Consorcio de Transporte Metropolitano
Campo de Gibraltar

PPT_CTMCG_02-2018_SUM_L

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES QUE HA DE REGIR EL CONTRATO DE SUMINISTRO E INSTALACIÓN DE SISTEMAS DE BILLETAJE PARA LA FLOTA URBANA DE AUTOBUSES INTEGRADOS CON EL CONSORCIO DE TRANSPORTE METROPOLITANO DEL CAMPO DE GIBRALTAR: ALGECIRAS, MEDIANTE PROCEDIMIENTO ABIERTO.

Índice

1 Antecedentes 2
2 La Red Tecnológica de Transporte 2
2.1 Arquitectura de la RTT 2
2.1.1 Red de usuarios. 3
2.1.2 Red de Cancelación. 3
2.1.3 Red de Ventas. 3
2.1.4 Red de Información. 3
2.1.5 Red de Operación 3
3 Alcance 4
4 Valoración técnica de las ofertas 4
4.1 Requisitos técnicos 5
4.1.1 Sistema de Ayuda a la Explotación (SAE) 5
4.1.2 Sistema de Información al Usuario (SIU) 6
4.1.3 Cajero de autoliquidación de recaudación 6
4.1.4 Soporte para títulos de transporte municipales 6
4.1.5 Cumplimiento de las Especificaciones Técnicas de la Red de Consorcios 7
4.1.6 Reparaciones y repuestos 7
4.1.7 Garantías 8
4.1.8 Integración con la librería de transportes 8
4.1.9 Transmisión en tiempo real 8
4.1.10 Telecarga 9
4.1.11 Creación de informes a demanda 9
4.2 Características técnicas 9
5 Organización 10
5.1 Suministrador y su Director de Integración 10
5.2 Director del Proyecto 11
6 Planificación 11
6.1 Prueba funcional 11
6.1.1 Pruebas a desarrollar 11
6.2 Cronograma de actuaciones 12
6.2.1 Especificaciones técnicas 12
6.2.2 Piloto operativo 13
6.2.3 Suministro e instalación 13
6.2.4 Puesta en servicio 13
7 Liquidación del suministro 14
7.1 Índices de calidad del contrato 14
7.2 Penalizaciones 14
7.3 Liquidación 14
8 Documentación 14
9 Formación 14
10 Confidencialidad de la información 15
11 ANEXOS: 15

1 Antecedentes

La Red de Consorcios de Transporte de Andalucía, en adelante RCTA, es la responsable de la implantación de los sistemas integrados del transporte público (SIT) que gestiona la movilidad de las nueve Áreas Metropolitanas de Andalucía.

El núcleo central sobre el que se vertebran todos los SIT del Transporte Público de Andalucía es la tarjeta de transporte, actualmente en un soporte Mifare Classic 1K.

Tras más de 10 años de implantación el soporte de la tarjeta de transporte va a evolucionar al modelo Desfire 4K EV2, lo que permitirá dotar a la Red de Transporte de los últimos avances tecnológicos de cara a ampliar las funcionalidades que los servicios de transporte ofrecen a los ciudadanos, creando una visión moderna y eficiente del Transporte Público de Andalucía.

En esta línea de renovación, se va a proceder a actualizar los sistemas de billetaje de la flota de transporte urbano para garantizar su compatibilidad con este nuevo soporte y las nuevas funcionalidades previstas.

2 La Red Tecnológica de Transporte

La explotación diaria del RCTA se apoya en una arquitectura TIC denominada Red Tecnológica de Transporte. Esta red, modela el comportamiento e integración de los diferentes elementos que forman parte de ella y define el modelo de comunicación e interconexión entre los mismos.

2.1 Arquitectura de la RTT

La RTT del RCTA, ver Ilustración 1, define un conjunto de redes interconectadas mediante interfaces de comunicación estandarizados, donde cada red puede contener varios tipos de elementos. Cada elemento debe cumplir con las normas establecidas en cada interfaz para su comunicación con los elementos de otras redes.

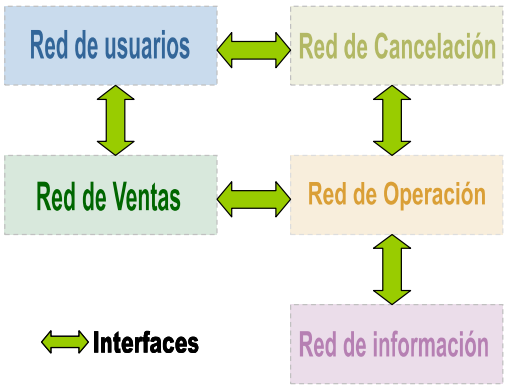


Ilustración 1 Modelo de la Red Tecnológica de Transporte

A continuación se describe la funcionalidad de cada una de estas redes.

2.1.1 Red de usuarios.

En esta red, encontramos los soportes de los títulos de transporte de los Consorcios. Los soportes válidos son tres: la tarjeta de memoria sin contacto Mifare 1Kb, la tarjeta de memoria sin contacto Desfire 4K EV2 y la tarjeta con contacto "Junta sesentaycinco". El equipamiento ofertado debe de ser compatible con las tres tecnologías y operar con ellas.

2.1.2 Red de Cancelación.

En esta red, encontramos los elementos que permiten la recepción de información vía 3G de cancelaciones de usuarios de la red de transporte y posicionamiento del medio de transporte a través de los dispositivos embarcados.

Los sistemas de billetaje objeto de esta licitación se encuentran ubicados en esta red.

2.1.3 Red de Ventas.

Consta de una red segura en alta disponibilidad que permite unir a los terminales de venta y recarga con los Centros Autorizadores de la RCTA, que son los encargados de la validación de las transacciones económicas.

2.1.4 Red de Información.

La red de información permite mostrar información de los servicios de transporte a los usuarios del transporte público. Para realizar esta labor, se opera de manera similar que en la red de cancelación, de modo que esta vez en lugar de dispositivos embarcados en medios de transporte, se enviará información a paneles informativos.

2.1.5 Red de Operación

Esta red es el núcleo de la operación de la RTT. En ella se encuentran los sistemas de explotación y de monitorización. A esta red es donde se enviará la información de venta y posicionamiento de los sistemas de billetaje.

Esta transmisión se realizar por una VPN encapsulada en el propio circuito de comunicación móvil.

3 Alcance

La implantación de la nueva solución de billetaje para urbanos dispondrá desde el inicio del soporte tanto para la tarjeta actual del Consorcio, Mifare Classic 1K como para la futura tarjeta Desfire. De esta forma, la flota estará actualizada cuando se decida migrar a la nueva tarjeta y no será necesario realizar cambios.

La prestación del suministro e instalación consistirá en:

1. ***Suministro e instalación de sistemas de billetaje.***
   Se entiende por solución de sistema de billetaje al conjunto compuesto por expendedora y sistema de gestión que permiten la operación y configuración de las mismas. El operador de transporte dispondrá de un sistema de gestión y un conjunto de expendedoras, así como de un Sistema de Ayuda a la Explotación (SAE). Además para la mejora de la explotación de la recaudación se suministrará un cajero de autoliquidación. Atendiendo a esta definición el alcance para el transporte urbano de la ciudad de Algeciras sería:
   a. Suministro e instalación de 25 expendedoras.
   b. Suministro e instalación de sistemas de gestión.
   c. Suministro e instalación de Sistema de Ayuda a la Explotación (SAE).
   d. Suministro e instalación de un cajero de autoliquidación de recaudación.
2. ***Adaptaciones de sistema tarifario.***
   Se debe indicar el coste que tendría la generación de un nuevo firmware de expendedora ante la entrega de una nueva versión de la librería de transporte de la RCTA.
   El adjudicatario se compromete a mantener la vigencia del coste durante 4 años a contar desde la fecha de la firma del contrato.

4 Valoración técnica de las ofertas

La documentación que deberá ser aportada como parte del proceso de valoración del sobre 2 mediante juicio de valor de la oferta será referenciada como DT.XX y la documentación que deba ser aportada como parte del proceso de valoración del sobre 3 mediante la aplicación de fórmulas será referenciada como DE.XX. Donde XX se corresponde con una secuencia numérica ascendente. La documentación a aportar es la siguiente:

<u>DOCUMENTACIÓN VALORABLE MEDIANTE JUICIO DE VALOR (a incluir en sobre 2)</u>

- DT.01 Documento Ficha Especificaciones Técnicas del Producto.
- DT.02. Documento de solución tecnológica.
- DT.03. Documento de procedimiento de gestión de RMA.
- DT.04. Documento de recursos humanos y técnicos.

- DT.05. Documento de soporte de Mantenimiento.

DOCUMENTACIÓN VALORABLE MEDIANTE FÓRMULAS (a incluir en el sobre 3 junto al anexo XII-Proposición Económica del PCAP)

- DE.01. Preciario
- DE.02. Documento de coste de Mantenimiento
- DE.03. Documentación relativa a los criterios de mejora valorados mediante la aplicación de fórmulas.

La valoración técnica de las ofertas se realizará en función a tres bloques funcionales: requisitos técnicos, características técnicas y criterios de mejora.

- ***Requisitos técnicos***: Son características mínimas que debe contener la solución ofertada. El incumplimiento de alguno de los requisitos conllevará la obtención de 0 puntos en la oferta técnica y por lo tanto la exclusión de la licitación al no cumplir con la solvencia técnica necesaria.
- ***Características técnicas:*** Se valorará la solución tecnológica presentada y algunos aspectos técnicos relevantes fuera de las necesidades y especificaciones técnicas de la RCTA pero que los operadores suelen demandar en su explotación diaria. Estas serán valoradas de acuerdo al máximo de puntuación indicado en el anexo de baremación (Anexo XIII de PCAP).
- ***Criterios de mejora:*** Algunos aspectos técnicos cuantificables pueden estar sujetos a una mejora por parte del licitador. Estos aspectos se indicarán en los siguientes apartados de este pliego como "Criterio sujeto a mejora valorada mediante la aplicación de fórmulas". En caso de incluir alguna de estas mejoras se deberá presentar con la oferta el documento DE.03.

4.1 Requisitos técnicos

4.1.1 Sistema de Ayuda a la Explotación (SAE)

Integrar el equipamiento embarcado con un Sistema de Ayuda a la Explotación para el seguimiento de los servicios y regulación de tráfico.

Las características generales que debe cumplir son:

- Supervisión centralizada en tiempo real del servicio prestado de toda la flota sobre mapa
- Gestión de comunicaciones con vehículos y conductores
- Gestión de líneas, paradas, servicios, horarios, gestión de tiempos de regulación
- Gestión de alarmas
- Actualización remota de las expendedoras.
- Descarga de información remota.
- Gestión de conductores, vehículos, inspectores

- Gestión de mensajes en paneles informativos
- Informes para la gestión y control del tráfico, además de poder analizar los datos históricos del servicio
- Sistemas multimedia (altavoces / micrófono)

El licitador deberá describir las funcionalidades en un apartado del documento de solución tecnológica. Documento de referencia DT.02.

4.1.2 Sistema de Información al Usuario (SIU)

Integración con SIU: Integración del equipamiento embarcado con un Sistema de Información al Usuario que permite la información al usuario mediante paneles informativos interiores y exteriores. Modelo, Fabricante y protocolo de comunicación de paneles de calle y paneles interiores. Portal Web para consulta de información en tiempo real. Aplicación para móviles.
El licitador deberá describir estas funcionalidades en un apartado del documento de solución tecnológica. Documento de referencia DT.02.

4.1.3 Cajero de autoliquidación de recaudación

Complementariamente, para optimizar la gestión de la recaudación del operador de transporte urbano, el sistema de billetaje dispondrá de un cajero de autoliquidación de la recaudación que será instalado en las instalaciones del operador de transporte. Las condiciones mínimas que debe cumplir el equipo son:

- Capacidad de al menos 50 liquidaciones diarias.
- Alta capacidad de monedas y media capacidad de billetes.
- Monedas: CAM (Coin Aceptor Module) y sistema de almacenado de monedas en bolsas con control de peso (MBS).
- Billetes: Aceptador de billetes y almacenado con capacidad al menos para 2.000 billetes.
- Plataforma software integrada en el sistema de gestión y SAE.
- Lector de código de barras uni o bidimensional para lectura del servicio y posterior liquidación.

4.1.4 Soporte para títulos de transporte municipales

La solución de billetaje debe ofrecer gestión para títulos de transporte propios, y soportar las siguientes funcionalidades:

- ***Tipo de soporte:*** Los soportes necesarios son papel y tarjeta sin contacto con Tecnología Mifare Plus o Desfire.
- ***Tipos de títulos:*** A continuación se describen las características de los títulos que deben ser soportados:
    - Soporte para títulos con monedero electrónico.
    - Soporte para títulos de bonos de viaje con caducidad temporal.

- Soporte para títulos temporales con gestión de períodos naturales (semana, mes natural o año natural) o por duración en días/meses.

La verificación de esta característica será realizada en una prueba funcional que tendrá lugar durante el proceso de licitación. Ver apartado 6.1.

4.1.5 Cumplimiento de las Especificaciones Técnicas de la Red de Consorcios

El equipamiento ofertado debe cumplir el Marco de Especificaciones Técnicas de la RCTA.

Para aquellos equipos que actualmente ya se encuentren adscritos al Marco de Especificaciones Técnicas de la RCTA solo será necesario indicar la referencia del modelo a través del formulario establecido en el Anexo X-I del Pliego de Cláusulas Administrativas Particulares. Esta referencia debe coincidir con la que se indicó en su día cuando se cumplimentó la ficha técnica.

Aquellos equipos que NO se encuentren adscritos al Marco de Especificaciones Técnicas de la RCTA deberán rellenar la ficha técnica del producto que permita evaluar sus prestaciones y validar su funcionamiento. Esta acción se realiza a través del portal met.ctan.es, para lo que será necesario que el licitador solicite las credenciales de acceso y registro al Consorcio de Transporte Metropolitano del Campo de Gibraltar. Las fichas de los productos que se registren en el portal, una vez cumplimentados (o Anexo X-I en su caso), deben imprimirse y agruparse en un documento. Documento con referencia DT.01. Fichas de Especificaciones Técnicas.

Resumiendo, las ofertas que presenten equipos que ya estén adscritos al Marco de Especificaciones Técnicas de la RCTA incluirán el Anexo X-I mientras que las que no lo estén incluirán el documento DT.01.

4.1.6 Reparaciones y repuestos

Con objeto de garantizar el correcto tratamiento de las reparaciones y gestión de los repuestos se establecen las siguientes condiciones de obligado cumplimiento para el adjudicatario:

1. *Tratamiento de las reparaciones.* El adjudicatario documentará su tratamiento mediante un procedimiento de gestión de RMA (Return Merchandise Authorization). Documento con referencia DT.03.

   Además, el licitador proporcionará a los operadores uno o varios puntos de atención para la gestión de reparaciones. Se valorará la proximidad geográfica de este punto como criterio sujeto a mejora valorable bajo criterios técnicos. Criterio sujeto a mejora valorada mediante fórmula. Documento de referencia DE.03.

2. *Tiempo de reparación.* Se establece un máximo de 15 días como período de reparación de un equipo en garantía operativa. En caso de no ser reparado en este plazo el

adjudicatario entregará un equipo nuevo al Operador. Criterios de mejora valorados mediante fórmulas. Documento con referencia DE.03.

3. *Preciario.* El adjudicatario hará entrega de un preciario de los repuestos y mano de obra asociada a las reparaciones. Los importes de los distintos conceptos podrán incrementar su valor como máximo el IPC anual. Esta información formará parte del sobre económico. Documento con referencia DE.01.

4.1.7 Garantías

1. *Garantía operativa.* El adjudicatario ofrecerá una garantía mínima de de 3 años en soporte y mantenimiento de los equipos y software suministrados. Durante este plazo cualquier avería en estos elementos será reparada sin coste. Criterios de mejora valorados mediante fórmulas. Documento con referencia DE.03.

2. *Garantía de existencia.* El adjudicatario garantizará la existencia de repuestos y tratamiento de las reparaciones durante un período mínimo de 10 años. Una vez pasado este tiempo, si el adjudicatario desea finalizar la garantía de existencia, deberá comunicar al Consorcio dicha circunstancia al menos 6 meses de antes de la fecha de fin de la prestación de este servicio. Criterios de mejora valorados mediante fórmulas. Documento con referencia DE.03.

   En caso de no poder garantizar la existencia por obsolescencia tecnológica, se ofrecerá la garantía con un equipo funcionalmente compatible. En caso de ser necesario algún tipo de adaptación los costes correrán a cargo del adjudicatario.

4.1.8 Integración con la librería de transportes

La RCTA encapsula toda la lógica de los sistemas tarifarios de las diferentes áreas metropolitanas en una librería de transporte que permite al integrador abstraerse de dicho funcionamiento reduciendo los tiempos, costes de adaptación e incidencias de transporte.

La librería está desarrollada en ANSI C y se puede compilar para cualquier entorno. Dicha librería será proporcionada ya compilada a cada licitador para que la integre en sus equipos.

Las especificaciones técnicas de la librería se describen en el anexo I de este pliego técnico.

En la reunión de lanzamiento del proyecto, se hará entrega al adjudicatario de la librería y se resolverán las dudas que pudiesen surgir.

4.1.9 Transmisión en tiempo real

Para poder atender a las necesidades que demandan los usuarios sobre los servicios de transporte público, la RCTA necesita disponer de la información de venta y posicionamiento de la flota que presta servicio en el ámbito de los Consorcios en tiempo real.

Por este motivo la información de venta y posicionamiento deberá ser enviada en tiempo real al Centro de Operación de la RCTA siguiendo las especificaciones descritas en el anexo II de este pliego técnico.

Este requisito debe ser compatible con las necesidades de transmisión del propio SAE.

