrofes) hay que verla en el capítulo D.7.1 en el Anexo D del documento MRT019.

(5)
Para controlar la situación de **coacción** hay que activar los bits b7 y b8 en el parámetro 'ASIGNACIÓN SALIDAS' del mapa estándar del **sistema CONACC** (capítulo 3), mientras que en los bits b13 a b16 del parámetro 'ASIGNACIÓN SALIDAS 2' (ver el capítulo D.1.12 en el Anexo D del documento MRT019) hay que indicar que la Salida que se quiere utilizar es la S8 y, por consiguiente, hay que indicar el tiempo de excitación deseado en el parámetro 'TIEMPOS SALIDAS S7 Y S8' (ver el capítulo D.1.6 en el Anexo D del documento MRT019).

(6)
Como sugerencia, el texto que aparezca en una anotación por **coacción** puede estar en minúsculas para diferenciarlo del texto de anotación normal (mismo texto pero en mayúsculas).

(7)
Si se pretende que se pueda "armar" sin necesidad de presentar una **Acreditación** y simplificar así la operativa, habría que poner el valor 2 en 'RS' para que el FW pida el **PIN** asignado al Terminal, para lo cual el programa **OEM** lo habrá cargado mediante la función *27 Crear_PIN*.

ESTA PÁGINA HA SIDO DEJADA EN BLANCO INTENCIONADAMENTE

código	título	relaciones
QAN-21	Usos específicos, usos especiales y señalización con HYDRA-II y/o con DEF-3002	- MRT019 : capítulo 3 (*Dirección 42*) (*Dirección 71*) - MRT019 : capítulo 5 (funciones *28, 32 y 129*) - BTP027 (Revisión Y y >>) - BTP041 (Revisión D y >>) - MIP-HYDRA-II - MIP-3002

Bajo un punto de vista histórico, todos los Terminales fabricados por Qontinuum consisten en una electrónica de control más el correspondiente Cabezal lector o lector-grabador, pudiendo ser dos los Cabezales lectores en los Terminales llamados bicéfalos (modelos XX-507 y XX-907) y pudiendo ser dos Terminales más dos Cabezales lectores o lectores-grabadores en los Terminales dobles (modelos XX-902).

En todos esos casos, los programas **OEM** deben considerar a cada Terminal como un todo, excepto a los Terminales dobles a los que deben considerar como dos todos por completo independientes (físicamente están situados en un mismo contenedor, pero a efectos lógicos se tratan como dos Terminales totalmente independientes, por lo que cada uno de ellos deberá tener un ID diferente de todos los demás de la Instalación; a efectos prácticos, en este documento se hace referencia con ID = N al primer Terminal (el que dispone del Cabezal #1) y con ID = M al segundo Terminal (el que dispone del Cabezal #2) de un mismo subsistema HYDRA-II o del mismo equipo modelo DEF-3002.

Con la aparición del subsistema HYDRA-II y de los Terminales *Modulares* modelo DEF-3002 (basados en una misma electrónica), algunas consideraciones deben ser hechas dado que, aunque cada conjunto formado por el subsistema HYDRA-II con el correspondiente Cabezal lector o a cada conjunto formado por el equipo modelo DEF-3002 con el correspondiente Cabezal lector-grabador forma un Terminal y aunque, por lo anteriormente expuesto, cada Terminal debe ser considerado como un todo, existen algunas aplicaciones en las que se produce la cooperación entre los dos Terminales instalados en un mismo subsistema HYDRA-II o en un mismo equipo modelo DEF-3002. Esta Nota de Aplicación tiene por objetivo ayudar a que los programas **OEM** puedan implementar tales aplicaciones, por lo que este documento debe ser interpretado conjuntamente con el documento BTP041 (dado que allí se definen y explican conceptos que aquí se dan por entendidos.

Para seleccionar cual de las prestaciones que son exclusivas para los subsistema HYDRA-II y para los equipos modelo DEF-3002 se quiere usar, hay que declararlo en el código “Control UEES” (Usos Específicos, Especiales y Señalización) del parámetro ‘IM’ de la función *28 Instalar_Terminal* o de la macrofunción *129 Instalar_fS=4*. Obviamente, cualquiera de las prestaciones sólo implica a los dos Terminales de un mismo subsistema HYDRA-II o de un mismo equipo modelo DEF-3002, debiendo ambos Terminales ser instalados indicando la misma opción (excepto cuando se indique otra cosa en los subcapítulos siguientes).

21.1 Utilización con Semáforo virtual

La utilización específica del **Semáforo virtual** debe ser activada indicando el valor 1 en el código "Control UEES" de los dos Terminales involucrados (del mismo subsistema HYDRA-II o del mismo equipo modelo DEF-3002), así como también debe cargarse en cada Terminal el parámetro 'LATENCIA ENTRADAS' para E1.

Al usar esta prestación, cuando se está realizando un acceso por uno de los dos Terminales, por ejemplo el de ID = N de la pareja vinculada, se bloquea el intento de uso en el Terminal con ID = M, por lo que el LED rojo del Cabezal lector o lector-grabador del Terminal con ID = M permanecerá encendido para indicarlo y, a cada intento de acceso, el FW generará un **marcaje normal** con CE=28. En tales circunstancias, también se inhibe en el Terminal con ID = M la "alarma puerta inmediata" (corresponde a la situación de "puerta forzada") relacionada con el punto de paso abierto, perdurando tal inhibición para este Terminal hasta que se cierre el punto de paso, mientras que en el Terminal con ID = N el FW controla si se agota el tiempo indicado en su parámetro 'LATENCIA ENTRADAS' para E1 para, de agotarse, activar la "alarma puerta" (corresponde a la situación de "puerta mantenida").

Para los dos Terminales de un mismo subsistema HYDRA-II o de un mismo equipo modelo DEF-3002 no es posible definir el uso concurrente de **Semáforo virtual** y de **Semáforo físico**, de manera que, si se intentara hacerlo, el FW correspondiente retornaría el código de estado *19 Parámetros erróneos* a la función *28 Instalar_Terminal* o a la macrofunción *129 Instalar_fS=4*.

21.2 Utilización en esclusa

21.2.1 Esclusa de tipo 1

La utilización específica en **esclusa** de tipo 1 debe ser activada indicando el valor 5 en el código “Control UEES” de los dos Terminales involucrados (del mismo subsistema HYDRA-II o del mismo equipo modelo DEF-3002).

Esta prestación implica el control por **Semáforo virtual** añadiendo, a la característica de doble punto de acceso, la más específica de recinto cerrado no excluyente de más de una persona. Por tal razón, el recinto puede ser grande.

Esta prestación se aplica a los dos Terminales que deban controlar los dos pasos de una **esclusa**. A cada Terminal se le conectará los elementos (Cabezal lector o lector-grabador, “pulsador auxiliar” para el sentido ‘Salida’, cerradura y sensor de puerta) adecuados para el punto de paso, por lo que los parámetros programados en cada Terminal corresponden a los elementos conectados sólo a él.

Dado que la función básica de una **esclusa** es la de no permitir el acceso por un punto de paso mientras esté abierto el otro, si tal circunstancia se diera, el FW rechaza el intento de acceso y genera un **marcaje normal** (si el intento se realiza por medio de un Cabezal) o un **marcaje especial** (si el intento se realiza por medio del “pulsador auxiliar” para el sentido ‘Salida’), en ambos casos con CE=28.

21.2.2 Esclusa de tipo 2

La utilización específica en **esclusa** de tipo 2 debe ser activada indicando el valor 2 en el código “Control UEES” de los dos Terminales involucrados (del mismo subsistema HYDRA-II o del mismo equipo modelo DEF-3002).

Esta prestación implica el control por **Semáforo virtual** añadiendo, a la característica de doble punto de acceso, la más específica de recinto cerrado excluyente de más de una persona. Por tal razón, el recinto debe ser necesariamente pequeño y, probablemente, estar dotado con algún elemento “autenticador” de la persona (como puede ser una báscula para biometría de Clase “5") o un elemento “detector” de presencia física (como puede ser un sensor de presión por peso, un sensor de temperatura, etc.).

Esta prestación se aplica a los dos Terminales que deban controlar los dos pasos de una **esclusa**. A cada Terminal se le conectará los elementos (Cabezal lector o lector-grabador, “pulsador auxiliar” para el sentido ‘Salida’, cerradura y sensor de puerta) adecuados para el punto de paso, por lo que los parámetros programados en cada Terminal corresponden a los elementos conectados sólo a él.

Dado que la función básica de una **esclusa** es la de no permitir el acceso por un punto de paso mientras esté abierto el otro, si tal circunstancia se diera, el FW rechaza el intento de acceso y genera un **marcaje normal** (si el intento se realiza por medio de un Cabezal) o un **marcaje especial** (si el intento se realiza por medio del “pulsador auxiliar” para el sentido ‘Salida’), en ambos casos con CE=28.