4.1.10 Telecarga

Capacidad de configurar remotamente el equipo embarcado para cambiarle el software o la configuración.

4.1.11 Creación de informes a demanda.

Capacidad de poder generar el operador nuevos informes a demanda sobre sus datos de explotación bien proporcionándole una herramienta a tal efecto o por acceso a la base de datos. En este último caso, será necesario la entrega del modelo de datos de la base de datos, documentando las tablas, campos y su función.
Si este requisito no estuviera soportado se puede optar por asumir la creación de 10 informes tipo que requiera el operador. El formato de dichos informes se consensuará con el operador en la fase de lanzamiento del proyecto.

4.2 Características técnicas

El licitador presentará un documento con la solución tecnológica del sistema de billetaje donde se describan todas las características de la solución y de forma expresa y en los términos indicados las funcionalidades que se detallan a continuación, ya que son objeto de baremación independiente. Documento de referencia DT.02. Solución tecnológica.

Si alguna característica requiere un documento adicional se indicará expresamente.

Se debe describir todas las funcionalidades de cada característica que se cumpla al objeto de su correcta valoración. También se indicará, si está incluida de serie o supone un coste adicional.

- ***Venta y recarga a bordo.*** Capacidad de emitir y recargar títulos de transporte a bordo del medio de transporte.
- ***Integración con sistemas de venta centralizados.*** Capacidad de integrar los sistemas de gestión del licitador con sistemas de gestión externos, como los sistemas de venta en taquilla de un operador, evitando la duplicidad de datos y configuración.
- ***Sistema de venta autónoma.*** Se valorará que la solución de billetaje disponga de un terminal de emisión y recarga de títulos autónomo, para ser instalado en lugares públicos dotados de vigilancia las 24 horas.
- ***Soporte de Mantenimiento.*** Aunque la licitación sea solo de suministro es necesario valorar técnica y económicamente el soporte de mantenimiento para poder evaluar la solución tecnológica completa. Desde este punto de vista se debe incluir en la oferta la siguiente documentación:

- Documento de Soporte de Mantenimiento. Este documento describirá los diferentes escenarios de soporte de mantenimiento con el desglose de coberturas y funcionalidades a los que tendrá acceso el operador de transporte para su contratación. Documento con referencia DT.05.
- Documento con el coste de Mantenimiento. Este documento detallará el coste de mantenimiento para un escenario de reparación y atención de incidencias. El coste del contrato vendrá delimitado por una componente fija más una variable en función del número de máquinas. Documento con referencia DE.02.

El procedimiento para gestionar las reparaciones siempre estará sujeto a lo indicado en el documento de gestión de RMA. Mientras que los costes derivados se regirán por el contrato de mantenimiento, y en su ausencia, por el preciario.

5 Organización

5.1 Suministrador y su Director de Integración

Se entiende por Suministrador a la parte contratante encargada de ejecutar el suministro, desarrollo, instalación y labores relacionadas, que actuará ante el Consorcio de Transporte Metropolitano del Campo de Gibraltar mediante la persona designada a tal efecto, el Director de integración, que se responsabilizará de organizar la ejecución del proyecto e interpretar y poner en práctica las directrices recibidas de la Dirección del Proyecto y proponer a ésta o colaborar con ella en la solución de los problemas que se planteen en la ejecución de los trabajos.

El adjudicatario realizará todos los trabajos necesarios para conseguir el objetivo de este contrato, y será plenamente responsable, técnica y legalmente, de su contenido, así como de los plazos de entrega.

El adjudicatario facilitará una relación del personal técnico que vaya a intervenir en los trabajos, con indicación de las funciones específicas de cada persona y unos medios materiales adecuados para su correcta realización. Documento con referencia DT.04. Recursos humanos y técnicos.

Todo el personal adscrito a la realización del trabajo tendrá la capacidad y preparación técnica adecuada a cada una de las fases y especialidades del contrato.

El equipo de trabajo que dispondrá el adjudicatario será definido en la oferta y no podrá modificarse excepto por causas justificadas, y previo consentimiento de la Dirección del Proyecto.

El adjudicatario realizará la totalidad de los trabajos de suministro, desarrollo e instalación. El Consorcio facilitará al adjudicatario cuanta información dispongan relacionada con el objeto de este contrato.

5.2 Director del Proyecto

El Consorcio de Transporte Metropolitano del Campo de Gibraltar nombrará un Director del Proyecto, cuyas funciones serán:

- Interfaz único con los adjudicatarios del proyecto.
- Dirigir y supervisar la realización y el desarrollo de los trabajos, así como aprobar el programa de los mismos.
- Determinar y hacer cumplir el método para la realización del trabajo contratado.
- Decidir la aceptación de las modificaciones propuestas por los adjudicatarios en el desarrollo de los trabajos.
- Definir los informes que crea oportunos sobre la marcha de los trabajos y que serán requeridos al Director de proyecto.
- Definir aquellos aspectos de carácter auxiliar no previstos expresamente en los documentos contractuales que fuera conveniente reglamentar.
- El Director del proyecto será el responsable de la coordinación de los trabajos y velará por el cumplimiento del contrato. En especial, será el que expida las certificaciones comunes si proceden, formule la liquidación y tramite las posibles incidencias que surjan en la tramitación del Contrato.

6 Planificación

6.1 Prueba funcional

Se concretará un día con todos los licitadores para realizar una prueba funcional de la expendedora y canceladora para comprobar que el equipo soporta las funcionalidades básicas de un sistema de billetaje.

6.1.1 Pruebas a desarrollar

El conjunto de pruebas a desarrollar serán:

1. Gestión de Líneas, servicios, conductores
2. Soporte de títulos propios
3. Capacidad de configuración remota
4. Creación de informes a demanda

En caso de no superar la prueba funcional, la oferta obtendrá 0 puntos en la valoración técnica.

6.2 Cronograma de actuaciones

La planificación de la ejecución del proyecto se estima en 5 meses con el detalle que indica la Ilustración 1.

Tareas	Responsable	1	2	3	4	5
Fase I: Operativa Urbana						
0 Funcionalidades para operación urbana						
Suministro de máquinas y cajero	Adjudicatario					
Instalación en los operadores de transporte	Adjudicatario					
Formación	Adjudicatario					
Implantación del piloto fase urbana	Operador y Adjudicatario					
Fase operativa del piloto urbano	Operador y Adjudicatario					
Puesta en servicio	Operador y Adjudicatario					
Fase II: Operativa Consorcio						
1 Especificaciones técnicas						
Documento final y software de la librería de transportes	Consorcio					
Documento final de transmisión en tiempo real	Consorcio					
Configuración del sistema tarifario urbano	Operador y Adjudicatario					
Adaptaciones software	Adjudicatario					
2 Piloto operativo						
Implantación del piloto del proyecto	Todos					
Fase operativa del piloto	Todos					
3 Suministro e instalación						
Formación	Adjudicatario					
Actas de recepción final de suministro	Consorcio					
Puesta en servicio	Todos					

Ilustración 1 Cronograma de actuaciones y tareas

6.2.1 Especificaciones técnicas

Como inicio del proyecto se entregará al adjudicatario el documento final y software de la librería de transporte y el documento final del protocolo de transmisión en tiempo real.

Las diferencias entre las versiones finales de estos documentos y las que se acompañan en la licitación no afectarán a la estimación económica ni temporal del proyecto.

El adjudicatario dispondrá de un período temporal para realizar la adaptación software necesaria.

También se entregarán las especificaciones del sistema tarifario urbano con el objeto de configurar las líneas, servicios de los operadores, títulos de transporte de los operadores, conductores y demás aspectos.

6.2.2 Piloto operativo

El Director de proyecto trasladará al adjudicatario el escenario de transportes donde se implantará la nueva solución y se testeará su correcto funcionamiento. Aunque el alcance se definirá en su momento, este siempre estará acotado a un operador de transporte.

Una vez la fase operativa del piloto concluya con éxito se procederá a la instalación en el resto de operadores y flota.

6.2.3 Suministro e instalación

El adjudicatario presentará un documento con el plan de instalación y formación del proyecto dividido por operadores que consensuará con el Director del Proyecto. Este documento será el que sirva de guía para el seguimiento de los índices de calidad del contrato.

El plan de instalación nunca podrá superar el plazo indicado en el cronograma de actuaciones de este pliego, aunque si el suministro tarda menos se podrá emplear el tiempo restante para instalaciones.

La formación se irá impartiendo según el orden de instalación de operadores cumpliendo dos premisas:

1- Todo el personal de un operador deberá estar formado cuando se instale su flota.
2- No podrá pasar más de 2 semanas entre la formación y la instalación de un operador.

Los operadores irán operando con el nuevo sistema a medida que se termine su implantación y se irán firmando certificaciones parciales de suministro e instalación por cada operador implantado, que permitirá emitir la factura correspondiente a ese operador.

Una vez finalizadas todas las instalaciones el Director del Proyecto emitirá el acta final de suministro e instalación del proyecto.

6.2.4 Puesta en servicio

Aunque la puesta en marcha se realizará de forma progresiva a medida que se vayan implantando operadores, se establecen dos hitos fundamentales de puesta en servicio del proyecto.

- ***Hito de tiempo real:*** Tendrá lugar cuando se finalicen todas las instalaciones y se corresponde con la tarea de puesta en servicio del cronograma de actuaciones. En este instante la RCTA activará la recepción en tiempo real de las ventas que se produzcan en el urbano.
  La información en tiempo real para la integración con el SAE deberá estar disponible desde el primer momento, es decir, desde la puesta en marcha del piloto operativo.
- ***Hito de migración a DESFIRE:*** Podrá o no coincidir con el hito anterior, ya que dependerá de otro proyecto consistente en la adaptación de la flota interurbana. En

este instante se pondrá en funcionamiento la nueva tarjeta de transporte de la RCTA. Se definirá un período de convivencia entre las dos tarjetas (actual Mifare Classic 1k y nueva Desfire 4k EV2), pasado el cual solo se permitirá el uso de la nueva tarjeta.

7 Liquidación del suministro

7.1 Índices de calidad del contrato

Para la medición de la ejecución del contrato se define el siguiente índice:

- ***Índice de consecución de integración (ICI).*** Se define como el cociente entre el número de días empleados en la integración de un operador imputables al adjudicatario y el número de días planificados.

7.2 Penalizaciones

Con aras de fomentar la responsabilidad por parte del adjudicatario, se establece un sistema de penalización por incumplimiento de los plazos de integración

Índice	Penalización
IICI > 1,5 y <=2	10% de penalización en la facturación del operador
IICI > 2	20% de penalización en la facturación del operador

7.3 Liquidación

La liquidación del suministro se realizará por pago único a la finalización del contrato y la factura se enviará al Consorcio descontando la penalización si procede.

8 Documentación

Se entregará la siguiente documentación en soporte electrónico y formato PDF.

- Manual de operación de conductor.
- Manual de operación y mantenimiento del equipo.
- Manual del sistema de gestión.

9 Formación

Se establecerán dos actuaciones formativas con el operador, una en la operativa urbana y otra en la integración metropolitana.

La duración de la actuación formativa puede exceder de una jornada de trabajo, quedará a criterio del adjudicatario en su propuesta. La actuación formativa si deberá tener dos partes, la primera dedicada al funcionamiento del equipamiento embarcado y la segunda dedicada a los sistemas de gestión. La primera está orientada a conductores y la segunda a personal de gestión

10 Confidencialidad de la información

La información a la que tenga acceso la empresa como consecuencia del contrato tendrá un carácter confidencial. No podrá transferir información alguna sobre los trabajos a terceras personas o entidades sin el consentimiento expreso y por escrito del Director del Proyecto.

La empresa adjudicataria, en cumplimiento de la "Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos Personales" y de su posterior desarrollo en el reglamento recogido en el Real Decreto 1720/2007, de 21 de diciembre, únicamente tratará los datos de carácter personal a los que tenga acceso en el marco del presente contrato conforme a las instrucciones del Director de Proyecto y no los aplicará o utilizará con un fin distinto al estipulado, ni los comunicará, ni siquiera para su conservación, a otras personas.

En el caso de que la empresa, o cualquiera de sus miembros, destinen los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será responsable de las infracciones cometidas.

Una vez finalizada la relación contractual, los datos de carácter personal tratados por la adjudicataria, así como el resultado del tratamiento obtenido, deberán ser destruidos o devueltos al Consorcio Metropolitano de Transporte del Campo de Gibraltar en el momento en el que el Director de Proyecto los solicite.

11 ANEXOS:

- Anexo I: Especificaciones técnicas del modelado librería validación títulos de transporte
- Anexo II: Especificaciones técnicas del API de transmisión de la solución de transmisión en tiempo real de la Red de Consorcios de Transporte de Andalucía

Red de Consorcios de Transporte
de Andalucía

Información en tiempo real

Documento de especificaciones técnicas del api de transmisión

Versión 1.1
03/08/17

Índice

1. Introducción 1
2. Arquitectura de la transmisión en tiempo real 1
3. Api RESTful 2
POST /tr/cancelaciones/operador/:id/tpc/:TPC?token=XXXXXX 2
POST /tr/posiciones/operador/:id/tpc/:TPC?token=XXXXXX 3
POST /tr/fichero/operador/:id/tpc/:TPC?token=XXXXXX 5
3.1. Formato de los errores. 6

Histórico

Fecha	Versión	Descripción
06/07/2017	1.0	Documento inicial
03/08/2017	1.1	Inserción de identificación de consorcio en urls Inserción de parada como parámetro en llamada a posicionamiento

1. Introducción

Este documento recoge las especificaciones técnicas del api de transmisión de la solución de transmisión en tiempo real de la Red de Consorcios de Transporte de Andalucía, en adelante RCTA.

Este protocolo será de aplicación a cualquier sistema que necesite enviar información de cancelación y posicionamiento de un medio de transporte en el ámbito de actuación de la RCTA.

2. Arquitectura de la transmisión en tiempo real

La Ilustración 1 muestra cual es la arquitectura para la solución de transmisión en tiempo real.

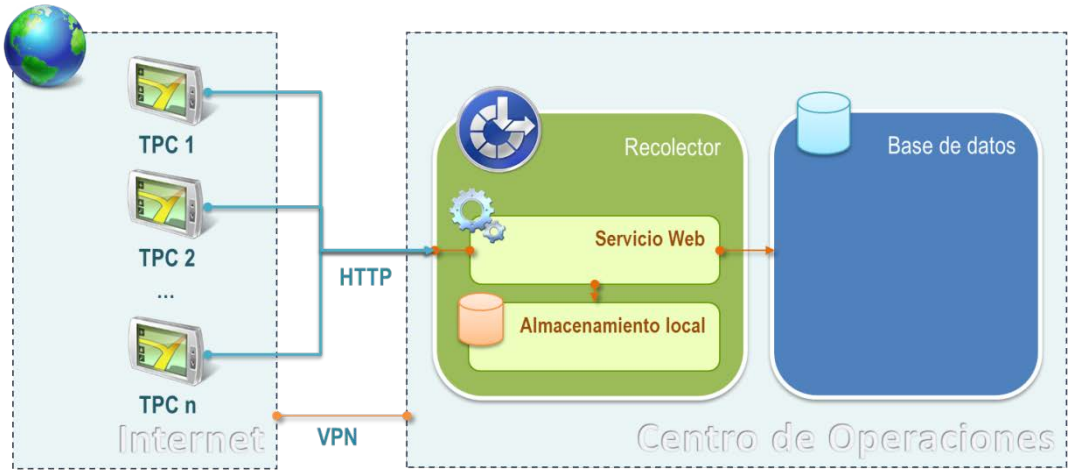


Ilustración 1 Modelo de transmisión en tiempo real

Los elementos que forman parte de la solución son los TPCs (Terminal Punto de Cancelación) y el Recolector.

Un TPC es cualquier dispositivo que gestione información de cancelación y/o posicionamiento, pueden ser pupitres de autobús, sistemas de venta en taquilla, validadores, etc.

El recolector es un software de la RCTA que proporciona un interfaz web para la comunicación de las ventas y posicionamiento.

La comunicación entre los TPCs y el Recolector se realiza a través de una VPN, Existiendo dos tipos de VPN: móviles y fijas.

La VPN móvil se utiliza cuando el método de transmisión del TPC es mediante 3G/4G y en este caso se establece la VPN mediante la configuración de un APN específico que proporciona la RCTA.

La VPN fija se utiliza cuando el TPC no está embarcado y su medio de transmisión es por red cableada. En este caso se establece un circuito IPSEC entre la ubicación del TPC y el Centro de Operaciones de la RCTA.

Las comunicaciones de las cancelaciones y el posicionamiento se realizan utilizando un API RESTful que proporciona el servicio web del Recolector.

El envío de la información está protegido mediante un mecanismo de autenticación por token. Se proporcionará a cada operador de transporte de un token personal e intransferible para el uso con sus dispositivos.

3. Api RESTful

A continuación se describen los recursos del api RESTful.

POST /tr/cancelaciones/consorcio/:idconsorcio/operador/:id/tpc/:TPC?token=XXXXXX

Envía una o varias cancelaciones realizadas en tiempo real desde un TPC activo. Las cancelaciones deben enviarse en el instante que se produzcan, si no fuese posible se almacenarían y enviarían en cuando existiera conectividad.

- **URL:** trans.ctan.es/recolector/v1/tr/cancelaciones/operador/:id/tpc/:TPC?token=XXXXXX
- **Parámetros (application/json):**

Campo	Tipo	Descripción
id	9999	Identificador del operador
TPC	9999	Código del TPC
token	Cadena	Token de acceso
Billete	99	Tipo Billete
Consorcio	99	Identificador del Consorcio donde se realiza el viaje
Línea	XXXXXXXX	Código de la línea en formato acrónimo
Sentido	9	Sentido de la línea
CS	YYMMDDhhmm	Código Servicio
HSC	YYMMDDhhmm	Hora Salida Cabecera
Secuencia	99999	Secuencia
Tarjeta	C99999999	Número tarjeta, donde C corresponde al Consorcio.
Hora	YYMMDDhhmmss	Hora de la operación
Origen	XX	Zona origen
Sorigen	XX	Subzona origen
Saltos	99	Saltos
Ssaltos	9	Saltos subzona
POrigen	9999999999	Parada origen
Destino	XX	Zona destino
PDestino	9999999999	Parada destino
Etapa	9	Etapa

Saldo	99999	Saldo restante
Importe	99999	Importe de la operación
Título	999	Identificador del título
Viajes	999	Viajes restantes
Firma	XXXXXXXXXXXXXXXX	Firma electrónica

Exceptuando los tres primeros campos que forman parte de la url el resto de campos se enviarán formateados en un objeto json de la siguiente forma:

Objeto = {campo:descripción,campo:descripción,…}

Si se envía una sola cancelación se enviará directamente el objeto formateado. Si se envían varias se seguirá el formato array:

Array = [Objeto,Objeto,…]

- **Autenticación**: Basada en el token de acceso.
- **Respuesta (201 / application/json):**

```
{
"E":99
}
```

Devuelve si el procesamiento de la cancelación se ha realizado con éxito. Los valores posibles son:

- E = 0: Cancelación procesada con éxito.
- E = 1: Cancelación almacenada con éxito para procesamiento posterior.
- E = Cualquier otro valor. Error en el procesamiento de la cancelación. El número devuelto indica el tipo de error.

- **Error (500 y 4XX):**

Código	Nombre	Descripción
500	AppError	Error desconocido en la aplicación.
401	NoAut	Token de acceso erróneo.

POST /tr/posiciones/ consorcio/:idconsorcio/operador/:id/tpc/:TPC?token=XXXXXX

Envía una o varias posiciones realizadas en tiempo real desde un TPC activo. Las posiciones se deben tomar y enviar cada 3 segundos.

- **URL:** trans.ctan.es/recolector/v1/tr/posiciones/operador/:id/tpc/:TPC?token=XXXXXX
- **Parámetros (application/json):**

Campo	Tipo	Descripción
id	9999	Identificador del operador
TPC	9999	Código del TPC

token	Cadena	Token de acceso
Consorcio	99	Identificador del Consorcio donde se realiza el viaje
Línea	XXXXXXXX	Código de la línea en formato acrónimo
Sentido	9	Sentido de la línea
CS	YYMMDDhhmm	Código Servicio
HSC	YYMMDDhhmm	Hora Salida Cabecera
Hora	YYMMDDhhmmss	Hora del registro de la posición
Tipo	9	Indica si la posición es normal (0) o de venta (1)
Parada	9999999999	Código de parada si tipo = 1 (venta), 0000000000 en otro caso
Latitud	NGGmmss.ss	Latitud
Longitud	WGGmmss.ss	Longitud
Antigüedad	9999	Antigüedad de la posición en segundos.
Satelites	99	Número de satélites con el que se ha obtenido la posición

Exceptuando los tres primeros campos que forman parte de la url el resto de campos se enviarán formateados en un objeto json de la siguiente forma:

Objeto = {campo:descripción,campo:descripción,…}

Si se envía una sola cancelación se enviará directamente el objeto formateado. Si se envían varias se seguirá el formato array:

Array = [Objeto,Objeto,…]

El parámetro de Antigüedad mide el desfase temporal entre la hora a que fue tomada una posición y la hora actual. En principio la antigüedad debe ser 0, salvo que exista un error en la toma de la posición por parte del GPS y se decida utilizar el dato anterior.

- **Autenticación**: Basada en el token de acceso.
- **Respuesta (201 / application/json):**

```
{
"E":99,
“TE”: 99
}
```

El campo E devuelve si el procesamiento de la posición se ha realizado con éxito. Los valores posibles son:

- E = 0: posicionamiento procesado con éxito.
- E = 1: posicionamiento almacenado con éxito para procesamiento posterior.
- E = Cualquier otro valor. Error en el procesamiento de la posición. El número devuelto indica el tipo de error.

El campo TE, corresponde al nuevo valor del tiempo de envío, inicialmente a 3 segundos. Este valor el que sería aplicable al siguiente envío de posiciones.

- **Error (500 y 4XX):**

Código	Nombre	Descripción
500	AppError	Error desconocido en la aplicación.
401	NoAut	Token de acceso erróneo.

POST /tr/fichero/ consorcio/:idconsorcio/operador/:id/tpc/:TPC?token=XXXXXX

Este recurso se debe utilizar cuando se produzca un fallo en el envío en tiempo real y haya que enviar con posterioridad la información de venta y posicionamiento registrada en el TPC.

- **URL:** /tr/fichero/operador/:id/tpc/:TPC?token=XXXXXX
- **Parámetros (multipart/form-data):**

Campo	Tipo	Descripción
id	9999	Identificador del operador
TPC	9999	Código del TPC
token	Cadena	Token de acceso
Fichero	Fichero	Fichero con los datos de cancelación y posiciones

El contenido del fichero tendrá formato json y seguirá la siguiente estructura:

```
{
Cancelaciones:ArraydeCancelaciones,
Posiciones:ArraydePosiciones
}
```

El formato de ArraydeCancelaciones y ArraydePosiciones se corresponde con el descrito en los puntos anteriores para el caso de envío múltiple.

- **Autenticación**: Basada en el token de acceso.
- **Respuesta (201 / application/json):**

```
{
"E":99
}
```

El campo E devuelve si el procesamiento del fichero se ha realizado con éxito. Los valores posibles son:

- E = 0: fichero procesado con éxito.
- E = 1: fichero almacenado con éxito para procesamiento posterior.
- E = Cualquier otro valor. Error en el procesamiento del fichero. El número devuelto indica el tipo de error.

- **Error (500 y 4XX):**

Código	Nombre	Descripción
500	AppError	Error desconocido en la aplicación.
401	NoAut	Token de acceso erróneo.

3.1. Formato de los errores.

Cuando el api devuelva un error controlado, normalmente errores 4xx, el json de respuesta tendrá el formato:

{ error: "Mensaje",Tipo:9}

Los valores de tipo pueden ser:

0: Mensaje de error.
1: Mensaje informativo.

Red de Consorcios de Transporte
de Andalucía

Librería de transportes

Documento de especificaciones técnicas

Referencia CTAN-RU-LT-DET

Versión 0.1

02/10/17

Índice

1. GLOSARIO DE TÉRMINOS UTILIZADOS 1

2. OBJETIVO 2

3. INTRODUCCIÓN A LA TARJETA MIFARE DESFIRE EV2 4

3.1. IDENTIFICADOR ÚNICO 4
3.2. ORGANIZACIÓN DE LA MEMORIA 5
3.2.1. Aplicaciones 5
3.2.2. Archivos 5
3.3. SEGURIDAD 7
3.3.1. Claves en las aplicaciones 7
3.3.2. Seguridad en los archivos. 7
3.4. RESUMEN DE COMANDOS DE LA TARJETA 9

4. DEFINICIÓN GENERAL DE LA API 11

4.1. CONVENIO DE INTERCAMBIO DE INFORMACIÓN. 11
4.1.1. Convenio de orden MSB y LSB 11
4.1.2. Convenio de organización del contenido 12
4.1.3. Convenio de espacio reservado para los arrays data_in y data_out 13
4.1.4. Registro TLV de Cabecera obligatorio en data_in y data_out. 13
4.1.5. Posibles registros TLV en data_out para cualquier función. 14
4.2. RESUMEN DE LAS FUNCIONES DISPONIBLES EN LA LIBRERÍA (API) 16
4.3. OPERATIVA 17
4.4. REDES SOPORTADAS 18

5. FUNCIONES DE LA API 20

5.1. VERSION 20
5.1.1. Descripción y uso. 20
5.1.2. Sintaxis. 20
5.1.3. Entradas. 20
5.1.4. Salidas. 20
5.2. INIT 22
5.2.1. Descripción y uso. 22
5.2.2. Sintaxis. 22
5.2.3. Entradas. 22
5.2.4. Salidas. 29
5.3. PROCESS 30
5.3.1. Descripción y uso. 30
5.3.2. Sintaxis. 30
5.3.3. Entradas. 30
5.3.4. Salidas. 38
5.3.5. Relación de Acciones <-> Respuestas 47
5.4. LASTERROR 49
5.4.1. Descripción y uso. 49
5.4.2. Sintaxis. 49
5.4.3. Entradas. 49
5.4.4. Salidas. 49
5.5. GETINFO 50
5.5.1. Descripción y uso. 50
5.5.2. Sintaxis. 50
5.5.3. Entradas. 50
5.5.4. Salidas. 50
5.6. RESUMEN DE TIPOS EN “DATA_IN” 55
5.7. RESUMEN DE TIPOS EN “DATA_OUT” 55

6. TABLA ASCII DE CARACTERES DE TEXTO 57

7. TABLA DE CARACTERES DE TRATAMIENTO ESPECIAL. 58

Histórico

Fecha	Versión	Descripción
02/10/2017	0.1	Documento inicial

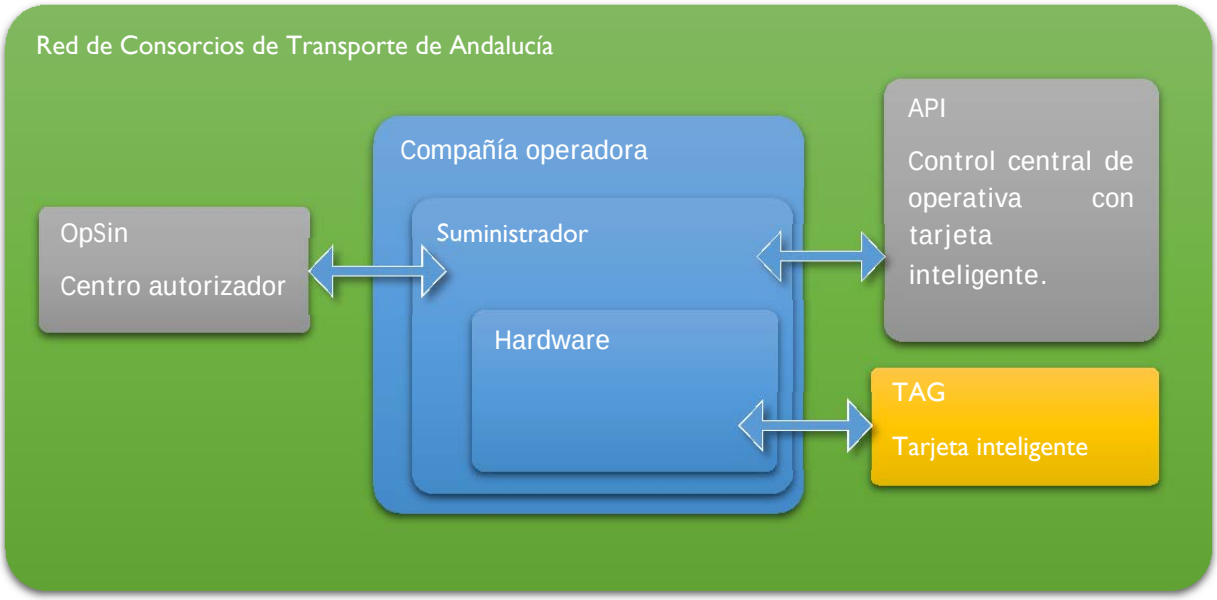
1. GLOSARIO DE TÉRMINOS UTILIZADOS

Termino	Descripción
Actuar con la tarjeta	Cualquier procedimiento de operación de venta, carga, recarga, cancelación, inspección, etc... que puede ser efectuada en un TAG
AID	Identificador de una aplicación de la tarjeta Desfire EV2.
AMK	Aplication Master Key o Clave maestra de la aplicación. Indica la clave principal de una aplicación con AID ≠ 00 00 00
API	Interface para la Programación de Aplicaciones. Se tratará de funciones externas que ofrece funciones necesarias para el desarrollo de un determinado software.
CID	Código de identificación de la acción a ejecutar. Cada registro/acción retornado en "data_out" de la función "Process()" dispone de un identificador numérico único. Este valor es tomado como referencia para los resultados de la acción.
FID	Identificador de un archivo, contenido dentro de una aplicación de la tarjeta Desfire EV2.
Hardware	Hace referencia a cualquier dispositivo utilizado para realizar las actuaciones con las tarjetas.
HOST o Software suministrador	Programa de la empresa suministradora que requiere la utilización de la librería para realizar transacciones con la tarjeta Desfire EV2
LSB	Posición menos significativa en un array de información
MK	Master Key o clave maestra. Indica la clave principal de la tarjeta, perteneciente a la aplicación AID = 00 00 00.
Modulo Centralizador	Conjunto de archivos que conforman la API
MSB	Posición más significativa en un array de información
Notaciones numéricas	En este documento se representaran varias notaciones numéricas que serán diferenciadas con la siguiente norma: Decimales: Representaremos el numero tal cual. Ejemplo 137. Hexadecimales : representado en notación "0x", ejemplo 0x123F Binarios: representados con una "b" al final, ejemplo 010011b
RAW	Información digital en bruto
Suministrador	Empresa suministradora de los dispositivos de venta, recarga, cancelación, inspección a las diferentes compañías anexadas a la operatividad del Consorcio de Transportes de Andalucía y que requieran del uso de la API.
TAG	Indica la tarjeta de proximidad DesFire EV2.
TLV	Indicativo de estructura de datos Tipo Longitud Valor.
UID	Identificador único de la tarjeta Desfire EV2.
Viajero o Usuario	Persona física propietaria de la tarjeta y por lo tanto al que se debe ofrecer toda la información necesaria de la transacción efectuada sobre su tarjeta.

2. OBJETIVO

Los requerimientos establecidos para la migración tecnológica de la tarjeta de la Red de Consorcios de Transportes de Andalucía desde su actual soporte MiFare Classic al nuevo soporte Desfire EV2, para cualquier operativa asociada (venta, recarga, uso, etc...), establecen que cualquier actuación sobre las tarjetas se realicen de forma exclusiva y centralizada por una única librería independiente y de uso obligado por cualquier sistema de Suministrador que requiera la interacción con la tarjeta de transporte.

Este marco de actuación queda reflejado en el siguiente esquema:



Cualquier software del suministrador/es de la solución de determinado operador de transporte, deberá utilizar la librería "*módulo centralizador*" para interactuar con la nueva tarjeta de transporte del Consorcio basada en tecnología DESFIRE EV2.

Mediante llamadas a las distintas funciones del API de esta librería, el software del suministrador será capaz de realizar operaciones de Venta, Recarga y Cancelación sobre las tarjetas de los usuarios.

Cuando hacemos referencia en este documento a *módulo centralizador*, se hace referencia al conjunto de archivos que conforman la librería que contiene las distintas operaciones contenidas en su API.

El uso del API de la librería establece un marco de trabajo único para cualquier suministrador de soluciones, asegurando los siguientes objetivos:

- **Seguridad**. Al existir un único *modulo centralizador* para las operaciones con la tarjeta, todas las operaciones que requieran autentificación y/o el uso de determinadas credenciales de acceso son procesadas/calculadas por dicho módulo y solo conocidas por él. Además también incluye todos los procedimientos de control lógico a realizar en las diferentes operativas de funcionamiento, venta, recarga, cancelación e inspección.

- **Flexibilidad**. El *modulo centralizador* estará preparado y desarrollado para poder ser utilizado en los entornos de desarrollo más actuales, ya que adopta la norma ISO (ISO/IEC 9899:1990) permitiendo la portabilidad entre plataformas y arquitecturas, aunque, para ello sería necesario disponer del módulo definitivo ("release") en el formato de salida requerido por el suministrador del operador en cuestión.

De forma inicial, se dispondrá de las librerías en los siguientes formatos

Sistema Operativo	Formato
Windows 32 bits	**Librería dinámica DLL nativa**
Linux	Librería .lib con cabecera de prototipo .h

• **Centralización**. El uso del *módulo centralizador* se basara en archivos de librerías de enlace directo (no será necesario ningún tipo de instalación adicional) de esta forma todos los sistemas que hagan uso de ella dispondrán de acceso a posibles actualizaciones de la misma. En caso de ser necesario una modificación/ampliación de la librería se podría utilizar el método "reemplazar y listo" para continuar con su funcionamiento.

Existirá disponible un método que permita conocer la versión de la librería en uso.

• **Independencia del hardware**. Esto permite mayor facilidad en su integración ya que el *módulo centralizador* es totalmente independiente del hardware utilizado, ya que este es responsabilidad de funcionamiento y uso por parte del Suministrador del mismo.

En este documento veremos como todas las funciones de la API para operar con las tarjetas de proximidad están basadas en órdenes básicas o primitivas.

3. INTRODUCCIÓN A LA TARJETA MIFARE DESFIRE EV2

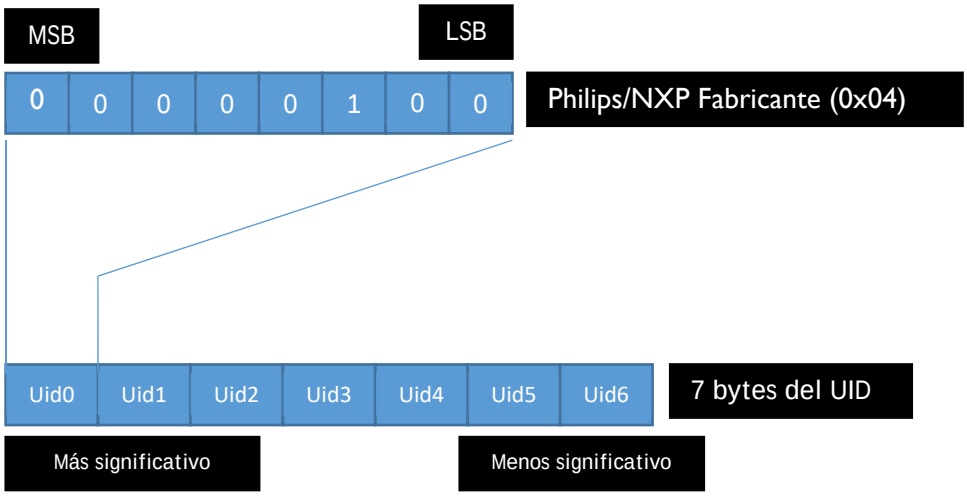
Este apartado repasa brevemente, sin entrar en profundidad, los detalles de la tarjeta Desfire EV2, destacando los puntos que tienen más relación con la librería.