21.3 Utilización en 'zona común'

La utilización específica en 'zona común' del control de una Partición en un **Panel de Alarmas externo** (sólo resulta aplicable a los Terminales de un equipo modelo DEF-3002) debe ser activada cargando el valor 4 en el código "Control UEES" y cargando de contenido el parámetro 'INTERACCIÓN PANEL' de los dos Terminales involucrados. De tales Terminales, el de ID = N es el que se conectará físicamente con el **Panel de Alarmas externo**, por lo que se le deberá cargar el valor 4 en el código "Control PANEL" y definir el parámetro 'INTERACCIÓN PANEL' al completo, mientras que en el segundo Terminal se deberá cargar el valor 0 en el código "Control PANEL" y sólo se usará el subparámetro 'Tiempo permanencia' del parámetro 'INTERACCIÓN PANEL'.

Cada uno de los Terminales implicados que tenga activado el bit b3 del parámetro 'MÁSCARA MISCELÁNEA 4' indicará (mediante el LED del Cabezal lector-grabador correspondiente) el estado actual de la 'zona común' del **Panel de Alarmas externo** (rojo = "armado", verde = "desarmado").

Cuando el equipo modelo DEF-3002 autorice a un usuario el acceso desde cualquiera de los dos puntos vinculados, "desarmará" la correspondiente Partición en el **Panel de Alarmas externo**, al igual que la "armará" (también desde cualquiera de los dos puntos de acceso) cuando el usuario realice la operativa adecuada. Mientras se realiza una operación en uno de los Terminales se bloqueará la operativa en el otro y viceversa, lo cual queda indicado en el oportuno Cabezal lector-grabador por el LED rojo encendido.

Cuando el programa **OEM** quiera conocer o modificar en el **Panel de Alarmas externo** el estado de la Partición físicamente vinculada, podrá hacerlo dirigiéndose a cualquiera de los Terminales implicados. El Operador deberá tener en cuenta que la última operación que haga sobre cada Terminal será el estado en el que quede la Partición en el **Panel de Alarmas externo** (por ejemplo, si "arma" desde el ID = N y posteriormente "desarma" desde el ID = M, la Partición en el **Panel de Alarmas externo** quedará "desarmada").

Los **marcajes normales** *55 "desarmado"* y *56 "armado"* generados por el FW debido a la presentación de una **Acreditación** por parte de los usuarios, se grabarán en el Terminal desde el cual se ha ordenado la acción de "desarmar" o de "armar".

Los **marcajes especiales** *55 "desarmado"* y *56 "armado"* generados por el FW debido a las ordenes enviadas por el programa **OEM** directamente a uno de los Terminales vinculados, se grabarán en ese Terminal.

El **marcaje especial** *56 "armado"* generado por el FW debido a las ordenes enviadas por el programa **OEM** directamente al **Panel de Alarmas externo** y comunicado por éste al equipo modelo DEF-3002, se grabará en el Terminal con ID = N dado que es el que tiene las conexiones físicas con la pertinente Partición en el **Panel de Alarmas externo**.

21.4 Utilización en doble intervención simultánea

La utilización especial de la **doble intervención simultánea** debe ser activada indicando el valor 8 en el código "Control UEES" y cargando de contenido el parámetro 'GRUPO DOBLE INTERVENCIÓN SIMULTÁNEA' del único Terminal involucrado(1), el cual estará dotado con dos Cabezales.

Esta prestación requiere que sean dos los usuarios autorizados y que realicen la presentación de sus respectivas **Acreditaciones** de manera concurrente en el tiempo, por lo que un usuario presentará su **Acreditación** en un Cabezal y el otro usuario presentará la suya en el otro Cabezal con una forzada simultaneidad (el desfase temporal no puede superar el tiempo indicado en el subparámetro **latencia Usuario**(2)).

Los dos Cabezales se colocarán físicamente a una distancia suficiente entre ellos para que una sola persona no pueda alcanzar a ambos simultáneamente (por ejemplo, extendiendo los brazos) ni pueda hacerlo antes de que acabe el tiempo indicado en el subparámetro **latencia Usuario**(2). Una explicación completa de esta prestación puede verse en el subcapítulo 2.4.2 de la Revisión Y (y posteriores) del documento BTP027.

En aquellas Instalaciones en las que se utilicen **Acreditaciones** dotadas con formato **fS=4**, el uso de la **doble intervención simultánea** inhabilita las siguientes posibilidades:

- utilizar el control anti **Pass-Back**;
- provocar la situación de **aplicación bloqueada**;
- renovar la **Fecha Caducidad**;
- 'desactivar' el **Estado Operativo**.

Además, el FW opera como si el bit b5[a] del parámetro 'MÁSCARA MISCELÁNEA 3' estuviera a 1.

NOTAS:

(1)
Para poder implementar esta utilización especial, tanto el subsistema HYDRA-II como el Terminal *Modular* modelo DEF-3002 quedan limitados a ser un único Terminal que controla a los dos Cabezales conectados.

(2)
Excepcionalmente en este caso, el FW tomará el tiempo indicado en el subparámetro **latencia Usuario** como décimas de segundo.

21.5 Utilización en doble intervención simultánea (extendida)

La utilización especial de la **doble intervención simultánea (extendida)** comporta el uso de dos Terminales *Modulares* del modelo DEF-3002 (aquí llamados A y B), situados uno (A) en el sentido de entrada y el otro (B) en el sentido de salida de un mismo punto de acceso[1] a un recinto que, por su naturaleza, requiere de este tipo de control, debiendo tal utilización ser activada (mediante la función *28 Instalar_Terminal* o a la macrofunción *129 Instalar_fS=4*) en ambos Terminales, indicando el valor 8 en el código "Control UEES"; además (también en ambos Terminales), hay que cargar con el valor adecuado el parámetro 'GRUPO DOBLE INTERVENCIÓN SIMULTÁNEA' y hay que cargar el bit b8 del parámetro 'CONTADOR AFORO' con el valor 0 para indicar sentido de entrada y con el valor 1 para indicar sentido de salida.

Esta prestación requiere que sean dos los usuarios autorizados y que realicen la presentación de sus respectivas **Acreditaciones** de manera concurrente en el tiempo, por lo que un usuario presentará su **Acreditación** en un Cabezal y el otro usuario presentará la suya en el otro Cabezal (ambos del mismo Terminal)[2] con una forzada simultaneidad (el desfase temporal no puede superar el tiempo indicado en el subparámetro **latencia Usuario**[3]).

El Terminal A sólo forzará la **doble intervención simultánea** cuando el subcampo 'CA' del parámetro 'CONTADOR AFORO' indique 0, mientras que cuando indique cualquier valor igual o mayor que 2 desactivará de manera virtual tal control[4], el cual sólo volverá a ser activado cuando el subcampo 'CA' indique 0.
El Terminal B funciona de manera coordinada con el Terminal A, de manera que ambos forman una pareja que deben necesariamente intercambiar señales físicas entre, respectivamente, las Salidas S5[5] y las Entradas E9[5], siendo la única diferencia que el Terminal B no utiliza su propio subcampo 'CA' sino que sólo lo hace el Terminal A, incrementando o decrementando el valor dependiendo de las circunstancias expuestas en los siguientes dos subcapítulos.

En aquellas Instalaciones en las que se utilicen **Acreditaciones** dotadas con formato **fS=4**, el uso de la **doble intervención simultánea (extendida)** inhabilita las siguientes posibilidades:

- utilizar el control anti **Pass-Back**;
- provocar la situación de **aplicación bloqueada**;
- renovar la **Fecha Caducidad**;
- 'desactivar' el **Estado Operativo**.

Además, el FW opera como si el bit b5[a] del parámetro 'MÁSCARA MISCELÁNEA 3' estuviera a 1.

21.5.1 entrada de usuarios

Dado que se trata de controlar el acceso a un recinto, las secuencias lógicas empiezan necesariamente en el Terminal A, lo cual ocurre de la siguiente manera:

1) La primera vez (el valor del subcampo 'CA' del parámetro 'CONTADOR AFORO' del Terminal A es = 0):

   1.1) a partir de la aceptación de tal primer acceso, el FW del Terminal A carga el subcampo 'CA' del parámetro 'CONTADOR AFORO' con el valor 2 (por los dos usuarios que han accedido en el proceso de **doble intervención simultánea**) y desactiva de manera virtual tal control[(4)];

   1.2) el Terminal B no recibe señal alguna por su Entrada E9[(5)], por lo que se sigue comportando normalmente con el control de **doble intervención simultánea** activado, de manera que, en ese momento, si los dos usuarios que han entrado conjuntamente quisieran salir también deberían hacerlo de manera conjunta[(6)].

2) La segunda vez (el valor del subcampo 'CA' del Terminal A es = 2):

   2.1) el Terminal A actúa con el control de **doble activación simultánea** desactivado, por lo que valida y acepta el marcaje de manera simple (sólo en el Cabezal nº 1)[(4)], lo señaliza activando su Salida S5[(5)] e incrementa en una unidad el subcampo 'CA' del parámetro 'CONTADOR AFORO';

   2.2) el Terminal B detecta la presencia de señal en su Entrada E9[(5)], por lo que desactiva su control de **doble intervención simultánea**.