La 'MiFare Desfire EV2' es una tarjeta de memoria que para la transmisión y recepción de datos con un lector utiliza una comunicación por radio frecuencia sin necesidad de utilizar baterías. Dentro del estándar ISO 14443 A y cumple con las 4 primeras normas de dicho estándar.

Existen varios modelos según su capacidad de almacenamiento, 2 kbytes, 4 kbytes y 8 kbytes. El tratamiento de todas ellas es idéntico, ya que solo cambia su tamaño de almacenamiento. En este proyecto serán utilizadas las de 4 kbytes.

3.1. IDENTIFICADOR ÚNICO

Dispone de un identificador "único" UID de 7 bytes. El cual dispone en su byte más significativo MSB el código de fabricante de la tarjeta, que en el caso de Philips/NXP su código es 0x04. De esta forma se establece la norma de lectura del UID para su control y representación, tanto en decimal como en hexadecimal.



Un ejemplo de UID podría ser Hexadecimal **0x042A59DAE82280**, Decimal **1172465319944832**

Este UID es establecido por el fabricante de la tarjeta y no es posible cambiarlo por ningún método.

3.2. ORGANIZACIÓN DE LA MEMORIA

La tarjeta tiene la capacidad de almacenar hasta 28 aplicaciones (AID) y en cada una de ellas hasta 16 archivos (FID).

Se debe tener en cuenta, como detalle, que el borrado de aplicaciones y/o archivos es "lógico", es decir no se borra físicamente en la tarjeta el espacio ocupado por dicho elemento, por lo que existen métodos que permiten recuperar dicho espacio ocupado.

3.2.1. Aplicaciones

La representación de una aplicación, AID, está compuesta por 3 bytes de propósito general, o sea, cuando es creada una nueva aplicación, el valor establecido en estos 3 bytes puede ser cualquiera, con la excepción de que dicho AID no sea el Hexadecimal **00 00 00** y que no esté ya creada.

La AID hexadecimal **00 00 00** es especial, ya que se trata por especificaciones de la propia estructura de la tarjeta Desfire EV2 de la aplicación "master". Esta aplicación NO puede contener Archivos y sus propiedades de acceso son diferentes al resto.

El resto de aplicaciones en hexadecimal **00 00 01** a la **FF FF FF**, pueden contener hasta 16 archivos como máximo y cada uno de ellos pueden ser de diferentes tipos de organización de datos.

Para poder crear/borrar aplicaciones, es necesario tener seleccionada la aplicación **00 00 00.**

Para poder crear/borrar archivos, es necesario tener seleccionada la aplicación contenedora de dicho archivo, como se ha comentado, la aplicación **00 00 00** NO permite contener archivos.

Los derechos de acceso de la Aplicaciones son detalladas más adelante.

3.2.2. Archivos

La representación de un archivo, FID, solo la compone un byte de propósito general, o sea, puede tener el valor desde **00** a **FF**. De forma independiente y común para cada uno de los archivos, se dispone de dos parámetros de relevante importancia, establecidos durante la creación:

- Derechos de acceso según las claves establecidas en la aplicación contenedora, explicados más adelante
- Método de cifrado para la codificación de las comunicaciones, que pueden ser:
    - Comunicación en plano.
    - Comunicación en plano securizada por DES/3DES MAC.
    - Comunicación cifrada en DES/3DES.

Los archivos pueden ser de 5 tipos diferentes, cada uno de ellos dispone de ciertas propiedades de control que indicamos a continuación:

- Archivo de datos estándar, código 0x00.

  Se trata de un archivo de almacenamiento de información estándar con un tamaño en bytes fijo, especificado en su creación. Se debe tener en cuenta que la organización de estos archivos internamente consumen bloques de 32 bytes (un archivo de, por ejemplo 1 byte, ocupara en la tarjeta 32 bytes).

- Archivo de datos con backup, código 0x01.

  Se trata de un archivo de almacenamiento exactamente igual que el anterior, pero con la peculiaridad de que dispone de un duplicado o backup, por lo tanto debe tenerse en consideración que ocupara el doble de espacio en la tarjeta.

  Durante toda su operativa, las transacciones se realizaran en el archivo duplicado, siendo necesario realizar una operación de "*commit transaction*" para que la información sea trasladada al archivo original.

  La tarjeta solo permite disponer de 8 archivos de este tipo como máximo y obligatoriamente deben estar numerados con un FID comprendido entre **00** y **07**.

- Archivo de dato de valor (siempre con backup), código 0x02.

  Permite controlar un valor numérico de 32 bits con signo. En su operativa se pueden establecer el valor mínimo, el valor máximo y la posibilidad de operativa a crédito activada o desactivada.

  Este tipo de archivos siempre está respaldado por backup, por lo que será necesario la utilización de la operación "*commit transaction*" para que la información sea trasladada al archivo original.

- Archivo de datos con registros lineales (siempre con backup), código 0x03.

  Permite crear un archivo que permite el almacenamiento de múltiples registros del mismo tamaño en bytes. Sera necesario indicar el tamaño del registro en bytes y la cantidad máxima de registros almacenados. El tamaño total del archivo ser calculado multiplicando el tamaño del registro por la cantidad de ellos.

  Para poder acceder a los datos, tanto en lectura como en escritura, será necesario indicar la posición del registro a la que se desea acceder.

  Este tipo de archivos siempre está respaldado por backup, por lo que será necesario la utilización de la operación "*commit transaction*" para que la información sea trasladada al archivo original.

- Archivo de datos con registros lineales cíclicos (siempre con backup), código 0x04.

  Este tipo de archivos en su definición es igual al anterior, permitiendo almacenar múltiples registros de un tamaño específico, pero su funcionamiento es controlado de forma cíclica, o sea, una vez el archivo tiene lleno completamente todos sus registros, comenzará a sobrescribir el más antiguo. Este funcionamiento lo realiza automáticamente la tarjeta.

  Este tipo de archivos siempre está respaldado por backup, por lo que será necesario la utilización de la operación "*commit transaction*" para que la información sea trasladada al archivo original.

3.3. SEGURIDAD

3.3.1. Claves en las aplicaciones

La aplicación master AID = 00 00 00 SOLO dispone de 1 clave denominada MASTER KEY (MK), ubicada única y exclusivamente en la posición 0. Las propiedades de esta clave pueden ser:

- Permiso de cambiar la Master Key sin la autentificación con la Master Key (si/no).
- Permiso de listar las aplicaciones sin autentificación con Master Key (si/no).
- Permiso de crear y borrar aplicaciones sin la autentificación con la Master Key (si/no).
- Permiso de cambiar estos parámetros sin la autentificación con la Master Key (si/no).

En cualquier otra aplicación AID ≠ 00 00 00 se puede disponer de hasta 14 claves configurables, donde la clave 0 es denominada como la "Application Master Key" (AMK):

Esta cantidad de claves se establece en el momento de la creación de la aplicación, para poder crear aplicaciones será necesario estar seleccionada la aplicación AID = 00 00 00 y tener los privilegios adecuados. Las propiedades de este conjunto de claves pueden ser:

- Es necesario la "Application Master Key" para cambiar cualquier clave.
- Es necesario la autentificación con la clave "N" (1...13) para cambiar cualquier clave.
- Es necesario la autentificación con la clave "N" (1...13) para cambiar la clave "N".
- Todas las claves están congeladas.
- Permiso de cambiar estos parámetros sin la autentificación de la "Application Master Key", (si/no, en este caso, estos parámetros se consideran congelados).
- Permiso de crear y borrar archivos sin necesidad de autentificación con la "Application Master Key" (si/no).
- Permiso para listar y leer propiedades de archivos sin necesidad de autentificación con la "Application Master Key" (si/no).
- Permiso de cambiar la "Application Master Key" sin la autentificación con la propia "Application Master Key" (si/no, en este caso la "Application Master Key" está congelada).

3.3.2. Seguridad en los archivos.

El acceso a los datos almacenados en los archivos está protegido individualmente por cada aplicación, en la cual, como se ha visto en el punto anterior, puede contener hasta 14 claves diferentes (0…13).

También es posible indicar como índice de clave los valores 14 y 15, que indican:

- 14 = Acceso libre, no es necesario ninguna clave para la realizar la operación.
- 15 = Acceso denegado, no es posible realizar la operación (operación congelada).

Por cada archivo será necesario indicar que clave (de la 0 a la 15) tiene derecho a realizar cada una de las siguientes operaciones:

- Lectura, leer valor y decrementos.
- Escritura, leer valor, decrementos y crédito limitado.

- Lectura/Escritura, leer valor, decrementos, crédito limitado e incrementar valor.
- Configuración de estos derechos de acceso.

Por ejemplo, para una AID concreta, además de su "Application Master Key (AMK)" (índice = 0), se ha añadido una nueva clave con el índice 1 la cual se desea utilizar para "solo lectura" en el archivo 00, por lo tanto, en la creación del archivo 00 es necesario indicar los siguientes derechos de acceso:

Derecho de acceso	Índice de clave
Lectura, leer valor y decrementos.	1
Escritura, leer valor, decrementos y crédito limitado.	0
Lectura/Escritura, leer valor, decrementos, crédito limitado e incrementar valor.	0
Configuración de estos derechos de acceso.	0

Otro aspecto que es definido en la creación de los archivos es el nivel de seguridad para las comunicaciones, que pueden ser acorde a las siguientes:

- Comunicaciones en plano.
- Comunicaciones DES/3DES MAC
- Comunicaciones completamente encriptadas DES/3DES

3.4. RESUMEN DE COMANDOS DE LA TARJETA

Detallamos a continuación una tabla con un resumen general de las acciones de operaciones que podrán ser utilizados de forma general con la tarjeta Desfire EV2. Referencia para todos los registros de órdenes que se explicaran más adelante en este documento.

Se debe tener en cuenta que el detalle de estas acciones cumple con la norma establecida como estándar por Philips Semiconductors en sus especificaciones de producto MF3 IC D40.

Ámbito	Comando	Detalles
Seguridad	0x0A	Autentificar
	0x54	Cambiar propiedades de seguridad de la clave maestra
	0x45	Leer propiedades de seguridad de la clave maestra
	0xC4	Cambiar claves
	0x64	Leer versión de claves
Nivel de tarjeta	0xCA	Crear aplicación
	0xDA	Borrar aplicación
	0x6A	Listar aplicaciones existentes.
	0x5A	Seleccionar una aplicación.
	0xFC	Formatear completamente la memoria
	0x60	Leer versión de fabricación
Nivel de aplicación	0x6F	Listar archivos de la aplicación seleccionada
	0xF5	Leer información de un archivo especifico
	0x5F	Cambiar los parámetros de acceso de un archivo
	0xCD	Crear archivo de datos estándar.
	0xCB	Crear archivo de datos estándar con backup
	0xCC	Crear archivo de dato de valor.
	0xC1	Crear archivo de registros lineales.
	0xC0	Crear archivo de registros lineales cíclico.
	0xDF	Borrar archivo.
Nivel de archivos	0xBD	Leer datos de archivo estándar o con backup
	0x3D	Escribir datos en archivo estándar o con backup
	0x6C	Leer valor de archivo de valor.
	0x0C	Incremento del valor en archivo de valor.
	0xDC	Decremento del valor en archivo de valor.

	0x1C	Incremento del valor limitado por el crédito establecido.
	0x3B	Escribir datos en un registro en un archivo de registros lineales o cíclicos.
	0xBB	Leer datos de registros de un archivo de registros lineales o cíclicos
	0xEB	Borra completamente un archivo de registros lineales o cíclicos.
	0xC7	Confirmar transacción. Valida todas las escrituras previamente realizadas en archivos de datos estándar con backup, de valor y registros.
	0xA7	Invalidar transacción, anula todas las escrituras previamente realizadas en archivos de datos estándar con backup, de valor y registros.

4. DEFINICIÓN GENERAL DE LA API

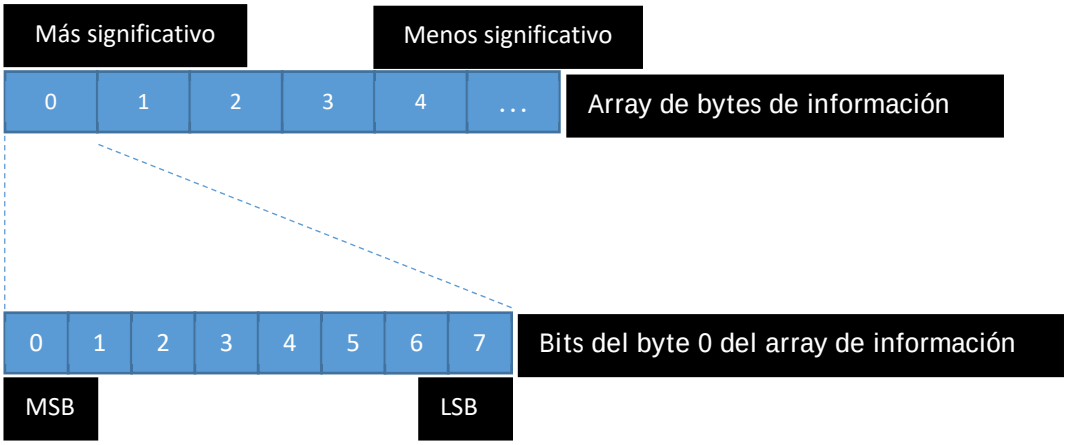
Debido a los requerimiento de seguridad en el uso de la nueva tarjeta, la manera de utilizar la librería por el software del suministrador establece una operativa donde el elemento central es la propia librería, siendo esta la encargada de centralizar y securizar todo el proceso de una determinada transacción: Venta, Recarga y Cancelación. El suministrador hace las funciones de intermediario entre su hardware (lector físico de tarjetas sin contacto) y la librería, abstrayéndose completamente de la operativa interna.

4.1. CONVENIO DE INTERCAMBIO DE INFORMACIÓN.

4.1.1. Convenio de orden MSB y LSB

Como normal general, es importante dejar claro la referencia del posicionamiento del byte y del bit más significativo y menos significativo en caso de los array's de datos.

El bit/byte Más significativo estará situado en el extremo izquierdo y el menos significativo en el extremo derecho. Queda esta información mucho más clara y detallada con la siguiente representación gráfica:



Ejemplo 1: si se desea transmitir en 1 solo byte el valor 137 en decimal, 0x89 en hexadecimal, quedaría representado de la siguiente forma:

Bytes	0
	0x89

Bits	0	1	2	3	4	5	6	7
	1	0	0	0	1	0	0	1

137 = 0x89 = 10001001b

Ejemplo 2: si se desea transmitir en 2 bytes el valor 30000 en decimal 0x7530 en hexadecimal, quedaría representado de la siguiente forma:

Bytes	0	1
	0x75	0x30

Bits	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	0	1	1	1	0	1	0	1	0	0	1	1	0	0	0	0

30000 = 0x7530 = 111010100110000b

4.1.2. Convenio de organización del contenido

Se define un convenio para el intercambio de la información establecido en todas las funciones de llamada a la API que hacen referencia a un puntero a datos ***data_in** o ***data_out**, estos array's de información deben cumplir con dicho convenio en caso contrario la información será rechazada.

La información será tratada en formato TLV (Tipo/Longitud/Valor), cada registro de información deberá cumplir dicha norma. En todas las tramas, el primer byte indica T (Tipo), los 2 siguientes indica L (Longitud) y el resto tendrá una longitud de "L" bytes que indica el V (Valor), es decir L indica la cantidad de bytes del registro **sin incluir ni T ni L**.

Bytes	0	1	2	3	.	.	.	N
Campo	T	L		V				

En un mismo array de datos "data _in" o "data_out" pueden ir tantos registros TLV como sea necesario, pero siempre serán iniciados por un registro TLV denominado registro de cabecera, el cual además de información general de operatividad, indica la cantidad de registros TLV que preceden.

```
<TLV de cabecera> <registro TLV 1> [… <registro TLV N>]
```

Por ejemplo, si es llamada a la función "Version()", esta devolverá en su array "data_out" la siguiente información estructurada:

```
<TLV de cabecera> <TLV de versión de núcleo> <TLV de versión de
validación> <TLV de versión de inspección> <TLV de comprobación
de datos>
```

4.1.3. Convenio de espacio reservado para los arrays data_in y data_out

La adoptación de la norma ISO (ISO/IEC 9899:1990), implica que los "punteros" de datos de intercambio NO dispone de método para determinar el tamaño de los mismos, por lo tanto se establece, por el ámbito de uso, que el responsable de asignar el tamaño adecuado para el intercambio de la información en los arrays "data_in" y "data_out" sea HOST y **tengan siempre una longitud de 1024 bytes (1 Kb)**.

La primera función de la librería será establecer a 0 el espacio reservado del array "data_out" mediante "set" directo a memoria.

4.1.4. Registro TLV de Cabecera obligatorio en data_in y data_out.

Detallamos ahora la sintaxis que debe cumplir el registro TLV de cabecera en todos los casos:

Byte	Campo	Detalles
0	**T**	**0xF1**
1…2	**L**	**Longitud en bytes del registro, sin incluir ni T ni L. valor 12.**
3	F1_VER	Versión del registro de cabecera. 1 = versión 1.
4…5	F1_CNT	Contador de la secuencia del proceso. Solo necesario para la función "Init()" y "Process()". Este contador se inicia a 0 cuando se inicia el proceso con la función de la API "Init()" y será incrementado en 1 de forma balanceada por el HOST y la librería, en las llamadas consecutivas a la función "Process()". La librería será la encargada de detectar que este valor tiene su secuencialidad correcta respecto al anterior, en caso de error producirá un retorno =2 (error) con 06_CERR = 1 = Error del campo CNT en cabecera. En la cabecera de la primera llamada de la función "Init()" → CNT=0 En la cabecera de la siguiente llamada a "Process()", en data_in, CNT=1 y en data_out, CNT=2 En la cabecera de la siguiente llamada a "Process()", en data_in, CNT=3 y en data_out, CNT=4 …
6..7	F1_FIRMA	Código de seguridad Se trata de un código de control obtenido a partir de un algoritmo realizado con todos los registros que forman el "RAW" complete de la información. Se detalla en un punto más Adelante.
8..9	F1_NREG	Nº de registros TLV contenidos a continuación de este registro de cabecera, o sea, sin contar el propio registro de cabecera.
10	F1_HH	Hora del sistema
11	F1_MM	Minuto del sistema
12	F1_SS	Segundos del sistema
13…14	F1_RFU	Reservados para futuro uso

4.1.5. Posibles registros TLV en data_out para cualquier función.

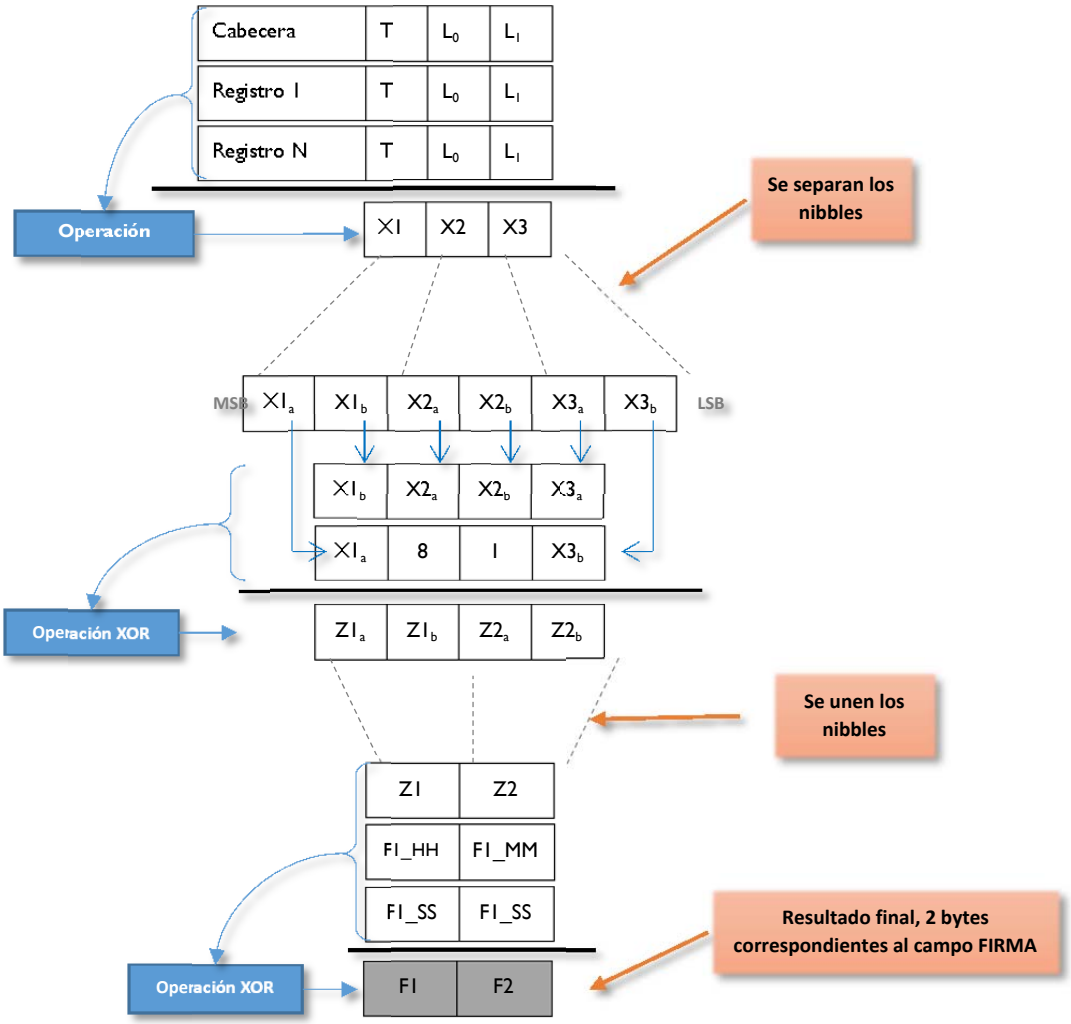
- Tiempo de ejecución de la función:

Byte	Campo	Detalles
0	**T**	**0xF2**
1…2	**L**	**Longitud = 4**
3…6	F2_TC	Tiempo en milisegundos consumido por la ejecución completa de la función

4.1.5.1. Calculo de la firma de seguridad

En el registro de cabecera hay un campo llamado FIRMA que debe ser calculado "antes" de realizar el envío de la información hacia la librería, de igual forma, la librería realizara el cálculo del campo FIRMA antes de producir la respuesta.

El cálculo es el resultado de efectuar el OR exclusivos "XOR" de una forma concreta a los bytes T y L de TODOS los registros que conforman el RAW completo de información, incluido el registro de cabecera, y para añadir variabilidad se incluirá también los campos F1_HH, F1_MM y F1_SS, El cálculo se indica en el siguiente esquema:



4.2. RESUMEN DE LAS FUNCIONES DISPONIBLES EN LA LIBRERÍA (API)

En esta tabla muestra un resumen de todas las funciones que dispone la API.

Función	Detalles
Version()	Función genérica que puede ser llamada en cualquier momento deseado que retorna las diferentes versiones de la API.
Init()	Función de inicio de operaciones, es obligatorio su llamada antes de iniciar el ciclo de operaciones con la función "Process()".
Process()	Función de proceso principal, permite la ejecución paso a paso de la operativa con una tarjeta.
LastError()	Función que retorna el último error interno producido en la función "Init()" o "Process()", en caso de se haya producido algún error. Este error es reseteado en la llamada a la función "Init()".
GetInfo()	Función que retorna la información visual o impresa que es necesario producir al viajero una vez finalizado el proceso completo con la tarjeta (retorno de "Process()" = 1), esta información es reseteada en la llamada de "Init()".

4.3. OPERATIVA

La manera en la cual será utilizada la librería será simple, la llamada a las funciones de la API tienen que ser ejecutadas en un determinado orden "Init() → Process() →Process()→ … → GetInfo()", y el software del suministrador es el encargado de hacer efectivas las acciones recibidas por la función "Process()" durante el ciclo de llamadas.

La función principal "Process()", opera como un *controlador* de operaciones según la información recibida por el HOST que utiliza la librería en el parámetro de entrada "data_in". "Process()" siempre devuelve 2 valores:

- El valor de retorno indicando "continuar/finalizado/error"

- Un 'array' de registros TLV denominado "data_out" con la información de acciones a tomar por el software del suministrador (HOST).

Cualquier transacción (VENTA, RECARGA, CANCELACIÓN, ETC …) con una nueva tarjeta colocada en el lector o dispensador (PICC) contactless, es iniciado siempre por el software del suministrador (HOST).

La primera llamada a la librería siempre debe ser siempre la función "Init()":

1. Se indica que se desea hacer (vender, validar, etc…).
2. Parámetros necesarios dependiendo del tipo de transacción con la tarjeta: Venta / Recarga / Cancelación, etc.

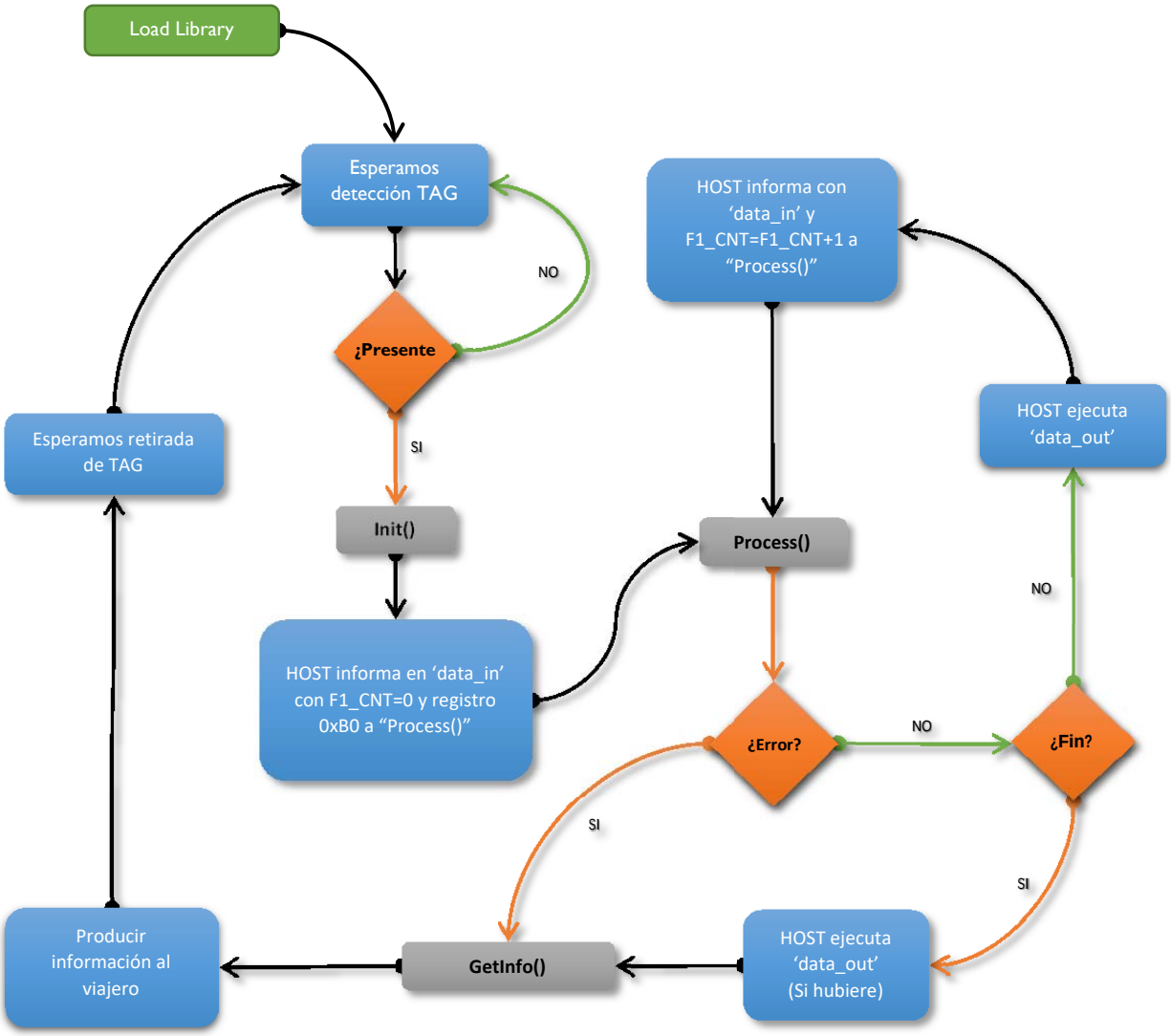
Tras la llamada a "Init()", el HOST realizará un ciclo de llamadas consecutivas a la función "Process()", esta retornará al HOST (en data_out) la lista de acción o acciones que debe realizar con la tarjeta presente (son responsabilidad del host de hacerlas efectiva físicamente) y, una vez finalizada la ejecución, informar de nuevo a la API con la función "Process()" de todos los resultados obtenidos de la ejecución de las acciones de forma individual. Este ciclo continuará hasta que la función "Process()" indique fin o error.

Independientemente de la operativa a realizar, en la primera llamada a la función "Process()" se espera que el HOST informe de los datos generales del TAG presente, entre ellos el UID del mismo, mediante el registro TLV **"0xB0"**

> Todas las acciones recibidas en los registros data_out de la funcion "Process()" deben tener un resultado/respuesta concreta que indicar en los registros data_in de la siguiente llamada a la funcion "Process()" (si este indica continuar).

> Si durante la ejecución de alguna acción recibida de la función "Process()", ya sea referente a la tarjeta o al lector, produce algún error, **el HOST debe interrumpir la ejecución de las acciones** e informar a la función "Process()" del resultado/respuesta de las acciones ejecutadas hasta el momento (incluida la que produjo el error).

El esquema siguiente representa el flujo de operación de llamadas a las funciones de la API por parte del HOST.



4.4. REDES SOPORTADAS

Detallamos los códigos de redes soportadas.

Código de red	Descripción
1	Área de Sevilla
2	Bahía de Cadiz
3	Área de Granada
4	Área de Málaga
5	Área de Gibraltar

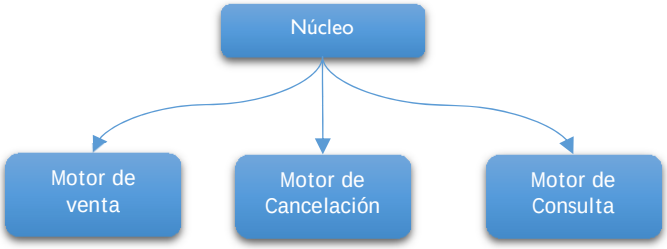
6	**Almería**
7	**Jaén**
8	**Córdoba**
9	**Huelva**

5. FUNCIONES DE LA API

5.1. VERSION

5.1.1. Descripción y uso.

Es importante disponer de las versiones operativas de los diferentes módulos de proceso que contiene la API, en su conjunto la API dispone de 4 versiones diferenciadas



Esta función puede ser llamada en cualquier momento sin que interrumpa o interfiera en cualquier otra llamada.

5.1.2. Sintaxis.

void Version(unsigned char *data_out)

5.1.3. Entradas.

Ninguna.

5.1.4. Salidas.

unsigned char *data_out

Array de información con los registros TLV del detalle de las versiones de los diferentes módulos además de información adicional para el programador.

Los registros son los siguientes:

- Versión del núcleo

Byte	Campo	Descripción
0	**T**	**0x01**
1…2	**L**	**longitud = 4**
3	01_V1	Valor de la versión mayor
4	01_V2	Valor de la versión menor.
5…6	01_BUILD	Valor de la compilación

- Versión del módulo de venta.

Byte	Campo	Descripción
0	**T**	**0x02**
1…2	**L**	**longitud = 2**
3	02_V1	Valor de la versión mayor
4	02_V2	Valor de la versión menor.

- Versión del módulo de validación

Byte	Campo	Descripción
0	**T**	**0x03**
1…2	**L**	**longitud = 2**
3	03_V1	Valor de la versión mayor
4	03_V2	Valor de la versión menor.

- Versión del módulo de inspección.

Byte	Campo	Descripción
0	**T**	**0x04**
1…2	**L**	**longitud = 2**
3	04_V1	Valor de la versión mayor
4	04_V2	Valor de la versión menor.

- Datos de comprobación para el desarrollador.

  Este registro siempre contendrá la misma información y podrá ser utilizada para determinar la correcta interpretación de los valores.

Byte	Campo	Descripción
0	**T**	**0x05**
1…2	**L**	**longitud = 7**
3	05_TEST1	Valor de test de 1 byte = 100000011b = 0x83 = **131**
4…5	05_TEST2	Valor de test de 2 bytes = 10000011 11100001b = 0x83E1 = **33761**
6…9	05_TEST3	Valor de test de 4 bytes = 00000001 00000011 00000111 00001111 = 0x103070F = **16975631**

5.2. INIT

5.2.1. Descripción y uso.

Esta función marca el inicio de la con un TAG, inicializa todo el entorno de control de la librería y establece los valores de inicio necesarios según la operativa indicada.

Es de obligatoria llamada antes de comenzar a operar con un nuevo TAG presente y solo debe realizarse 1 vez esta llamada al inicio para toda la operativa con dicho TAG.

La llamada a esta función provocará el "reset" interno de las variables que utiliza la librería para operar, una llamada en medio de un ciclo provocará un error en la transacción.

5.2.2. Sintaxis.

```
void Init(   const unsigned int id_operativa,
             const unsigned char * data_in,
              unsigned char * data_out )
```

5.2.3. Entradas.

const unsigned int id_operativa

Código que indica el tipo de operativa que se desea realizar.

Código	Operativa	Gestionado por el módulo
1	Compra	Venta
2	Recarga	Venta
3	Particularización (no es posible su anulación)	Venta
4	Consulta información	Inspección
5	Devolución	Venta
6	Sustitución	Venta
7	Regularización de saldo	Venta
8	Anulación	Venta
10	Cancelación	Cancelación
11	Anulación de la última cancelación	Cancelación

const unsigned char *data_in

Array de registros TLV con la información de los parámetros de inicio necesarios para realizar la operativa indicada.

- **Registro de datos de situación actual (módulo de cancelación).**

  Parámetros básicos de la situación lógica del equipo que va a efectuar la operativa.

  Aplicable a la red : Todas.