3) Las siguientes veces (el valor del subcampo 'CA' del Terminal A es > 2):

   3.1) El Terminal A se sigue comportando igual que en el punto 2.1 (aunque sin tener que activar su Salida S5[(5)] dado que ésta permanece activada todo el tiempo);

   3.2) El Terminal B se sigue comportando igual que en el punto 2.2 (aunque sin tener que desactivar la **doble intervención simultánea** dado que ya lo está).

21.5.2 salida de usuarios

En cualquier momento a partir de la entrada de dos o más usuarios, cualquiera de ellos puede querer salir, de manera que las secuencias lógicas empiezan ahora en el Terminal B, lo cual ocurre de la siguiente manera:

1) Si la Entrada E9(5) del Terminal B está activada (significa que el subcampo 'CA' del parámetro 'CONTADOR AFORO' del Terminal A indica un valor > 2, razón por la cual desactiva o mantiene desactivado su control de **doble intervención simultánea**) :

1.1) a partir de la aceptación del acceso sencillo, el FW del Terminal B lo señaliza mediante un pulso en su Salida S5(5);

1.2) el Terminal A recibe un pulso por su Entrada E9(5), por lo que decrementa en una unidad el subcampo 'CA' del parámetro 'CONTADOR AFORO';

2) Si la Entrada E9(5) del Terminal B está desactivada (significa que el subcampo 'CA' del parámetro 'CONTADOR AFORO' del Terminal A indica un valor igual o inferior a 2(7)):

2.1) reactiva el control de **doble intervención simultánea** y, a partir de la aceptación del acceso, el FW del Terminal B lo señaliza mediante un pulso en su Salida S5(5);

2.2) el Terminal A recibe el pulso por su Entrada E9(5) y, en consecuencia, pone a 0 el subcampo 'CA' del parámetro 'CONTADOR AFORO' y reactiva su control de **doble intervención simultánea**.

3) Si el subcampo 'CA' del parámetro 'CONTADOR AFORO' del Terminal A indica un valor inferior a 2, dicho Terminal activa su Salida S4 (**Semáforo físico**) para que el Terminal B rechace cualquier intento de acceso de salida. Los LED de los Cabezales del Terminal B permanecerán en rojo mientras dure tal circunstancia.

21.5.3 en resumen

El Terminal A sólo opera controlando la **doble intervención simultánea** cuando el valor del subcampo 'CA' de su parámetro 'CONTADOR AFORO' es = 0, mientras que con cualquier otro valor tal control permanece desactivado.

El Terminal B sólo opera controlando la **doble intervención simultánea** cuando su Entrada E9(5) está desactivada,

De todos modos, y dado que el contenido de los subcampos 'CA' resulta accesible a los programas **OEM**, son éstos los que deben considerar todas las casuísticas factibles en las diversas Instalaciones donde convenga utilizar la **doble intervención simultánea (extendida)**, teniendo en cuenta que el subcampo 'CA' del parámetro 'CONTADOR AFORO' que indica algún valor sólo es el correspondiente al Terminal A.

NOTAS:

(1)
Para poder implementar esta utilización especial, cada uno de los dos Terminales *Modular*es modelo DEF-3002 queda limitado a comportarse como un único Terminal que controla a los dos Cabezales que debe tener conectados.

(2)
Los dos Cabezales de cada Terminal (tanto de A como de B) deberán estar físicamente colocados a una distancia suficiente entre ellos para que una sola persona no pueda alcanzar a ambos simultáneamente (por ejemplo, extendiendo los brazos) ni pueda hacerlo antes de que acabe el tiempo indicado en el subparámetro **latencia Usuario**(3). Una explicación práctica de esta prestación puede verse en el subcapítulo 2.4.3 de la Revisión Y (y posteriores) del documento BTP027.

(3)
Excepcionalmente en este caso, el FW tomará el tiempo indicado en el subparámetro **latencia Usuario** como décimas de segundo.

(4)
Mientras el valor contenido en el subcampo 'CA' del parámetro 'CONTADOR AFORO' sea 2 o superior, el FW del Terminal ignora la funcionalidad de **doble intervención simultánea (extendida)** y opera como un Control de Acceso normal al ignorar a las **Acreditaciones** que se puedan presentar en el Cabezal nº 2, en el cual se encenderá y apagará secuencial y repetidamente el LED rojo para indicar que está bloqueado (fuera de servicio).

(5)
Dada la utilización atípica de estas Salidas y Entradas, en el siguiente cuadro se establece la relación entre la funcionalidad del FW y el necesario cableado físico en las placas:

funcionalidad	serigrafía en la placa	bornas
Salida S5	OUT1 (en conector CN13)	38 y 39
Entrada E9	IN1 (en conector CN9)	30 y 31

Para una mayor información hay que ver el Manual Informativo del Producto MIP-3002.

(6)
Tales parejas hay que entenderlas formadas no necesariamente por los mismos usuarios sino por dos de ellos cuyo grupo Usuario esté indicado en el parámetro 'GRUPO DOBLE INTERVENCIÓN SIMULTÁNEA'.

(7)
Si tal valor no es 0 sólo puede ser por un error del programa **OEM** al cargar valor en el parámetro 'CONTADOR AFORO'.

21.6 Utilización en Control del aforo

La utilización especial de Control del **aforo** comporta el uso de un Terminal *Modular* del modelo DEF-3002 del que se utilizarán los dos Terminales implícitos (aquí llamados A y B), situados uno (A) en el sentido de entrada y el otro (B) en el sentido de salida de un recinto que, por su naturaleza, requiere de este tipo de control, debiendo tal utilización ser activada (mediante la función *28 Instalar_Terminal* o a la macrofunción *129 Instalar_fS=4*) en ambos Terminales, indicando el valor 6 en el código "Control UEES". También hay que cargar el bit b8 del parámetro 'CONTADOR AFORO' con el valor 0 en el Terminal A (para indicar sentido de entrada) y con el valor 1 en el Terminal B (para indicar sentido de salida), debiendo finalmente cargar en el Terminal A el número máximo de **aforo** del recinto en el parámetro 'LÍMITE AFORO'.

Esta prestación pretende controlar el aforo de un recinto, de manera que cuando se alcance el límite indicado en el parámetro 'LÍMITE AFORO', el Terminal A rechazará todo intento de acceso generando un **marcaje normal** *28 Acceso en suspenso*, no saliendo de tal situación hasta que en el Terminal B se produzca un paso correcto, lo cual implica una salida y por tanto la disponibilidad de una plaza, por lo que el Terminal A vuelve a tratar normalmente a la primera **Acreditación** que se le presente. Estando el Terminal A en la circunstancia de rechazar los intentos de acceso, mantiene activada la Salida S3 para un posible uso externo (por ejemplo, un semáforo luminoso).

Excepcionalmente, si el Terminal A y el Terminal B contienen el valor 6 en el código "Control LOP" (cargado mediante la función *28 Instalar_Terminal* o a la macrofunción *129 Instalar_fS=4*) aquellas **Acreditaciones** cuyo **NIS** aparezca declarado en un elemento 'Cápsula_6' serán aceptadas excepcionalmente y procesadas como si el Terminal no controlara el **aforo**, de manera que los accesos serán aceptados si cumplen las condiciones normales para ello(1).

El Terminal B funciona de manera coordinada con el Terminal A, de manera que ambos forman una pareja que deben necesariamente intercambiar información, siendo la única diferencia que el Terminal B no utiliza su propio subcampo 'CA' sino que sólo lo hace el Terminal A, incrementando o decrementando el valor dependiendo de las circunstancias expuestas en los siguientes dos subcapítulos.

Existe la posibilidad de utilizar un segundo Terminal *Modular* modelo DEF-3002 para controlar un segundo punto de paso en el sentido de salida del recinto (sería el Terminal C), en cuyo caso se utilizará la Salida S2 del Terminal C para conectarla a la Entrada E2(2) del Terminal A, de manera que éste considere por igual a la información recibida tanto del Terminal B como del Terminal C en cuanto se refiere a la disminución del contenido del subcampo 'CA' del parámetro 'CONTADOR AFORO'.

21.6.1 entrada de usuarios (Terminal A)

Dado que se trata de controlar el acceso a un recinto, la secuencia lógica empieza necesariamente en el Terminal A, lo cual ocurre de la siguiente manera:

1) Si el **NIS** de la **Acreditación** presentada aparece en un elemento 'Cápsula_6' de la Lista_Otras_Prestaciones, se trata con total normalidad y sin afectación alguna al Control del **aforo**.

2) Si el **NIS** de la **Acreditación** presentada no aparece en un elemento 'Cápsula_6' (o si tal Lista no está declarada) se calcula la diferencia entre el valor contenido en el parámetro 'LÍMITE AFORO' y el valor contenido en el subcampo 'CA' del parámetro 'CONTADOR AFORO':

2.1) si tal diferencia es inferior en más de una unidad se trata normalmente a la **Acreditación** y, si el acceso se permite, el FW del Terminal A incrementa en una unidad el subcampo 'CA' del parámetro 'CONTADOR AFORO';

2.2) si tal diferencia es inferior en una unidad se trata igual que en el punto 2.1 pero al acabar, y por haber quedado cubierto el **aforo**, el Terminal A activa el LED rojo del Cabezal;
2.3) si tal diferencia es 0 (por tanto el **aforo** está completo), cualquier **Acreditación** presentada que no cumpla con el punto 1 es rechazada generando un **marcaje normal** *28 Acceso en suspenso*.

21.6.2 salida de usuarios (Terminal B)

El Terminal B controla el sentido de salida del recinto, por lo que la secuencia lógica ocurre de la siguiente manera:

1) Si el **NIS** de la **Acreditación** presentada aparece en un elemento 'Cápsula_6' de la Lista_Otras_Prestaciones, se trata con total normalidad y sin afectación alguna al Control del **aforo**.
2) Si el **NIS** de la **Acreditación** presentada no aparece en un elemento 'Cápsula_6' (o si tal Lista no está declarada) se procesa normalmente tal **Acreditación**, y si el paso se formaliza se indica (internamente dado que se trata de la misma electrónica) al Terminal A, de manera que el Terminal A decrementa en una unidad el contenido del subcampo 'CA' del parámetro 'CONTADOR AFORO', por lo que tal contador quedará con un valor inferior al indicado en el parámetro 'LÍMITE AFORO' y, por tanto, podrá aceptar nuevas entradas al recinto.

21.6.3 salida de usuarios (Terminal C)

El Terminal C controla el sentido de salida del recinto, por lo que la secuencia lógica ocurre de la siguiente manera:

1) Si el **NIS** de la **Acreditación** presentada aparece en un elemento 'Cápsula_6' de la Lista_Otras_Prestaciones, se trata con total normalidad y sin afectación alguna al Control del **aforo**.
2) Si el **NIS** de la **Acreditación** presentada no aparece en un elemento 'Cápsula_6' (o si tal Lista no está declarada) se procesa normalmente tal **Acreditación**, y si el paso se formaliza se indica al Terminal A por medio de la conexión de la Salida S2 del Terminal C a la Entrada E2 del Terminal A, de manera que el Terminal A decrementa en una unidad el contenido del subcampo 'CA' del parámetro 'CONTADOR AFORO', por lo que tal contador quedará con un valor inferior al indicado en el parámetro 'LÍMITE AFORO' y, por tanto, podrá aceptar nuevas entradas al recinto.

NOTAS:

(1)
La utilización del recurso de excepción al Control del **aforo** implica que tanto en el Terminal A como en el B (e incluso en el C si se utiliza) el contenido de los elementos 'Cápsula_6' en la Lista_Otras_Prestaciones debe ser el mismo, dado que en caso contrario el control no se realizará correctamente.

(2)
El valor declarado para la Entrada E2 en el parámetro 'LATENCIA ENTRADAS' debe ser 0, quedando por tanto tal Entrada sin otro uso posible.

21.7 Señalización

La apertura y cierre del contenedor (si lo hay) podría significar un acto de **"tamper"**), por lo cual se generan, respectivamente, los **marcajes especiales** *46 "vandalismo en el Terminal Modular"* y *94 Final vandalismo en el Terminal Modular"*. Como consideración importante, hay que tener en cuenta que si se desea un aviso acústico de tal situación de alerta, éste sólo se podrá efectuar desde el Cabezal que forme parte del Terminal con ID = N (utilizando el correspondiente parámetro 'MÁSCARA AVISOS SONOROS').

En el caso de que se utilice el módulo de alimentación ininterrumpida modelo FA/SAI-1, la señalización para indicar tanto el inicio de la situación de alimentación desde la batería como el final de tal situación se generan, respectivamente, los **marcajes especiales** *13 "alimentación en precario"* y *12 Final "alimentación en precario"*. Esta señalización se puede obtener del Terminal con ID = N, siempre que haya sido instalado mediante la función *28 Instalar_Terminal* o la macrofunción *129 Instalar_fS=4* con el bit 'b27' del parámetro 'IM' activado

código	título	relaciones
QAN-22	Complemento al Control de Intrusión: - Terminales *Especiales* modelos DEF-PCTn - Terminales *Especiales* modelo QScope - API-QSCOPE	- MRT019 : capítulo 3 (*Direcciones 83 a 86*) - MRT019 : capítulo 5 (función *28* / macrofunción *129* - MRT019 : capítulo 6 (Nota de Aplicación QAN-17) (Nota de Aplicación QAN-20) - MRT019 : Anexo F - MRT019 : Anexo H - MRT024 - MIP-PCTn

El Control de Intrusión de Qontinuum está formado por **Paneles de Intrusión** (los cuales lo son de manera nativa) modelo DEF-3003 y modelo DEF-3003/L, y/o por los obsoletos Terminales *Modulares* modelo MIF-709 (los cuales pueden operar como **Panel tipo mixto**) y/o por los Terminales *Modulares* modelo DEF-3001(los cuales pueden operar como **Panel tipo mixto o Panel tipo interno**), pero el mayor rendimiento del Control de Intrusión se puede obtener cuando se complementa con otros tipos de equipos que flexibilizan la típica centralización tanto de señales como de actuaciones e, incluso, de imágenes.

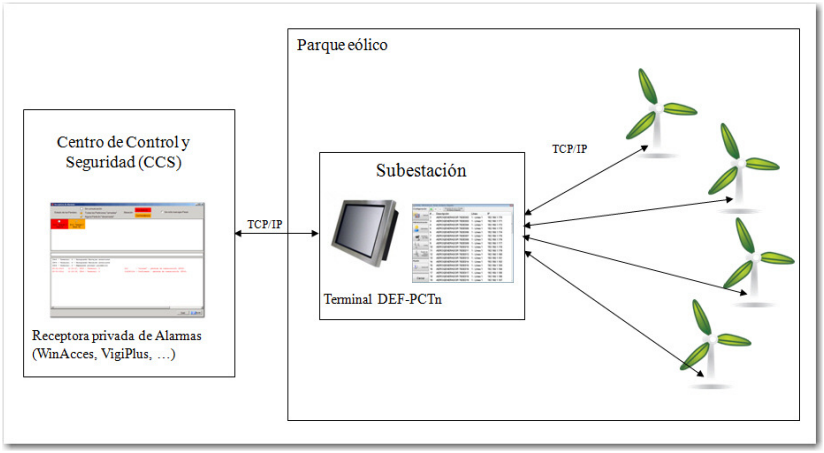
22.1 Primer complemento

En circunstancias habituales, los Paneles de Qontinuum ejercen un control "local" de las señales y permiten, bajo estrictas condiciones, actuaciones de los usuarios también en "local" (como el "desarmado" y/o el "armado" mediante las pertinentes **Acreditaciones**).

En circunstancias habituales, la receptora de la Instalación, normalmente situada en el Centro de Control y Seguridad (CCS), recibe (o recoge) sistemáticamente y en tiempo real las señales producidas en los Paneles, y permite a los Operadores de tal programa realizar actuaciones (telecontrol) de todo tipo, lo cual les otorga total capacidad de gestión sobre dichos Paneles.

Sin embargo, puede ocurrir que algunas Instalaciones, en razón de sus circunstancias, requieran de una cierta flexibilidad tanto en la recepción de las señales como, y muy especialmente, en la ejecución de las actuaciones, apareciendo entonce una situación "intermedia" que debe ser satisfecha.

Como ejemplo, un caso paradigmático de tal necesidad lo encontramos en los Parques eólicos, en los cuales el concepto "local" se aplica al Panel situado en cada aerogenerador mientras que el concepto "remoto" se aplica a la receptora situada en el CCS. En cada Parque eólico existe un edificio (normalmente llamado subestación) en la que se pretende que el personal pueda monitorizar, en tiempo real, la situación de todos y cada uno de los Paneles, y hacerlo con total independencia del CCS, de manera que si hay que "desarmar" o hay que "armar" uno o todos los Paneles pueda hacerse de inmediato y desde la subestación (tal y como muestra el siguiente esquema):



Los Terminales *Especiales* modelos DEF-PCTn[(1)] son los que aportan la solución al problema planteado por la existencia de la situación "intermedia", y lo hacen en base a proporcionar la capacidad de monitorización del estado de los Paneles y la capacidad de actuación sobre ellos, pero sin que tal control "intermedio" resulte en detrimento de las funcionalidades de la receptora (situada en el CCS) dado que sigue siendo desde tal programa **OEM** desde donde se configuran y activan (y también desactivan) los Terminales *Especiales* modelos DEF-PCTn.