	Código	Operativa	
Necesario para	1	Compra	
	2	Recarga	
	3	Particularización (no es posible su anulación)	
	4	Consulta información	
	5	Devolución	
	6	Sustitución	
	7	Regularización de saldo	
	8	Anulación	
	10	Cancelación	•
	11	Anulación de la última cancelación	•

Byte	Campo	Descripción
0	**T**	**0xC0**
1…2	**L**	**Longitud = 12**
3	C0_RED	Código de identificador de la red de integración. * Ver redes soportadas.
4	C0_OPERADOR	Código de identificación operador
5	C0_ZONA	Código de la zona actual
6	C0_SZONA	Código de la subzona actual
7…8	C0_LINEA	Código de la línea
9…10	C0_PARADA	Código de la parada
11	C0_SENTIDO	Código del sentido: **Para sistemas cerrados**: 0 = Ida; 1 = vuelta; 2 = Circular ida; 3 = Circular vuelta; 9 = sin sentido **Para sistemas abiertos**: 0 = Entrada; 1 = Salida
12	C0_SISTEMA	Sistema 0 = Sistema abierto. 1 = Sistema cerrado
13…14	C0_COMERCIO	Número del comercio

- **Registro de datos de situación actual (módulo de ventas).**

  Parámetros básicos de la situación lógica del equipo que va a efectuar la operativa.

  Aplicable a la red: Todas.

	Código	Operativa	
Necesario para	1	Compra	•
	2	Recarga	•
	3	Particularización (no es posible su anulación)	•
	4	Consulta información	
	5	Devolución	•
	6	Sustitución	•
	7	Regularización de saldo	•
	8	Anulación	•
	10	Cancelación	
	11	Anulación de la última cancelación	

Byte	Campo	Descripción
0	**T**	**0xC1**
1…2	**L**	**Longitud = 6**
3	C1_RED	Código de identificador de la red de integración. * Ver redes soportadas.
4	C1_OPERADOR	Código de identificación operador
5	C1_ZONA	Código de la zona actual
6	C1_SZONA	Código de la subzona actual
7…8	C1_COMERCIO	Número del comercio

- **Registro de fecha y hora de operación.**

  Indica la fecha y hora "efectiva" de la operativa a realizar. Lo normal será indicar en estos campos la fecha y hora actual del sistema que realiza la operación.

  Aplicable a la red: Todas.

	Código	Operativa	
Necesario para	1	Compra	•
	2	Recarga	•
	3	Particularización (no es posible su anulación)	•
	4	Consulta información	
	5	Devolución	•
	6	Sustitución	•
	7	Regularización de saldo	•
	8	Anulación	•
	10	Cancelación	•
	11	Anulación de la última cancelación	•

Byte	Campo	Descripción
0	**T**	**0xC5**
1…2	**L**	**Longitud = 6**
3	**C5_DIA**	Día actual (1..31)

4	**C5_MES**	Mes actual (1..12)
5	**C5_ANO**	Año actual (17 = 2017)
6	**C5_HORA**	Hora actual (0..23)
7	**C5_MINUTO**	Minuto actual (0..59)
8	**C5_SEGUNDO**	Segundo actual (0..59)

- **Registro de parámetros auxiliares para la operativa de cancelación o anulación de la cancelación.**

  Parámetros adicionales necesarios indicar en la operativa de cancelación o anulación.

  Aplicable a la red: Todas.

	Código	Operativa	
Necesario para	1	Compra	
	2	Recarga	
	3	Particularización (no es posible su anulación)	
	4	Consulta información	
	5	Devolución	
	6	Sustitución	
	7	Regularización de saldo	
	8	Anulación	
	10	Cancelación	•
	11	Anulación de la última cancelación	•

Byte	Campo	Descripción
0	**T**	**0xC6**
1…2	**L**	**Longitud = 2**
3	**C6_MIN_PB**	Minutos para considerar passback también utilizado como tiempo de acompañante
4	**C6_MIN_ANUL**	Minutos para permitir anulación

- **Registro de tarificación dependiendo de saltos ubicados en la tarjeta.**

  Parámetros de la tarifa a aplicar en aquellas cancelaciones cuyo precio depende del número de saltos configurados en la propia tarjeta.

  Aplicable a la red: (1-Área de Sevilla).

	Código	Operativa	
Necesario para	1	Compra	
	2	Recarga	
	3	Particularización (no es posible su anulación)	
	4	Consulta información	
	5	Devolución	
	6	Sustitución	
	7	Regularización de saldo	
	8	Anulación	
	10	Cancelación	•
	11	Anulación de la última cancelación	

Byte	Campo	Descripción

0	**T**	**0xC7**
1…2	**L**	**Longitud = N** **los bytes 3 al 7 se repiten por cada salto/tarifa a indicar**
3	**C7_SALTOS**	Nº de saltos Valor entre 0 y 15
4…5	**C7_BASE**	Precio en céntimos de euro de tarifa base
6…7	**C7_ADICIO**	Precio en céntimos de euro para tarifa adicional.
…		

- **Registro de tarificación origen/destino.**

  Parámetros de la tarifa a aplicar en aquellas cancelaciones cuyo precio es obtenido según los saltos zonales producidos entre zona de origen (obtenida de los parámetros de situación actual y la zona destino indicada en este propio registro.

  Aplicable a la red: Todas.

	Código	Operativa	
Necesario para	1	Compra	
	2	Recarga	
	3	Particularización (no es posible su anulación)	
	4	Consulta información	
	5	Devolución	
	6	Sustitución	
	7	Regularización de saldo	
	8	Anulación	
	10	Cancelación	•
	11	Anulación de la última cancelación	

Byte	Campo	Descripción
0	**T**	**0xC8**
1…2	**L**	**Longitud = 7**
3	C8_ZDEST	Código de zona destino
4…5	C8_BASE	Precio en céntimos de euro de tarifa base
6…7	C8_ADICIO	Precio en céntimos de euro para tarifa adicional.
8…9	C8_PENALIZ	Precio en céntimos de euro de penalización por ruptura de transbordo.

La zona de origen es tomada del registro de situación actual.

- **Registro de parámetros de transbordo.**

  Información necesaria para determinar, durante el proceso de cancelación, si se ha producido transbordo o no.

Aplicable a la red: Todas.

	Código	Operativa	
Necesario para	1	Compra	
	2	Recarga	
	3	Particularización (no es posible su anulación)	
	4	Consulta información	
	5	Devolución	
	6	Sustitución	
	7	Regularización de saldo	
	8	Anulación	
	10	Cancelación	•
	11	Anulación de la última cancelación	

Byte	Campo	Descripción
0	**T**	**0xC9**
1…2	**L**	**Longitud = N** **Los bytes 6 al 15 se repiten por cada salto a indicar.**
3	C9_PET2	Porcentaje de control de descuento en transbordos para la segunda etapa
4	C9_PET3	Porcentaje de control de descuento en transbordos para la tercera y posteriores etapas.
5	C9_MGRA	minutos de gracia para transbordos
6	C9_SAL	Numero de saltos (entre 0 y 15)
7…8	C9_TG	Tiempo en minutos de tiempo máximo de transbordo global
9	C9_NG	Número máximo de transbordos globales
10…11	C9_TI	Tiempo en minutos de tiempo de transbordo interno
12	C9_NI	Número máximo de transbordos internos
13	C9_RIEI	Aplicar restricción IEI (Interno Externo Interno)
14	C9_TP	Tipo de tiempo de prevalencia (0=global/1=interno)
15	C9_NP	Numero de prevalencia (0=global/1=interno)
…		

- **Registro de tipo de información a solicitar.**

  Indica que tipo de información se debe obtener en la operativa de Consulta de Información. En el apartado de detalles de la función "GetInfo" se detalla cada uno de los campos que estarán disponibles como resultado en la ejecución de esta función.

  Se debe tener en cuenta, que cuanta más información es solicitada, será necesario realizar más operativas de acceso y lectura a la tarjeta, lo que conllevará más tiempo de proceso.

  Aplicable a la red: Todas.

	Código	Operativa	
Necesario para	1	Compra	
	2	Recarga	
	3	Particularización (no es posible su anulación)	
	4	Consulta información	•

	5	Devolución	
	6	Sustitución	
	7	Regularización de saldo	
	8	Anulación	
	10	Cancelación	
	11	Anulación de la última cancelación	

Byte	Campo	Descripción
0	**T**	**0xCA**
1…2	**L**	**Longitud = 1**
3	CA_TIPO	Tipo de información a solicitar **1** = Información básica de la tarjeta. Se comprende los datos de titularidad de la tarjeta e identificación y saldos del título. **2** = Información general de la tarjeta. Además de la información anterior, se añade el estado del viaje actual. **3** = Información completa de la tarjeta. Además de la información anterior, se añade todos los registros históricos de uso, de cargas y de reservas.

- **Registro de importe.**

  Indica que importe debemos utilizar para realizar la operativa de carga/recarga y regularización del saldo.

  Aplicable a la red: Todas.

	Código	Operativa	
Necesario para	**1**	Compra	•
	2	Recarga	•
	3	Particularización (no es posible su anulación)	
	4	Consulta información	
	5	Devolución	
	6	Sustitución	
	7	Regularización de saldo	•
	8	Anulación	
	10	Cancelación	
	11	Anulación de la última cancelación	

Byte	Campo	Descripción
0	**T**	**0xCB**
1…2	**L**	**Longitud = 5**
3	CB_SIGNO	Signo del importe. Solo tiene sentido para la operativa de regularización de saldo. 0 = Positivo 1 = Negativo.
4…7	CB_IMPTE	Importe representado en céntimos de euro.

- **Registro de cantidad de pasajeros para anular.**

  Indica un valor de cantidad de pasajeros necesaria para la operativa de anulación.

Aplicable a la red: Todas.

	Código	Operativa	
Necesario para	1	Compra	
	2	Recarga	
	3	Particularización (no es posible su anulación)	
	4	Consulta información	
	5	Devolución	
	6	Sustitución	
	7	Regularización de saldo	
	8	Anulación	
	10	Cancelación	
	11	Anulación de la última cancelación	•

Byte	Campo	Descripción
0	**T**	**0xCC**
1…2	**L**	**Longitud = 1**
3	CC_VIAJEROS	Cantidad de pasajeros

5.2.4. Salidas.

unsigned char *data_out

La función "Init" solo ofrece información general.

5.3. PROCESS

5.3.1. Descripción y uso.

Función que centraliza todas las operaciones a realizar con la tarjeta presente según la operativa indicada en la función "Init()", que obligatoriamente deber haber sido llamada con anterioridad.

La primera llamada a la función "Process()", la que inicia el ciclo, necesita solo el registro de información del TAG presente, registro de Tipo **0xB0**. A partir de dicho momento el HOST debe atender al código de retorno proporcionado, para la continuación o interrupción del ciclo.

- En caso de retorno **= 2** erróneo, el HOST debe obtener el LastError y el GetInfo para determinar el motivo del error y la información a mostrar al viajero.
- En caso de retorno **= 0**, el HOST debe "ejecutar" las acciones recibidas en el array "data_out" y conformar el array "data_in" para realizar una nueva llamada a la función "Process()" [1] (ciclo).
- En caso de retorno **= 1**, el HOST debe "ejecutar" las acciones recibidas en el array "data_out", en caso de que los hubiera. Si no fuera necesario ejecutar ninguna acción, el array "data_out" solo contendrá el registro de cabecera con el campo F1_NREG a 0. Tras ello, obtener los datos con el uso de la función "GetInfo()" para ofrecer la información al viajero.
- Es necesario que la ejecución de las acciones recibidas se realicen "**en el mismo orden**" que están establecidas en el array "data_out".
- En caso de que la ejecución de alguna acción produzca un error, el HOST NO debe continuar con la ejecución de las acciones y solo informar de nuevo la función "Process()" con las que ya hubiere ejecutado, por supuesto, incluyendo la que produjo el error.
- Se entiende pues, que mientras la función "Process()" retorne el valor 0 (correcto y continuar), el HOST debe permanecer en el ciclo de llamadas.

5.3.2. Sintaxis.

```
unsigned int Process(      const unsigned char *data_in,
                           unsigned char *data_out )
```

5.3.3. Entradas.

const unsigned char *data_in

Registros TLV con la información según el ciclo actual del proceso.

En la primera llamada solo contendrá el registro con la información de la tarjeta presente (0xB0) y en las llamadas restantes contendrá la información de resultado requerida por las

[1] Información más detallada en el punto "relación de acciones ←→ respuestas"

acciones obtenidas en el array "data_out" retornado de la función "Process()" del ciclo anterior.

- **Información del TAG presente.**

  Registro especial de obligado uso y único (junto con el registro de cabecera) en la primera llamada a la función "Process()".

  Tras la llamada a la función "Init()", la primera llamada a la función "Process()" debe ser con este registro, el cual contiene la información e identificación de la tarjeta TAG que va a ser tratada.

Byte	Campo	Descripción
0	**T**	**0xB0**
1…2	**L**	**Longitud = 10**
3…9	B0_UID_TAG	7 bytes correspondientes al UID del TAG presente
10…11	B0_ATQA	2 bytes de la respuesta del request efectuado a la tarjeta
12	B0_SAK	1 byte de la respuesta de aceptación del comando select efectuado a la tarjeta

- **Información de resultado en la ejecución de la acción.**

  Utilizado como respuesta de las acciones 0x10 (autenticar), 0x14 (seleccionar aplicación), 0x19 (grabar archivo), 0x1B (incrementar valor), 0x1C (decrementar valor), 0x1D (incrementar valor crédito), 0x1E (grabar registro), 0x20 (vaciar registros), 0x21 (confirmar transacciones) y 0x22 (invalidar transacciones), además de en cualquier caso de error producido en la acción.

Byte	Campo	Descripción
0	**T**	**0xB1**
1…2	**L**	**Longitud=4**
3	B1_CID	Código de identificación de la acción.
4	B1_UNIDAD	Código de la unidad que ha producido el error 0 = Sin unidad, solo para el caso de correcto. 1 = Lector 2 = TAG 30 = Centro autorizador Consorcial
5…6	B1_RES	Código de resultado producido, según tablas adjuntas.

  - De la unidad Lector y TAG

B1_RES	Estado	Descripción
0x0000	CORRECTO	Acción realizada correctamente.

0x000C	NO_CHANGES	No se han realizado cambios, no es necesario CommitTransaction / AbortTransaction
0x000E	OUT_OF_EEPROM_ERROR	No hay suficiente NV-Memory para completar el comando
0x001C	ILLEGAL_COMMAND_CODE	Código de comando no soportado
0x001E	INTEGRITY_ERROR	CRC o MAC No coinciden los datos, los bytes no son válidos.
0x0040	NO_SUCH_KEY	No es válido el ID de clave especificado.
0x007E	LENGTH_ERROR	Longitud de comando no valido.
0x009D	PERMISSION_DENIED	La configuración actual no admite el comando solicitado
0x009E	PARAMETER_ERROR	Valor del parámetro no valido.
0x00A0	APPLICATION_NOT_FOUND	Aplicación no existe en el PICC
0x00A1	APPL_INTEGRITY_ERROR	Error irreparable en la aplicación, esta será deshabilitada.
0x00AE	AUTHENTICATION_ERROR	La autentificación actual no permite el comando solicitado
0x00AF	ADDITIONAL_FRAME	Additional data frame is expected to be sent
0x00BE	BOUNDARY_ERROR	La lectura o escritura excede los límites del archivo.
0x00C1	PICC_INTEGRITY_ERROR	Error irreparable con el PICC, este será deshabilitado.
0x00CA	COMMAND_ABORTED	Previous Command was not fully completed Not all Frames were requested or provided by the PCD
0x00CD	PICC_DISABLED_ERROR	El PICC está deshabilitado por un error irreparable
0x00CE	COUNT_ERROR	El número de aplicaciones está limitado a 28, imposible crear más.
0x00DE	DUPLICATE_ERROR	La creación del archivo o aplicación ha fallado porque ya existe
0x00EE	EEPROM_ERROR	No se puede completar la operación de escritura en la NV-Memory debido a perdida de alimentación, se ha activado el mecanismo de backup/rollback interno *
0x00F0	FILE_NOT_FOUND	El archivo no existe
0x00F1	FILE_INTEGRITY_ERROR	Error irreparable con el archivo, este será deshabilitado *
0xFFnn	GENERAL_ERROR	Error general con código indicado en nn

- De la unidad Centro Autorizador Consorcial.

  En este caso, código correcto no existe, puesto que las respuestas correctas del centro autorizador son transmitidas con un TLV diferente a este.

B1_RES	Estado	Descripción
0x0001	SIN_COMUNICACIÓN	No ha sido posible conectar con el centro autorizador.
0x0002	SIN_RESPUESTA	Se ha establecido la conexión pero no se recibe respuesta en el tiempo establecido.
0x0003	SIN_RESPUESTA_LOGICA	Se ha recibido respuesta, pero no cumple el formato adecuado.

- **Información de las propiedades de la clave maestra de la aplicación actualmente seleccionada.**

  Utilizado como respuesta de la acción 0x45 (Propiedades de la clave maestra).

Byte	Campo	Descripción
0	**T**	**0xB2**
1…2	**L**	**Longitud = 3**
3	B2_CID	Código de identificación de la acción.
4	B2_KS	1 byte con la información de las propiedades de la clave maestra según las especificaciones técnicas de la tarjeta DESFIRE EV2. En caso de AID = 00 00 00 bit7 bit6 bit5 bit4 bit3 bit2 bit1 bit0

RFU	flag que indica que la MK es necesaria para modificar estas propiedades.	flag que indica que es necesaria la MK para borrar/crear aplicaciones	flag que indica que es necesaria la MK para listar aplicaciones	flag que indica que es necesaria la MK para cambiar la MK (=0 indica MK congelada)		

En caso de AID ≠ 00 00 00

bit7	bit6	bit5	bit4	bit3	bit2	bit1	bit0
0x0 = APK necesaria para cambiar la APK 0x1 … 0xD = La clave de aplicación especificada es necesaria para cambiar las claves. 0xE = Autentificación con la misma clave es necesaria para cambiar la clave. 0xF =Todas las claves, excepto la APK están congeladas.				flag que indica que la APK es necesaria para modificar estas propiedades.	flag que indica que es necesaria la APK para borrar/crear archivos	flag que indica que es necesaria la APK para listar archivos	flag que indica que es necesaria la APK para cambiar la APK (=0 indica APK congelada)

.