Aunque los Terminales *Especiales* modelos DEF-PCTn disponen de capacidad para atender a las comunicaciones con un programa **OEM**, lo único que se puede hacer desde éste es la "preconfiguración" (necesaria en todos los Terminales de Qontinuum) y la gestión de la relación de Operadores autorizados (mediante los elementos 'Cápsula_3' en la Lista_Otras_Operaciones expuesta en el capítulo 3), de manera que cuando los Operadores presenten su **Acreditación** al Terminal *Especial* modelos DEF-PCTn, éste les permita operar. Para tal tipo de Terminal, los programas **OEM** sólo tienen disponible el uso de las siguientes funciones de la API básica del **sistema CONACC** (el ID siempre debe ser = 1):

1 Petición_Status (en el campo LNG siempre retorna 0);
16 Leer_RAM (sólo sirve para la Lista_Otras_Prestaciones)
17 Grabar_RAM (sólo sirve para la Lista_Otras_Prestaciones)
18 Reset
19 Leer_FW (valores 0 y 8 en el Byte alto de ADDR)
20 Leer_EEPROM
21 Grabar_EEPROM
25 Leer_Reloj
26 Grabar_Reloj
27 Cambiar_Password
28 Instalar_Terminal
29 Info_Instalación
32 Info_Terminal
33 Reconfigurar_Terminal (tipo A)
33 Reconfigurar_elementoIP (tipo B)
33 Reconfigurar_capaVirGO (tipo C)
40 Stat_Listas/Tablas (sólo puede retornar los valores 00, 10, 50 y 53)
43 Update_Listas (valor 4 en el Byte bajo de ADDR)
44 Delete_Listas (valor 4 en el Byte bajo de ADDR)

Ante cualquier otra función y/o macrofunción se retornará el código de estado 01.

Los programas **OEM** que quieran implementar comunicaciones con los Terminales *Especiales* modelos DEF-PCTn deben tener en cuenta lo siguiente:

1) cada uno de tal tipo de Terminal *Especial* debe ser tratado como un **elemento IP**, por lo que las comunicaciones son las estándar del **sistema CONACC** (utilización de la torre de protocolos TCP/IP/Ethernet);
2) por cada Terminal hay que asignar y usar un Puerto 'socket' con la dirección IP que se le haya dado (consta en el elemento **TInGW** incorporado en el Terminal);
3) todos los datos que afectan a tal tipo de comunicaciones (puerto TCP, dirección IP, máscara de subred y puerta de enlace) pueden ser modificados por los medios típicos del **sistema CONACC** (función *33 Reconfigurar_elementoIP*);
4) la Lista_Otras_Prestaciones sólo debe ser definida para contener a los elementos 'Cápsula_3' (funciones *16 Leer_RAM* y *17 Grabar_RAM*);
5) si se quiere que las descripciones identificadoras(2) de cada Panel así como de las Particiones, de las Entradas y de las Salidas que se vayan a usar se muestren en la monitorización, hay que cargarlas previamente en los Paneles (funciones *21 Grabar_EEPROM* y *20 Leer_EEPROM*) siguiendo las pautas indicadas en el Anexo H;
6) todos los **marcajes Panel** que se generan como consecuencia del uso de los Terminales *Especiales* modelos DEF-PCTn se consolidan en los oportunos Terminales *Modulares* que integran un Panel, por lo que los programas **OEM** no deben pretender encontrarlos en la memoria de los Terminales *Especiales* modelos DEF-PCTn.

El 'código Producto' del Terminal *Especial* modelos DEF-PCTn es 261, y el FW incorporado tiene asignado el nombre "MoniPAi" (Monitor de Paneles de Alarmas integrados) dado que está diseñado para ser implementado, en el futuro, en otras plataformas.

22.1.1 Otras características

Una primera característica notable que aporta el FW "MoniPAi" es la capacidad de mostrar en la pantalla del Terminal *Especial* modelos DEF-PCTn (además del estado y circunstancias de las Particiones y de las Entradas y de las Salidas asociadas), las imágenes, en "tiempo real", de hasta tres cámaras(3).

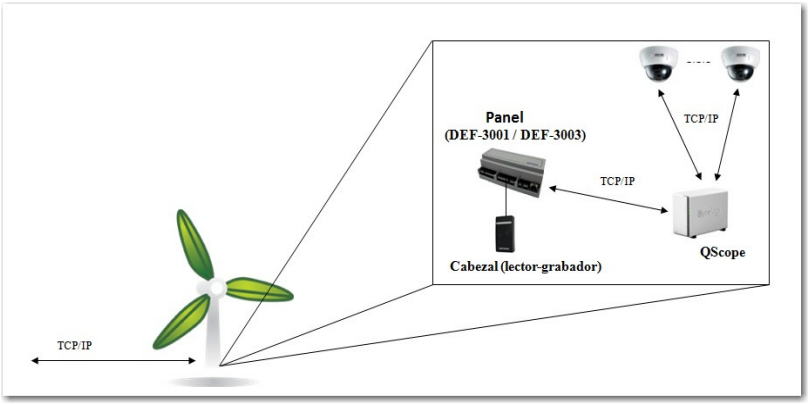
Una segunda característica notable que se aporta es la de poder presentar, también en "tiempo real", las imágenes que genera una cámara que haya sido vinculada (en la configuración del FW "MoniPAi") a una Entrada, de manera que, cuando se produzca un cambio de estado en tal Entrada, "MoniPAi" conmuta la presentación que tuviera en pantalla a la de las imágenes generadas por tal cámara. Esta característica puede ser aplicada en una relación del tipo {Entrada <–> # cámara}(4), de manera que al producirse tal relación se muestran las oportunas imágenes, y al acabar la visualización (por acción del Operador o por agotamiento del tiempo máximo previsto), el FW regresa a la situación en la que estuviera al producirse tal relación.

22.2 Segundo complemento

En circunstancia habituales, y tomando como paradigmático el mismo caso de un Parque eólico, se parte de la base de que es necesaria la existencia de imágenes retrospectivas, por lo que todas las imágenes generadas por todas las cámaras situadas en todos los aerogeneradores deben llegar al grabador (o batería de grabadores) situados en la subestación del Parque, lo cual implica que necesariamente haya un uso muy importante del ancho de banda disponible en la red del Parque. Tal cosa no representa ninguna limitación si la instalación dispone de suficiente ancho de banda, pero puede llegar a ser un problema si no fuera el caso dado que las imágenes tendrían que perder resolución y espaciarse en el tiempo su generación y recogida, con la consiguiente pérdida de eficacia en los casos en los que fuera necesario un análisis de las imágenes (situaciones de alarma, auditorías, etc.).

En circunstancias habituales, y ante la necesidad de efectuar desde el programa **OEM** un análisis (cuya necesidad siempre será posterior a las imágenes grabadas), y dado que la grabación se realiza de todas las imágenes que llegan desde todas las cámaras, no existe otra manera de seleccionar imágenes que ir haciendo aproximaciones basadas en el momento de la grabación al compararlo con el momento de, por ejemplo, una alarma que se haya producido, resultando todo ello en un proceso laborioso y, por tanto, lento.

Los Terminales *Especiales* modelo QScope tienen aplicada la funcionalidad de actuar como grabadores de imágenes, siendo el resultado de aplicar el "principio de localidad" a los aerogeneradores dado que es en ellos donde realmente se generan las imágenes, por lo que éstas son directamente grabadas (sin tener que circular por la red del Parque) y quedan almacenadas "localmente" (aunque nada priva que también pudieran tomarse, incluso en tiempo real y mediante la API-QSCOPE, desde el CCS si se quisiera consolidarlas allí):



Además, y a diferencia de cuando se usan grabadores habituales, al usar grabadores de imágenes modelo QScope se dispone de la intercomunicación de éstos con los **Paneles tipo internos** integrados en los Terminales *Modulares* modelo DEF-3001 o con los **Paneles de Intrusión** modelo DEF-3003 y modelo DEF-3003/L, lo cual posibilita que ante cualquier situación crítica(5) los grabadores de imágenes modelo QScope agrupen todas las imágenes vinculadas a la situación crítica(5) y las dejen directamente disponibles al programa **OEM**, evitando así tediosas búsquedas posteriores.

Aunque los grabadores de imágenes modelo QScope disponen de capacidad para atender a las comunicaciones con un programa **OEM**, lo único que se puede hacer desde tal programa es la "preconfiguración" (necesaria en todos los Terminales de Qontinuum) así como obtener (por medio de la API-QSCOPE) el acceso a las imágenes que fueron almacenadas al ser recibidas de las cámaras conectadas.

Para los grabadores de imágenes modelo QScope, los programas **OEM** sólo tienen disponible el uso de las siguientes funciones de la API básica del **sistema CONACC** (el ID siempre debe ser = 1):

1 Petición_Status (en el campo LNG siempre retorna 0);
18 Reset
19 Leer_FW (valor 0 en el Byte alto de ADDR)
20 Leer_EEPROM
21 Grabar_EEPROM
25 Leer_Reloj
27 Cambiar_Password
28 Instalar_Terminal
29 Info_Instalación
32 Info_Terminal
33 Reconfigurar_elementoIP (tipo B)

Ante cualquier otra función y/o macrofunción se retornará el código de estado 01.

Los programas **OEM** que quieran implementar comunicaciones con los grabadores de imágenes modelo QScope deben tener en cuenta lo siguiente:

1) cada uno de tal tipo de Terminal *Especial* debe ser tratado como un **elemento IP**, por lo que las comunicaciones son las estándar del **sistema CONACC** (utilización de la torre de protocolos TCP/IP/Ethernet);
2) por cada Terminal hay que asignar y usar un Puerto 'socket' con la dirección IP que se le haya dado (consta en el elemento **TlnGW** situado en el Terminal);
3) todos los datos que afectan a tal tipo de comunicaciones (puerto TCP, dirección IP, máscara de subred y puerta de enlace) pueden ser modificados por los medios típicos del **sistema CONACC** (función *33 Reconfigurar_elementoIP*);
4) si se quiere que las descripciones identificadoras(2) de cada grabador de imágenes así como de las cámaras que tenga conectadas se muestren en la monitorización, hay que cargarlas en cada Terminal *Especial* (funciones *20 Leer_EEPROM* y *21 Grabar_EEPROM*) siguiendo las pautas indicadas en el Anexo H;
5) la actualización del reloj de cada grabador de imágenes modelo QScope es responsabilidad del correspondiente **Panel tipo interno**, por lo que los programas **OEM** no tienen potestad para hacerlo.

El 'código Producto' del Terminal *Especial* modelo QScope es 201.

22.2.1 Consideraciones

Una vez que un grabador de imágenes modelo QScope haya arrancado (por conexión a la alimentación eléctrica), verifica la existencia y validez del elemento **TInGW** que debe tener conectado, de manera que si éste no existe o no es válido el FW genera un **marcaje Panel** con CEP=2900h y queda en un bucle[6] de reintentos sistemáticos de lectura del elemento **TInGW**, no generando ningún otro marcaje hasta que lo consiga, en cuyo momento intentará comunicar con las cámaras correspondientes, generando por cada cámara a la que se deba conectar un **marcaje Panel** con CEP=280Nh[7] si puede hacerlo y un **marcaje Panel** con CEP=290Nh[7] si no puede, al igual que también genera un **marcaje Panel** con CEP=290Nh[7] cuando, en cualquier momento, pierda la comunicación con la cámara, no generando ningún otro marcaje en los reintentos de conexión consecutivos fallidos hasta que consiga reconectar, en cuyo momento genera un **marcaje Panel** con CEP=280Nh[7]. De manera periódica, el FW verifica que el elemento **TInGW** siga estando accesible y siga siendo el mismo, y si no se da el caso genera un **marcaje Panel** con CEP=2900h pero sigue operando normalmente[8].

Cada vez que un grabador de imágenes modelo QScope arranca su funcionamiento lógico debido a un 'Reset' forzado por comunicaciones, antes de iniciarlo genera un **marcaje Panel** con CEP=2500h[7] para que posteriormente, cuando este marcaje sea recogido por el Terminal *Modular* que integre al Panel, y al llegar finalmente al programa **OEM** que haga de receptora, se pueda constatar que hubo un paro en la recogida y grabación de imágenes. Una vez el grabador de imágenes QScope haya arrancado de nuevo, se produce el proceso indicado en el párrafo anterior.

Cada vez que un **Panel tipo interno** arranca su funcionamiento lógico (sea por conexión a la alimentación eléctrica o sea debido a un 'Reset' forzado localmente o por comunicaciones), y además de ejecutar una serie de acciones internas, intenta conectar con el grabador de imágenes modelo QScope cuya dirección IP consta en el elemento **TInGW** incorporado; si lo consigue genera un **marcaje Panel** con CEP=2300h, mientras que si no lo consigue genera un **marcaje Panel** con CEP=2400h y sigue intentando, de manera sistemática pero sin generar nuevos marcajes, conseguir la conexión, y cuando finalmente lo consigue genera un **marcaje Panel** con CEP=2300h. También genera un **marcaje Panel** con CEP=2400h cuando se agotan los intentos de 'Heart Beat' (establecidos en **TInGW**), lo cual puede significar una desconexión o problemas relacionados con el elemento **TInGW** en el grabador de imágenes modelo QScope (explicados en el primer párrafo).

Cada vez que un **Panel tipo interno** afronta una situación crítica[5], actúa en consecuencia y genera los oportunos **marcajes Panel** (ver el Anexo F), pero también ordena (mediante una 'baliza'[9]) al grabador de imágenes modelo QScope que debe generar un racimo de imágenes tomadas de la(s) cámara(s) indicada(s) en la orden así como durante cuanto tiempo después y, lo que puede ser más importante, desde cuanto tiempo antes[10], de forma que el racimo lo formen suficientes imágenes significativas como para facilitar el posterior análisis. Como consecuencia inmediata de enviar tal orden, el FW del **Panel tipo interno** genera un **marcaje Panel** con CEP=2A00h[9].

En el momento de generarse una situación crítica[5] puede darse el caso de que el grabador de imágenes modelo QScope involucrado no esté operativo o de que si que lo esté pero presente algún problema funcional, o que todo el proceso resulte correcto o que se produzcan problemas con alguna cámara, etc., pero en todos los casos, los correspondientes **marcajes Panel** alusivos a tales situaciones se generan indicando la misma 'baliza', de manera que el programa **OEM** pueda agruparlos convenientemente para lograr un mejor tratamiento posterior.

En consecuencia del cumplimiento total (A) o del incumplimiento total (B) o del cumplimiento parcial (C) por parte del grabador de imágenes modelo QScope de la orden de 'baliza', se genera uno o varios **marcaje Panel** con el CEP correspondiente, los cuales se convierten en secuencias simples (dentro del global de los **marcajes Panel**) las cuales serán recogidas por el **Panel tipo interno** y transmitidos finalmente a la receptora de manera que el programa **OEM** pueda facilitar al Operador actuar en consecuencia.

(A) Secuencia simple de **marcajes Panel** en condiciones de cumplimento total:

valor en CEP :	Descripción :
el que corresponda a la situación crítica(5)	el valor en el campo 'Fecha' del **marcaje Panel** corresponde a la 'baliza' enviada a QScope
2A00h	orden de 'baliza' enviada a QScope
260Nh(11)	orden de 'baliza' cumplida por QScope (racimo creado y completado)

- implica que el grabador de imágenes modelo QScope ha generado el racimo y éste está disponible para ser accedido por medio de la API-QSCOPE(el FW de QScope habrá generado tantos **marcajes Panel** con CEP=260Nh como cámaras se hayan indicado en la orden de 'baliza', lo cual tiene sólo el sentido de aportar más información sobre la composición del racimo).

(B) Secuencia simple de **marcajes Panel** en condiciones de incumplimiento total:

valor en CEP :	Descripción :
el que corresponda a la situación crítica(5)	el valor en el campo 'Fecha' del **marcaje Panel** corresponde a la 'baliza' enviada a QScope
2A00h	orden de 'baliza' enviada a QScope
2400h	no hay comunicación con QScope

- implica que el grabador de imágenes modelo QScope no comunica, por lo que no se ha creado el correspondiente racimo de imágenes, aunque si QScope estuviera funcionando recogiendo imágenes de las cámaras se podrían recuperar posteriormente las imágenes por el método habitual de búsqueda por fechas;

valor en CEP :	Descripción :
el que corresponda a la situación crítica[5]	el valor en el campo 'Fecha' del **marcaje Panel** corresponde a la 'baliza' enviada a QScope
2A00h	orden de 'baliza' enviada a QScope
2700h	orden de 'baliza' no cumplida por QScope (racimo no creado)

- el valor 2700h en CEP implica que el grabador de imágenes modelo QScope comunica, pero no ha podido generar el racimo de imágenes previsto al no disponer de espacio libre en el disco o si fuera el caso de que tal 'baliza' existiera previamente (se trataría de un error a ser comunicado de inmediato a Qontinuum), por lo que el programa **OEM** debe asumir que tal racimo no existe en QScope;

(C) Secuencia simple de **marcajes Panel** en condiciones de cumplimento parcial:

valor en CEP :	Descripción :
el que corresponda a la situación crítica[5]	el valor en el campo 'Fecha' del **marcaje Panel** corresponde a la 'baliza' enviada a QScope
2A00h	orden de 'baliza' enviada a QScope
270Nh	orden de 'baliza' no consolidada por QScope (racimo no completado)[11]

- los valores 270Nh en CEP implican que el racimo existe pero que no se ha formado con las imágenes del momento de la orden y las posteriores (aunque puedan existir imágenes anteriores) correspondientes a la cámara indicada, por lo que tal racimo no está completo.