5	B2_NK	1 byte con el número de claves que la aplicación tiene alojadas. En caso de que la aplicación actualmente seleccionada sea la AID = 00 00 00, este valor será 1.

- **Información de la versión de claves solicitada.**

  Utilizado como respuesta de la acción 0x64 (Leer versión de claves).

Byte	Campo	Descripción
0	**T**	**0xB3**
1…2	**L**	**Longitud = 2**
3	B1_CID	Código de identificación de la acción.

4	B3_KV	1 byte indicando la versión de claves

- **Lista de aplicaciones existentes en la tarjeta.**

  Utilizado como respuesta de la acción 0x6A (Listar aplicaciones).

  Para la operativa de esta acción la aplicación AID = 00 00 00 debe estar seleccionada previamente.

Byte	Campo	Descripción
0	**T**	**0xB4**
1…2	**L**	**Longitud.** **Depende de la cantidad de AIDs contenidas en el registro.** **En caso de no existir ninguna aplicación en la tarjeta, se indicara en la longitud un valor de 0.** **En esta lista NO debe incluirse la aplicación maestra AID = 00 00 00, ya que se considera que esta siempre existe en la tarjeta.**
3	B4_CID	Código de identificación de la acción.
4…6	$B4_AID_0$ … $B4_AID_N$	3 bytes por cada identificación de aplicación AID obtenida de la tarjeta
…		

- **Información de la versión de fabricación de la tarjeta.**

  Utilizado como respuesta de la acción 0x60 (Información de la tarjeta).

  Informará con toda la información de las especificaciones de la tarjeta presente.

Byte	Campo	Descripción	
0	**T**	**0xB5**	
1…2	**L**	**Longitud = 29**	
3	B5_CID	Código de identificación de la acción.	
4	B5_HVID	Información hardware	código del vendedor
5	B5_HTI		Código del tipo
6	B5_HST		Código del subtipo
7	B5_HMAV		Código de la versión Mayor
8	B5_HMIV		Código de la versión menor
9	B5_HSZ		Código del tamaño de almacenamiento
10	B5_HCP		Código del tipo de protocolo de comunicaciones
11	B5_SVID	Información del software	código del vendedor
12	B5_STI		Código del tipo
13	B5_SST		Código del subtipo

14	B5_SMAV		Código de la versión Mayor
15	B5_SMIV		Código de la versión menor
16	B5_SSZ		Código del tamaño de almacenamiento
17	B5_SCP		Código del tipo de protocolo de comunicaciones
18...24	B5_UID	Identificador único de la tarjeta	
25...29	B5_BNO	Número de lote de producción	
30	B5_CWP	Código de la semana de producción.	
31	B5_YP	Código del año de producción.	

- **Lista de archivos existentes en la aplicación actualmente seleccionada.**

  Utilizado como respuesta de la acción 0x6F (Listar archivos).

Byte	Campo	Descripción
0	**T**	**0xB6**
1...2	**L**	**Longitud** **Depende de la cantidad de archivos FIDs contenidos en la aplicación actualmente seleccionada.** **En caso de no existir ningún archivo en la aplicación, se indicara en la longitud un valor de 1.** **Esta acción no es posible realizarse si la aplicación seleccionada en la tarjeta es la AID = 00 00 00, ya que esta NO puede contener archivos.**
3	B6_CID	Código de identificación de la acción.
4	FID_0 ... FID_N	1 byte por cada identificación de archivo FID obtenido de la aplicación.
...		

- **Propiedades de un archivo.**

  Utilizado como respuesta de la acción 0xF5 (Información de archivo).

  La información suministrada en este registro depende del tipo de archivo al cual se refiera, nos podemos encontrar con 5 diferentes agrupados en 3 tipos, datos estándar (archivos de tipo 0x00 y 0x01), valor (de tipo 0x02) o registros (de tipo 0x03 y 0x04).

  - **Información de archivo de datos estándar (0x00) o de backup (0x01)**

Byte	Campo	Descripción
0	**T**	**0xB7**
1...2	**L**	**Longitud = 9**
3	B7_CID	Código de identificación de la acción. 0xB7: Propiedades del archivo.
4	B7_FID	Código de identificación del archivo

5	B7_FT	Puede ser 0x00 = Archivo estándar 0x01 = Archivo estándar de backup.
6	B7_CC	Configuración de las comunicaciones. 0x00 = Comunicaciones en plano. 0x01 = Comunicaciones en plano aseguradas con DES/3DES por MAC 0x02 = Comunicaciones aseguradas con cifrado DES/3DES completo
7…8	B7_ACC	Condiciones o derechos de acceso. Indica con que numero de clave de la aplicación donde está ubicado el archivo se puede hacer la acción requerida. <table><tr><th>bit15 … bit12</th><th>bit11 … bit8</th><th>bit7 … bit4</th><th>bit3 … bit0</th></tr><tr><td>lectura</td><td>Escritura</td><td>Lectura/Escritura</td><td>Cambiar condiciones de acceso</td></tr></table> En cada una de las agrupaciones de 4 bits arriba detalladas, se establece el valor del número de clave (número de clave que debe estar alojada en la aplicación contenedora del archivo), con la cual es necesario realizar la "autentificación" en la aplicación para poder tener el acceso que indica la agrupación en concreto. Existe 3 valores, además del número de clave que puede ser posible indicar: 0 = APK, indica que es necesario la clave maestra de la aplicación. 0xE = Acceso libre, no es necesario ninguna autentificación. 0xF = Acceso congelado o sin acceso.
9…11	B7_TAM	Tamaño del archivo

- **Información de archivo de valor (0x02).**

Byte	Campo	Descripción
0	**T**	**0xB7**
1…2	**L**	**Longitud = 19**
3	B7_CID	Código de identificación de la acción.
4	B7_FID	Código de identificación del archivo
5	B7_FT	0x02 = Archivo de tipo valor.
6	B7_CC	Configuración de las comunicaciones. (ver archive standard)
7…8	B7_ACC	Condiciones o derechos de acceso. (ver archive standard)
9…12	B7_VAL_MIN	Valor mínimo permitido.
13…16	B7_VAL_MAX	Valor máximo permitido.
17…20	B7_LIM_CRE	Valor del límite del crédito permitido.
21	B7_CRE	Flag que indica si el crédito limitado está permitido =1 o no =0.

- **Información de archivo de datos registros linear (0x03) o cíclicos (0x04).**

Byte	Campo	Descripción
0	**T**	**0xB7**
1…2	**L**	**Longitud = 15**
3	B7_CID	Código de identificación de la acción.
4	B7_FID	Código de identificación del archivo
5	B7_FT	Puede ser 0x03 = Archivo de registros lineales. 0x04 = Archivo de registros cíclicos.
6	B7_CONF	Configuración de las comunicaciones. (ver archive standard)
7…8	B7_ACCESS	Condiciones o derechos de acceso. (ver archive standard)
9…11	B7_TAM_REG	Tamaño del registro (1 solo registro)
12…14	B7_MAX_REG	Cantidad máxima de registros que admite.
15…17	B7_CUR_REG	Cantidad actual de registros almacenados. Este número es igual al máximo número de registros que pueden ser leídos del archivo.

- **Datos de lectura de un archivo estándar.**

Utilizado como respuesta de la acción 0xBD (Leer archivo).

Byte	Campo	Descripción
0	**T**	**0xB8**
1…2	**L**	**Longitud a especificar dependerá de la longitud del campo info**
3	B8_CID	Código de identificación de la acción.
4…6	B8_AID	3 bytes del Identificador de la aplicación contenedora del archivo
7	B8_FID	1 byte del Identificador del archivo
8…N	B8_INFO	N bytes correspondientes a la información leída del archivo.

- **Datos de lectura de un archivo de valor.**

Utilizado como respuesta de la acción 0x6C (Leer valor).

Byte	Campo	Descripción
0	**T**	**0xB9**
1…2	**L**	**Longitud = 9**
3	B9_CID	Código de identificación de la acción.
4…6	B9_AID	3 bytes del Identificador de la aplicación contenedora del archivo

7	B9_FID	1 byte del Identificador del archivo
8…11	B9_VALOR	4 bytes con el valor del archivo

- **Datos de lectura del registro de un archivo de registros.**

  Utilizado como respuesta de la acción 0xBB (Leer registro)

Byte	Campo	Descripción
0	**T**	**0xBA**
1…2	**L**	**Longitud depende de la longitud del valor**
3	BA_CID	Código de identificación de la acción.
4…6	BA_AID	3 bytes del Identificador de la aplicación contenedora del archivo.
7	BA_FID	1 byte del Identificador del archivo.
8	BA_REG	1 byte indicando el registro leído, entre 0 y número existente de registros -1, siendo 0 el último almacenado cronológicamente.
9…N	BA_VALOR	N bytes correspondientes a la información leída del registro del archivo.

- **Datos de respuesta de petición del Centro Autorizador del Consorcio.**

  Utilizado como respuesta de la acción 0x30 (Operativa con el Centro Autorizador)

Byte	Campo	Descripción
0	**T**	**0xBB**
1…2	**L**	**=N**
3	B_CID	Código de identificación de la acción.

Pendiente de definición

5.3.4. Salidas.

unsigned int

Código de retorno de la función.

Código	Detalles
0	Correcto y continuar
1	Correcto y finalizar

2	Error de proceso

unsigned char *data_out

En caso de error "código de retorno = 2"

En caso de que el código de retorno de la función sea **2=Error**, Es indicativo que se ha producido un error de SISTEMA (por ejemplo algún parámetro erróneo, o falta algún parámetro esencial).

El contenido de *data_out incluirá el array TLV con la información del error producido.

El campo F1_CNT en el registro de cabecera no será gestionado y tendrá un valor 0.

> No debe confundirse este registro de error con, por ejemplo una *validación de rechazo*, esta última NO será informada como error, sino como *1=correcto y finalizar*, ya que la función "GetInfo()" será la encargada de informar del resultado de la operativa con la tarjeta.

- **Información de error producido.**

Byte	Campo	Descripción
0	**T**	**0x99**
1…2	**L**	**longitud = 3**
3	99_MOD	1 byte con el código del módulo que produjo el error
4…5	99_CERR	2 bytes con el código del error producido, es dependiente del modulo Ver capítulo 8 para la relación de errores.

Referencias a la tabla de errores en el documento "Tabla de códigos de error de la funcion Process"

En caso de correcto, "código de retorno = 0 o 1"

En cualquier otro caso, el contenido de *data_out incluye el array de registros (uno por cada acción) con las acciones que son necesario ejecutar por el HOST.

En caso de no existir ninguna acción a ejecutar, solo contendrá el registro de cabecera con el campo N_REG=0.

Las acciones recibidas deben ser ejecutadas por el HOST en el estricto orden en el que se han recibido en el array. Cada acción está identificado por un valor único y secuencial CID que identifica dicha acción en caso de producirse algún error en su ejecución (ver registro 0xB1 en "data_in").

Si el HOST, durante la ejecución de las acciones, se produjera un error, debe interrumpir el proceso e informar a la librería mediante la llamada a la función "Process()" con el registro 0xB1.

- **Autentificación.**

Byte	Campo	Descripción
0	**T**	**0x10**
1…2	**L**	**Longitud = N.**
3	10_CID	Código de identificación de la acción
4	10_KN	Índice de la clave en la tarjeta (0..13)
5	10_KT	Tipo de encriptación de la clave. 0 = DES/3DES (Clave 0AKEY de 8 bytes) 1 = 3KDES (Clave 0AKEY de 24 bytes) 2 = AES (Clave 0AKEY de 16 bytes)
6…N	10_KEY	La clave, su tamaño variara dependiendo del tipo de encriptación 0A_KT.

- **Obtener la configuración de la APK de la aplicación actualmente seleccionada.**

Byte	Campo	Descripción
0	**T**	**0x11**
1…2	**L**	**Longitud = 1**
3	11_CID	Código de identificación de la acción

- **Leer versión de una clave de la aplicación actualmente seleccionada.**

Byte	Campo	Descripción
0	**T**	**0x12**
1…2	**L**	**Longitud = 2**
3	12_CID	Código de identificación de la acción
4	12_KN	1 byte que especifica el número de clave de la cual se solicita la versión. En caso de que la aplicación actualmente seleccionada sea la AID= 00 00 00, este valor debe ser =0, en caso contrario, AID ≠ 00 00 00, el valor debe ser entre 0 y el máximo de claves alojadas en dicha aplicación.

- **Listar aplicaciones existentes en la tarjeta.**

Byte	Campo	Descripción

0	**T**	**0x13**
1…2	**L**	**Longitud = 1**
3	13_CID	Código de identificación de la acción

- **Selección de una aplicación.**

Byte	Campo	Descripción
0	**T**	**0x14**
1…2	**L**	**Longitud = 4**
3	14_CID	Código de identificación de la acción
4…6	14_AID	3 bytes del código de identificación de la aplicación a seleccionar

- **Obtener información de fabricación de la tarjeta.**

Byte	Campo	Descripción
0	**T**	**0x15**
1…2	**L**	**Longitud = 1**
3	15_CID	Código de identificación de la acción

- **Listar archivos de la aplicación actualmente seleccionada.**

Byte	Campo	Descripción
0	**T**	**0x16**
1…2	**L**	**Longitud = 1**
3	16_CID	Código de identificación de la acción

- **Obtener información de un archivo de la aplicación actualmente seleccionada.**

Byte	Campo	Descripción
0	**T**	**0x17**
1…2	**L**	**Longitud = N**
3	17_CID	Código de identificación de la acción
4	17_FID	Código de identificación del archivo del que se solicita la información.

- **Lectura de archivo estándar de datos.**

Byte	Campo	Descripción
0	**T**	**0x18**
1…2	**L**	**Longitud = 9**
3	18_CID	Código de identificación de la acción
4	18_FID	1 byte de código de identificación del archivo a leer.
5	18_CS	Cifrado de la comunicación 0 = Comunicación plana 1 = Cifrado por DES/3DES MACing 3 = Cifrado completo DES/3DES
6…8	18_POS	Posición de inicio de la lectura.
9…11	18_LONG	Longitud de datos que se desean leer.

- **Escritura en archivo estándar de datos.**

Byte	Campo	Descripción
0	**T**	**0x19**
1…2	**L**	**Longitud = N, depende del tamaño de la información a escribir.**
3	19_CID	Código de identificación de la acción
4	19_FID	1 byte de código de identificación del archivo a escribir
5	19_CS	Cifrado de la comunicación 0 = Comunicación plana 1 = Cifrado por DES/3DES MACing 3 = Cifrado completo DES/3DES
6…8	19_POS	Posición de inicio de la escritura.
9…N	19_INFO	N bytes de la información a grabar en el archivo.

- **Lectura de archivo de valor.**

Byte	Campo	Descripción
0	**T**	**0x1A**
1…2	**L**	**Longitud = 3**
3	1A_CID	Código de identificación de la acción
4	1A_FID	1 byte de código de identificación del archivo a leer.
5	1A_CS	Cifrado de la comunicación 0 = Comunicación plana 1 = Cifrado por DES/3DES MACing

		3 = Cifrado completo DES/3DES

- **Incremento (Credit) de archivo de valor.**

Byte	Campo	Descripción
0	**T**	**0x1B**
1…2	**L**	**Longitud = 7**
3	1B_CID	Código de identificación de la acción
4	1B_FID	1 byte de código de identificación del archivo a incrementar el valor.
5	1B_CS	Cifrado de la comunicación 0 = Comunicación plana 1 = Cifrado por DES/3DES MACing 3 = Cifrado completo DES/3DES
6…9	1B_VALOR	Valor de incremento.

- **Decremento (Debit) de archivo de valor.**

Byte	Campo	Descripción
0	**T**	**0x1C**
1…2	**L**	**Longitud = 7**
3	1C_CID	Código de identificación de la acción
4	1C_FID	1 byte de código de identificación del archivo a incrementar el valor.
5	1C_CS	Cifrado de la comunicación 0 = Comunicación plana 1 = Cifrado por DES/3DES MACing 3 = Cifrado completo DES/3DES
6…9	1C_VALOR	Valor de decremento.

- **Incremento limitado por el crédito establecido en archivo de valor.**

Byte	Campo	Descripción
0	**T**	**0x1D**
1…2	**L**	**Longitud = 7**
3	1D_CID	Código de identificación de la acción
4	1D_FID	1 byte de código de identificación del archivo a incrementar el valor.
5	1D_CS	Cifrado de la comunicación 0 = Comunicación plana

		1 = Cifrado por DES/3DES MACing 3 = Cifrado completo DES/3DES
6…9	1D_VALOR	Valor de incremento.

- **Escritura de datos en archivo de registros.**

Byte	Campo	Descripción
0	**T**	**0x1E**
1…2	**L**	**Longitud = 9**
3	1E_CID	Código de identificación de la acción
4	1E_FID	1 byte de código de identificación del archivo
5	1E_CS	Cifrado de la comunicación 0 = Comunicación plana 1 = Cifrado por DES/3DES MACing 3 = Cifrado completo DES/3DES
6…8	1E_POS	Posición de inicio en bytes de inicio de la grabación de los datos dentro del propio registro. (entre 0 y 3B_DATOS-1)
9…11	1E_LNG	Longitud de información a escribir (entre 1 y 3B_DATOS - 3B_POS)
12…N	1E_DATOS	Información a escribir.