(D) Ejemplo de la secuencia de **marcajes Panel** que se habrá producido como consecuencia de que el **Panel tipo interno** haya ordenado a QScope (pasándole una 'baliza') la creación de un racimo utilizando imágenes de dos cámaras, y mientras que la cámara #1 está operativa la cámara #2 no lo está, por lo que la imagen del momento de recibir la orden 'de baliza' y las posteriores de tal cámara no pueden ser consolidadas por QScope en el racimo dado que no se están recibiendo, pero las que puedan existir anteriores a tal orden serán consolidadas sólo si la desconexión de tal cámara se produjo dentro del tiempo declarado en el parámetro 'TaC' (ver el subcapítulo 22.3); si la desconexión se produjo antes del límite impuesto por tal parámetro, entonces no se consolida ninguna imagen en el racimo:

valor en CEP :	Descripción :
el que corresponda a la situación crítica(5)	el valor en el campo 'Fecha' del **marcaje Panel** corresponde a la 'baliza' enviada a QScope
2A00h	orden de 'baliza' enviada a QScope
2601h	orden de 'baliza' cumplida parcialmente por QScope : racimo creado y consolidado para la cámara #1
2702h	orden de 'baliza' no consolidada por QScope : (racimo no completado para la cámara #2)

- en los cuatro marcajes se repite el valor de la 'baliza' (valor **crono** situado en el campo 'Fecha').

22.3 Tercer complemento

La API-QSCOPE ha sido diseñada para facilitar a los programas **OEM** las operativas adecuadas a la funcionalidad de los Terminales *Especiales* modelo QScope, por lo cual resulta ser una API pública de propósito específico y uso restringido.

Se trata de una "capa de abstracción" que queda situada entre el programa de aplicación y la API-CONACC (se trata de la API de nivel medio CONALL.DLL, la cual queda por encima del **driver** Q2_DRV32.DLL), de manera que resulte más sencillo para el **OEM** implementar las comunicaciones necesarias entre sus aplicaciones y los Terminales *Especiales* modelo QScope.

La API-QSCOPE también es utilizada por los Terminales *Especiales* modelos DEF-PCTn (Versión de FW 01.01.00 y posteriores) para obtener en tiempo real las imágenes de hasta tres cámaras y mostrarlas de manera concurrente en la opción de monitorización oportuna proporcionada por el FW “MoniPAi”.

Dada la funcionalidad de los Terminales *Especiales* modelo QScope como grabadores de imágenes, y dado el tipo de entorno en el que tales equipos probablemente se instalen, es muy lógico pensar que se pretenda acceder a las imágenes desde más de un programa **OEM** (todos los cuales deben utilizar la API-QSCOPE), por lo que el FW admite hasta un máximo de cinco sesiones de comunicación abiertas concurrentemente, pudiendo ser una de ellas la conexión que se establezca desde un Terminal *Especial* modelo DEF-PCTn), de manera que si se pretende establecer una sexta sesión de comunicación, el FW retorna un código de estado *112 Límite de conexiones excedido*.

Los programas **OEM** deberán tener en cuenta que el FW de los Terminales *Especiales* modelo QScope sólo acepta todas las funciones proporcionadas por la API-QSCOPE si el Operador implicado en el establecimiento de la **sesión segura** de comunicaciones es el nª 1 (ver el parámetro ‘NO’ en la función *0 Ini_PORT* en la Revisión Z o posterior del capítulo 5 del documento MRT019). Por tanto, sería conveniente que el programa **OEM** protegiera a la Instalación de operativas no deseables que pudieran comprometer el buen funcionamiento del sistema, para lo cual debería establecer las **sesiones seguras** de comunicación utilizando en el parámetro ‘NO’ a los valores 2 ó 3, mientras que debería utilizar el valor 1 para aquellos Operadores a los que quiera permitir la ejecución de las funciones:

ReconfigureGw()	(API-CONACC)
StaticReconfigureQscopeCams()	(API-CONACC)
InstallTerm()	(API-CONACC)
DeleteCluster()	(API-QSCOPE)
DeleteCamCluster()	(API-QSCOPE)

al ser éstas de uso potencialmente dañino para la integridad lógica del sistema si se ejecutan libremente por parte de los varios posibles Operadores.

Como última medida de seguridad, el FW de QScope rechazará las antedichas funciones retornando un código de estado *01 Operación no implementada* si se pretende ejecutarlas cuando las **sesiones seguras** de comunicación hayan sido establecidas con el valor 2 ó 3 en el parámetro ‘NO’ de la función *0 Ini_PORT*.

La información completa sobre la API-QSCOPE hay que verla en el documento MRT024 y en la documentación explícita de ayuda de la propia API (documento Qscope.xml).

NOTAS:

(1)

Una explicación detallada sobre la funcionalidad y prestaciones de los Terminales *Especiales* modelo DEF-PCTn puede verse en el documento MIP-PCTn.

(2)

A partir de la Versión de FW 08.06.02 para los Terminales *Modulares* modelo MIF-709 y de la Versión de FW 09.04.06 para los Terminales *Modulares* modelo DEF-3001 y de la Versión de FW 01.00.00 para los Terminales *Especiales* modelo QScope y de la Versión de FW 10.00.00 para los **Paneles de Intrusión** modelo DEF-3003 y modelo DEF-3003/L, los programas **OEM** pueden trasladar tales descripciones a la memoria de dichos Terminales, de manera que cuando el Terminal *Especial* modelos DEF-PCTn comunique con los Paneles y/o con el Terminal *Especial* modelo QScope tome tales descripciones para mostrarlas en la pantalla de monitorización; para ello, el programa **OEM** debe utilizar la función *21 Grabar_EEPROM* para almacenar (en la memoria EEPROM de los Paneles y de los Terminales que constituyen los grabadores de imágenes) la información correspondiente a las antedichas descripciones.

Para minimizar la transferencia de las descripciones identificadoras desde los Terminales *Modulares* modelo DEF-3001 y/o desde los **Paneles de Intrusión** modelo DEF-3003 y modelo DEF-3003/L y desde los Terminales *Especiales* modelo QScope hacia los Terminales *Especiales* modelo DEF-PCTn, existe el campo serialización (dirección absoluta 128) en los mapas de memoria auxiliares (ver el Anexo H).

El programa **OEM** debería incorporar un mecanismo de serialización (por ejemplo, empezando en el valor 1) que deberá incrementar cada vez que actualice una o varias descripciones y/o cada vez que modifique la configuración de Entradas y/o Particiones (al llegar al valor 255 deberá volver a 1) con la intención de que el FW del Terminal *Especial* modelos DEF-PCTn pueda averiguar que se han actualizado las descripciones, de manera que las tomará por completo de la memoria EEPROM del Terminal *Modular* modelo DEF-3001 o del **Panel de Intrusión** modelo DEF-3003 o modelo DEF-3003/L o del Terminal *Especial* modelo QScope, actualizandolas en su propia memoria (desde donde las tomará mientras no haya nuevos cambios). Gracias a este mecanismo se reduce en gran manera la necesidad de transferir tales descripciones de manera sistemática por la red.

Cuando el programa **OEM** quiera modificar las descripciones, es muy recomendable que primero las actualice y, a continuación, cambie el valor contenido en la dirección absoluta 128.

Cuando el valor sea diferente de 0, el FW del Terminal *Especial* modelos DEF-PCTn cargará las descripciones de manera automática siempre al arrancar el funcionamiento (por ejemplo, después de un 'Reset') y en la primera comunicación que ocurra a cada hora transcurrida, quedando el valor 0 reservado para uso del FW "MoniPAi".

Este mecanismo global también es aplicado por el Terminal *Especial* modelos DEF-PCTn para cargar de nuevo la configuración correspondiente a las Particiones, a las Entradas y a la Salidas correspondientes al Terminal por si se hubiera realizado algún cambio desde el programa **OEM**.

(3)

Si el grabador de imágenes utilizado es un Terminal *Especial* modelo QScope, las cámaras son hasta tres de las hasta siete que pueden estar conectadas, y tales imágenes se toman directamente de las cámaras, mientras que si el grabador de imágenes es de otro fabricante las hasta tres cámaras son aquellas que están conectadas a tal grabador, y las imágenes se toman del grabador.

(4)
Una aplicación práctica de tal aportación se daría, por ejemplo, en el caso de querer que la apertura de la puerta de acceso pudiera ser visualizada por el personal de la subestación, de manera que, parametrizando en el Terminal *Especial* modelo DEF-PCTn la relación entre la Entrada (del **Panel tipo interno**) a la que se conecte el sensor de la puerta y la cámara que cubra tal puerta, en el monitor aparecerían las oportunas imágenes.

(5)
Situación crítica es aquella que se produce como consecuencia inmediata de una circunstancia ("desarmado", "armado", accesos, alarmas, etc.) que el **Panel tipo interno** identifica y controla (generando los correspondientes **marcaje Panel**), y de la cual se quiere disponer de un racimo de imágenes construido alrededor de una 'baliza' para agilizar el acceso posterior.
En otras palabras: toda situación crítica se identifica por un código CE=113 más un código CEP (ver el Anexo D) más un número de cámara (o cámaras), por lo que, en su definición, no deben existir registros duplicados para una misma situación crítica (si los hubiera, el FW de los **Paneles tipo internos** sólo consideran al primer registro de la tabla e ignoran a los posibles duplicados).
El programa **OEM** debe facilitar la definición de las situaciones críticas así como también debe facilitar su selección por parte del Operador del programa (ver el Anexo D).
A título de ejemplo, los programas de Qontinuum para el Control de Accesos físicos WinAcces y WinAcces+ (ambos incorporan la receptora para los Paneles) disponen de una opción que visualiza en una ventana todos aquellos eventos que constan marcados como seleccionables para formar parte de la definición de situaciones críticas. Tales eventos son los específicos más alguno que otro con un CE no especificado como **marcaje Panel** pero que puede ser de uso conveniente (como los CE=34 y CE=88). Los antedichos programas de Qontinuum toman tal información de un archivo que forma parte del sistema multi idioma y los muestran para que el Operador seleccione aquellos que considere oportunos para ser relacionados con una o con varias cámaras. En resumen, los eventos seleccionados deberían ser sólo aquellos que, cuando se produzcan, vinculen a una o varias cámaras.

(6)
En un proceso de arranque, y durante la ejecución del bucle de reintentos sistemáticos de lectura del elemento **TInGW**, el grabador de imágenes resulta del todo inoperativo, de manera que, al no poder comunicar con ninguna cámara, no graba imágenes, y al no poder conocer cual es su propia dirección IP tampoco puede atender a los intentos de establecer comunicación realizados por el **Panel tipo interno**, el cual, ante tal situación, genera un **marcaje Panel** con CEP=2400h que llegará al programa de receptora del CCS (de manera que se puedan tomar las medidas correctivas oportunas).

(7)
El valor de N (1 a 7) corresponderá al de la cámara en concreto, siendo guardados tales marcajes en la memoria del grabador de imágenes modelo QScope y recogidos (cuando corresponda) por el **Panel tipo interno** cuando éste conozca tal existencia como consecuencia de uno de los procesos de control ejecutados sistemáticamente para saber si la comunicación se mantiene abierta.

(8)
El grabador de imágenes modelo QScope sigue operando normalmente aunque haya dejado de reconocer al elemento **TInGW** (porque éste haya sido quitado), pero ante la situación de 'Reset' por comunicaciones o de paro/marcha por alimentación, la situación pasa a ser la expuesta para el arranque(6), mientras que si el elemento **TInGW** original hubiera sido cambiado por otro, y también en el arranque(6), todo pasaría a funcionar normalmente en base a la información contenida en este nuevo elemento **TInGW**.

(9)
La ‘baliza’ aparece contenida en el campo ‘Fecha’ de los marcajes, y en puridad corresponde al **crono** del momento en el que el **Panel tipo interno** detectó la situación crítica[5].

(10)
Tal cosa resulta posible dada la singular manera que utiliza el FW del Terminal *Especial* modelo QScope para almacenar las imágenes a medida que las recibe de las cámaras conectadas, de manera que fácil y rápidamente las incluye en el racimo correspondiente a la ‘baliza’.

(11) El valor de N (1 a 7) corresponderá al de cada una de las cámaras que estén involucradas en la orden ‘baliza’ con independencia de si en ese momento están o no operativas (dado que tal control lo efectúa el FW de QScope por la vía de un **marcaje Panel** con CEP=290Nh[6]).

ESTA PÁGINA HA SIDO DEJADA EN BLANCO INTENCIONADAMENTE

código	título	relaciones
QAN-23	Terminales de la Familia DEF operando en formato **fS=5**	- MRT019 : capítulo 3 (*Direcciones 8 y 91*) - Q2_UTIL : Versión 8.01 y >>

La Familia DEF es específica para operar con **Acreditaciones** dotadas con estructura **fS=4**. Sin embargo, y de manera excepcional, a partir de la Versión 09.15.00 del FW para los Terminales de la Familia DEF, resulta posible instalar y tratar las **Acreditaciones** en formato f**S=5**, esto es leyendo sólo el número de serie completo de la **Acreditación** (la otra posibilidad existente hasta la aparición de tal Versión de FW hay que verla en la Nota de Aplicación QAN-08).

La única razón justificable para aceptar la disminución de prestaciones que representa no operar en formato **fS=4** consiste en querer iniciar el funcionamiento de la Instalación sin requerir o sin utilizar la infraestructura necesaria para el formato **fS=4** (por ejemplo, el Kit DEF-500) y sin, por tanto, la responsabilidad de tener que acometer la **Prepersonalización** y la **Personalización** de las **Acreditaciones** 'DESFire'.

El formato **fS=5** tiene su razón de ser en el interés que pudiera tener la Instalación en disponer en forma de **NIS** la totalidad del UID de las **Acreditaciones** 'DESFire' (dado que tal número es irrepetible); tal cosa es así cuando se trata de **Acreditaciones** nativas, pero sin embargo el hecho de introducir la emulación de **Acreditaciones** vía NFC (Smartphone) genera necesariamente una numeración independiente que podría provocar, al unir ambas numeraciones, la existencia de duplicados en una misma Instalación; por esta razón el **NIS** en el formato **fS=5** es de 8 Bytes (siendo los UID de 7 Bytes), de manera que el **sistema CONACC** utiliza un mecanismo lógico para crear **NIS** realmente únicos contenidos en 56 bits (los 7 Bytes bajos).

La utilización del formato **fS=5** implica que el programa **OEM** deberá definir la **Lista_Blanca** o la **Lista_Negra** y/o la Lista_Especial y/o la Lista_Otras_Prestaciones indicando la no existencia del Byte extra llamado *marcador*, valorando por tanto a 0 el bit b7 del Nibble alto del parámetro 'TIPO DE LISTA' (ver la *Dirección 8* en el capítulo 3).

Una de las características de las Instalaciones que usan **Acreditaciones** dotadas con la estructura **fS=4** es el necesario uso concurrente de los **TInCap** (**TInCLA**, **TInACC**, etc.), de manera que una Instalación no puede funcionar con Terminales de la Familia DEF sin la presencia del elemento **TInCap** adecuado. Sin embargo, es posible forzar a los Terminales de la Familia DEF (usando el FW Versión 09.15.00 y posteriores y el programa de utilidad Q2_UTIL Versión 08.01.00 y posteriores) a operar en formato **fS=5**, para lo cual, y con independencia de la presencia o no de un **TInCap**, no hay que "preconfigurar" al Terminal utilizando la opción *Instalar_fS=4* del grupo *Funciones* del programa de utilidad Q2_UTIL sino utilizando la opción *Instalar_Terminal* del mismo grupo, en cuyo caso, y dado que se pretende efectuar la "preconfiguración" de un Terminal de la Familia DEF a un formato **fS=n** que no es el 4, el Operador de Q2_UTIL recibirá una advertencia al respecto. Con idéntica intención de informar al Operador, el programa **OEM** debería advertir al Operador de tal situación si la "preconfiguración" se realiza desde el programa **OEM** utilizando la función *28 Instalar_Terminal* en detrimento de la macrofunción *129 Instalar_fS=4* (ambas forman parte de la API de bajo nivel contenida en el **driver** Q2_DRV32.DLL), para lo cual deberá analizar el 'código Producto' (mediante la función *19 Leer_FW*) y deducir si el Terminal es de la Familia DEF (la relación entre las Familias y cada 'código Producto' aparece en la Ayuda para Q2_UTIL en la entrada : *código Producto*).

23.1 Coexistencia de Acreditaciones 'MIFARE' con Acreditaciones 'DESFire'

En las Instalaciones donde coexistan **Acreditaciones** 'MIFARE' y 'DESFire' y ambas deban ser usadas de manera simultánea, no es aceptable que para 'DESFire' se utilice el formato **fS=5** sino que debe hacerse con el formato **fS=3** para homogeneizar el tratamiento con las **Acreditaciones** 'MIFARE' (ver la Nota de Aplicación QAN-08).

23.2 Conversión de formato fS=5 a formato fS=4

Si en alguna Instalación donde se utilicen acreditaciones 'DESFire' dotadas con formato **fS=5** se quiere pasar a operar con formato **fS=4**, entonces se producirá una incompatibilidad formal de los **NIS** así construídos entre el formato **fS=5** y el formato **fS=4**, de manera que, cuando tal conversión sea necesaria(1), el programa **OEM** deberá eliminar todos los bits sobrantes (una manera de hacerlo sería pasar el valor de cada **NIS** en formato **fS=5** (por tanto, ocupando 7 Bytes) de decimal a hexadecimal, eliminar (por ejemplo) los 3 Bytes de mayor peso y pasar el nuevo valor hexadecimal a decimal); en el muy remoto caso de que se produzca un duplicado del valor obtenido (una posibilidad entre 2.147.483.647), el programa **OEM** debería advertirlo y forzar el cambio de una de las dos **Acreditaciones** por otra (por supuesto, con las comprobaciones de rigor para evitar un nuevo duplicado de **NIS**).

NOTAS:

(1)

La conversión no sería necesaria en el caso de que, aunque la Instalación quisiera pasar de formato **fS=5** a formato **fS=4**, no tuviera importancia alguna la información existente hasta el momento (numeración de las **Acreditaciones** 'DESFire' entregadas a los usuarios, marcajes recogidos, etc.), de manera que, en la práctica, resultaría en una puesta en marcha partiendo de cero y en la que, por tanto, la generación de los **NIS** podría ser por completo independiente de los UID.