- **Lectura de archivo de registros.**

Byte	Campo	Descripción
0	**T**	**0x1F**
1…2	**L**	**Longitud = 9**
3	1F_CID	Código de identificación de la acción
4	1F_FID	1 byte de código de identificación del archivo
5	1F_CS	Cifrado de la comunicación 0 = Comunicación plana 1 = Cifrado por DES/3DES MACing 3 = Cifrado completo DES/3DES
6…8	1F_REGP	Registro de inicio que desea ser leído, entre 0 y número de registros existentes -1, siendo 0 el último registro almacenado.
9…11	1F_REGN	Cantidad de registros a leer, comenzando siempre por el ultimo insertado y en orden cronológico. En caso de indicar 0, deberá ser leído todos los registros existentes.

- **Vaciado/borrado completo de archivo de registros.**

Byte	Campo	Descripción

0	**T**	**0x20**
1…2	**L**	**Longitud = 3**
3	20_CID	Código de identificación de la acción
4	20_FID	1 byte de código de identificación del archivo que se desea vaciar.
5	20_CS	Cifrado de la comunicación 0 = Comunicación plana 1 = Cifrado por DES/3DES MACing 3 = Cifrado completo DES/3DES

- **Confirmación de transacciones.**

  Repercutirá en todas las transacciones efectuadas en los archivos que dispongan de backup (estándar con backup, valor y registros).

Byte	Campo	Descripción
0	**T**	**0x21**
1…2	**L**	**Longitud = 1**
3	21_CID	Código de identificación de la acción

- **Invalidación de todas las transacciones.**

  Repercutirá a todas las efectuadas hasta el momento en los archivos que dispongan de backup (estándar con backup, valor y registros).

Byte	Campo	Descripción
0	**T**	**0x22**
1…2	**L**	**Longitud = 1**
3	22_CID	Código de identificación de la acción

- **Solicitud de operativa con el Centro Autorizador.**

  En determinados casos de necesidad por la operativa en ejecución, será necesario que el HOST efectúe comunicaciones (conexión, envío y recepción) con el Centro Autorizador Consorcial *OpSin*. En esta acción, la librería suministrara una relación de datos que serán necesarios para efectuar la comunicación.

  Sera responsabilidad del HOST realizar los mecanismos parametrizados para llevar a cabo correctamente dicha conexión, envío y recepción de datos de respuesta del Centro Autorizador.

Byte	Campo	Descripción
0	**T**	**0x3**

Pendiente de definición

1…2	L	Longitud = N
3	30_CID	Código de identificación de la acción
4…10	30_UID	Identificador único de la tarjeta
11	30_TPET	Código del tipo de petición a realizar 1 = Venta 2 = Recarga
12…N	30_DAT	Datos de la solicitud

5.3.5. Relación de Acciones <-> Respuestas.

Como se ha detallado, la funcion "Process()" envía en su "data_out" las acciones a realizar por el HOST y espera en su próxima llamada que en "data_in" se especifique el resultado de todas las ordenes realizadas.

Esto indica que cada acción solicitada tiene específicamente una respuesta concreta que ofrecer en caso de éxito, o una respuesta estándar en caso de error.

Aquí indicamos una tabla de correspondencia entre las acciones que pueden solicitar la función y las respuestas esperadas.

Acción	Descripción	Respuesta Éxito	Respuesta Fracaso
0x10	Autentificar	0xB1	0xB1
0x11	**Propiedades de la aplicación**	**0xB2**	0xB1
0x12	**Leer versión claves**	**0xB3**	0xB1
0x13	**Listar aplicaciones**	**0xB4**	0xB1
0x14	Seleccionar aplicación	0xB1	0xB1
0x15	**Información de fábrica**	**0xB5**	0xB1
0x16	**Listar archivos**	**0xB6**	0xB1
0x17	**Información archivo**	**0xB7**	0xB1
0x18	**Leer archivo**	**0xB8**	0xB1
0x19	Grabar archivo	0xB1	0xB1
0x1A	**Leer valor**	**0xB9**	0xB1
0x1B	Incrementar valor	0xB1	0xB1
0x1C	Decrementar valor	0xB1	0xB1
0x1D	Incrementar valor crédito	0xB1	0xB1
0x1E	Grabar registro	0xB1	0xB1
0x1F	**Leer registro**	**0xBA**	0xB1

0x20	Vaciar registros	0xB1	0xB1
0x21	Confirmar (commit)	0xB1	0xB1
0x22	Invalidar (rollback)	0xB1	0xB1
0x30	Operativa con el Centro Autorizador	**0xBB**	0xB1

5.4. LASTERROR

5.4.1. Descripción y uso.

Su cometido es informar del ultimo error registrado por la librería, básicamente debe ser llamada cada vez que la función "Process()" devuelva un resultado = 2 (error).

5.4.2. Sintaxis.

void LastError(unsigned char *data_out)

5.4.3. Entradas.

Ninguna.

5.4.4. Salidas.

unsigned char *data_out

*Hacer referencia al data_out en caso de error de la funcion "Process()"

5.5. GETINFO

5.5.1. Descripción y uso.

Una vez finalizado todo el proceso con la tarjeta, ya sea con éxito o sin él, esta función ofrece todos los datos necesarios para producir la información, tanto visual como impresa, que debe ofrecerse al usuario.

5.5.2. Sintaxis.

void GetInfo(unsigned char * data_out)

5.5.3. Entradas.

Ninguna

5.5.4. Salidas.

unsigned char *data_out

Array de registros TLV con los diferentes datos necesarios para su uso en la información al viajero.

- Resultado de operativa efectuada.

Byte	Campo	Descripción
0	**T**	**0x07**
1…2	**L**	**longitud = 2**
3…4	07_CRO	Código del resultado de la última operación efectuada. Ver tabla a continuación

Ámbito	Código 07_CRO	Descripción
General	0x0000	No hay operación efectuada
	0x0030	ERROR_CABECERA
	0x0031	ERROR_VARIABLES
	0x0032	ERROR_MONDERO
	0x0033	ERROR_HISTORICO
	0x0034	TARJETA_ANULADA
	0x0035	TARJETA_NO_OPERATIVA
	0x0036	ERROR_VERSION
	0x0037	ERROR_MODO_PRUEBAS
	0x0038	BLOQUES_VAR_ERRONEOS
	0x0039	HISTORICO_ERRONEO
	0x003A	ERROR_PUNTERO_VIAJES
	0x003B	ERROR_MAXIMO_MOVIMIENTOS

	0x003C	ERROR_PUNTERO_VARIABLES
	0x003D	ERROR_MATRIZ_RECUPERACION
Módulo de venta	0x0100	Error en venta
	0x0101	Venta correctamente efectuada
	0x0201	Recarga correctamente efectuada
Módulo de validación	0x0300	Error en Validación
	0x0301	CORRECTO_TEMPORAL
	0x0302	CORRECTO_TEMPORAL_TRANSBORDO
	0x030A	MONEDERO_CANCELACION_1
	0x030B	MONEDERO_CANCELACION_N
	0x030C	MONEDERO_TRANSBORDO_1
	0x030D	MONEDERO_TRANSBORDO_N
	0x0314	ANUL_CORRECTA
	0x0369	MENSUAL_CADUCADA
	0x036A	MENSUAL_PASSBACK
	0x036C	SIN_SALDO
	0x036D	ERROR_TIPO_BONO
	0x0370	SOBREPASO_VIAJEROS
	0x0377	ERROR_ID_CONSORCIO
	0x0378	ERROR_FECHA_LIMITE
	0x0379	PRECIO_9999
	0x037A	ERROR_SALTOS
	0x037B	OTRO_CONSORCIO
	0x037C	FORZAR_ACOMP_NO_PERMITIDO
	0x037D	ANUL_ERROR_CANTIDAD
	0x037E	ANUL_SIN_USO
	0x037F	ANUL_SOBREPASO_VIAJEROS
	0x0380	ANUL_FUERA_DE_AMBITO
	0x0381	ANUL_VIAJE_YA_ANULADO
Módulo de inspección	0x0400	Error en inspección
	0x0401	Inspección correctamente efectuada

- Información de campo numérico.

Byte	Campo	Descripción
0	**T**	**0x08**
1…2	**L**	**longitud = 9**
3…6	08_CC	Código de campo *Tabla de códigos de campo detallada a continuación.
7	08_SGN	Signo del valor 0 = positivo 1 = negativo
8…11	08_VALOR	Valor del campo

TABLA DE CODIGOS DE CAMPOS

La columna **C6_Tipo** indica que el campo será entregado en caso de solicitar dicho tipo de información. En el caso de solicitar información de la tarjeta.

La columna **Opcional** indica que dicho campo NO es esencial y por lo tanto no será devuelto por la función si no existe.

Ámbito	Código HEX	Descripción		C6_Tipo = 1	C6_Tipo = 2	C6_Tipo = 3	Opcional
Identificación de tarjeta	08 01 03 00	Propietario de la tarjeta		•	•	•	
	08 01 04 00	Responsable de numeración		•	•	•	
	08 01 05 00	Número de tarjeta		•	•	•	
	08 01 06 00	Digito de control		•	•	•	
	08 01 07 00	Modelo		•	•	•	
	08 01 0B 00	Mes de emisión		•	•	•	
	08 01 0C 00	Año de emisión		•	•	•	
	08 01 0F 00	Tipo de documento		•	•	•	
	08 01 10 00	Tipo de asistencia		•	•	•	
Identificación del titulo	08 10 30 00	Propietario del titulo		•	•	•	
	08 10 31 00	Número del titulo		•	•	•	
	08 10 32 00	Clase del titulo		•	•	•	
	08 10 34 00	Características 1 de tarifa		•	•	•	
	08 10 35 00	Características 2 de tarifa		•	•	•	
	08 10 36 00	Operatividad		•	•	•	
	08 10 37 00	Passback		•	•	•	
	08 10 38 00	Tipo de sistema de tarifas		•	•	•	
	08 11 3B 00	Clave aleatoria		•	•	•	
	08 13 30 00	Regularización económica	Propietario del titulo	•	•	•	
	08 13 31 00		Identificación del título	•	•	•	
	08 13 3D 00		Cantidad	•	•	•	
	08 13 3E 00		Signo	•	•	•	
	08 15 30 00	Restricción de uso	Propietario del titulo	•	•	•	•
	08 15 31 00		Identificación del título	•	•	•	•
	08 15 42 00		Uso	•	•	•	•
	08 16 30 00	Fechas de validez	Propietario del titulo	•	•	•	•
	08 16 31 00		Identificación del título	•	•	•	•
	08 16 4A 00		Año inicio validez	•	•	•	•
	08 16 4B 00		Mes inicio de validez	•	•	•	•
	08 16 4C 00		Día inicio de validez	•	•	•	•
	08 16 4D 00		Año fin de validez	•	•	•	•
	08 16 4E 00		Mes fin de validez	•	•	•	•
	08 16 4F 00		Día fin de validez	•	•	•	•
	08 18 30 00	Limitación horaria	Propietario del titulo	•	•	•	•
	08 18 31 00		Identificación del título	•	•	•	•
	08 18 52 00		Hora de inicio	•	•	•	•
	08 18 53 00		Hora final	•	•	•	•
	08 18 55 00		Lunes	•	•	•	•
	08 18 56 00		Martes	•	•	•	•
	08 18 57 00		Miércoles	•	•	•	•
	08 18 58 00		Jueves	•	•	•	•
	08 18 59 00		Viernes	•	•	•	•
	08 18 5A 00		Sábado	•	•	•	•
	08 18 5B 00		Domingo	•	•	•	•
Monedero	01 1F 00 00		Saldo en céntimos de euro	•	•	•	
Ultimo Movimiento **aa** **02** = Ultimo movimiento **05** = Última reserva	aa 20 60 00	Movimiento sin reserva	Numero de línea		•	•	
	aa 20 61 00		Flota		•	•	
	aa 20 4A 00		Año		•	•	
	aa 20 4B 00		Mes		•	•	
	aa 20 4C 00		Día		•	•	
	aa 20 62 00		Hora		•	•	
	aa 20 63 00		Minuto		•	•	
	aa 20 64 00		Sentido		•	•	
	aa 20 65 00		Consorcio		•	•	
	aa 20 66 00		Etapa		•	•	
	aa 20 67 00		Control sistemas cerrados		•	•	
	aa 21 60 00	Movimiento con reserva	Numero de línea		•	•	
	aa 21 61 00		Flota		•	•	
	aa 21 4A 00		Año		•	•	
	aa 21 4B 00		Mes		•	•	
	aa 21 4C 00		Día		•	•	
	aa 21 62 00		Hora		•	•	
	aa 21 63 00		Minuto		•	•	
	aa 21 64 00		Sentido		•	•	
	aa 21 65 00		Consorcio		•	•	
	aa 21 66 00		Etapa		•	•	
	aa 21 67 00		Control sistemas cerrados		•	•	
	aa 22 30 00	Importe y viajeros	Propietario del titulo		•	•	
	aa 22 31 00		Identificación del título		•	•	
	aa 22 3D 00		Cantidad		•	•	
	aa 22 6A 00		Número de viajeros que viajan juntos		•	•	

			utilizando el mismo titulo				
	aa 22 6B 00		Anulaciones de viajeros		•	•	
	aa 24 70 00	Zonas y saltos	Zona		•	•	•
	aa 24 71 00		Subzona		•	•	•
	aa 24 72 00		Saltos zona		•	•	•
	aa 24 73 00		Saltos subzona		•	•	•
	aa 28 75 00	Zonas origen / destino	Zona origen		•	•	•
	aa 28 76 00		Zona destino		•	•	•
	aa 29 77 00	Cont. Urbano / interurbanos	Numero de etapas urbanas efectuadas		•	•	•
	aa 29 78 00		Número de etapas interurbanas efectuadas		•	•	•
	aa 2A 77 00	Minutos urbano / interurbano	Minutos límite para poder efectuar transbordo urbano		•	•	•
	aa 2A 78 00		Minutos límite para poder efectuar transbordo interurbano		•	•	•

Históricos **aa** **03** Histórico de movimientos **06** = Historico de reservas **nn** Los campos de movimientos se encuentran organizados en registros el valor numérico de **nn** representa el valor del registro en el que está ubicado el campo.	aa 20 60 nn	Movimiento sin reserva	Numero de línea			•	
	aa 20 61 nn		Flota			•	
	aa 20 4A nn		Año			•	
	aa 20 4B nn		Mes			•	
	aa 20 4C nn		Día			•	
	aa 20 62 nn		Hora			•	
	aa 20 63 nn		Minuto			•	
	aa 20 64 nn		Sentido			•	
	aa 20 65 nn		Consorcio			•	
	aa 20 66 nn		Etapa			•	
	aa 20 67 nn		Control sistemas cerrados			•	
	aa 21 60 nn	Movimiento con reserva	Numero de línea			•	
	aa 21 61 nn		Flota			•	
	aa 21 4A nn		Año			•	
	aa 21 4B nn		Mes			•	
	aa 21 4C nn		Día			•	
	aa 21 62 nn		Hora			•	
	aa 21 63 nn		Minuto			•	
	aa 21 64 nn		Sentido			•	
	aa 21 65 nn		Consorcio			•	
	aa 21 66 nn		Etapa			•	
	aa 21 67 nn		Control sistemas cerrados			•	
	aa 22 30 nn	Importe y viajeros	Propietario del titulo			•	
	aa 22 31 nn		Identificación del título			•	
	aa 22 3D nn		Cantidad			•	
	aa 22 6A nn		Número de viajeros que viajan juntos utilizando el mismo titulo			•	
	aa 22 6B nn		Anulaciones de viajeros			•	
	aa 24 70 nn	Zonas y saltos	Zona			•	•
	aa 24 71 nn		Subzona			•	•
	aa 24 72 nn		Saltos zona			•	•
	aa 24 73 nn		Saltos subzona			•	•
	aa 28 75 nn	Zonas origen / destino	Zona origen			•	•
	aa 28 76 nn		Zona destino			•	•
	aa 29 77 nn	Cont. Urbano / interurbanos	Numero de etapas urbanas efectuadas			•	•
	aa 29 78 nn		Número de etapas interurbanas efectuadas			•	•
	aa 2A 77 nn	Minutos urbano / interurbano	Minutos límite para poder efectuar transbordo urbano			•	•
	aa 2A 78 nn		Minutos límite para poder efectuar transbordo interurbano			•	•

Log de Cargas **nn** Los campos de log de cargas se encuentran organizados en registros el valor numérico de **nn** representa el valor del registro en el que está ubicado el campo.	04 40 90 nn	Movimiento PA	ID comercio que realiza el movimiento			•	
	04 40 91 nn		Red de integración del que escribe el movimiento			•	
	04 40 4A nn		Año			•	
	04 40 4B nn		Mes			•	
	04 40 4C nn		Día			•	
	04 40 62 nn		Hora			•	
	04 40 63 nn		Minuto			•	
	04 40 92 nn		Segundo			•	
	04 10 30 nn	Identificación del titulo	Propietario del titulo			•	•
	04 10 31 nn		Número del titulo			•	•
	04 10 32 nn		Clase del titulo			•	•
	04 10 34 nn		Características 1 de tarifa			•	•
	04 10 35 nn		Características 2 de tarifa			•	•
	04 10 36 nn		Operatividad			•	•
	04 10 37 nn		Passback			•	•
	04 10 38 nn		Tipo de sistema de tarifas			•	•
	04 15 30 nn	Restricciones de uso	Propietario del titulo			•	•
	04 15 31 nn		Número del titulo			•	•
	04 15 42 nn		Uso			•	•
	04 16 30 nn	Fechas de validez	Propietario del titulo			•	•
	04 16 31 nn		Número del titulo			•	•
	04 16 4A nn		Año			•	•
	04 16 4B nn		Mes			•	•
	04 16 4C nn		Día			•	•
	04 16 4D nn		Año finalización			•	•
	04 16 4E nn		Mes finalización			•	•
	04 16 4F nn		Día finalización.			•	•

	04 18 30 nn	Limitación horaria	Propietario del titulo			•	•
	04 18 31 nn		Número del titulo			•	•
	04 18 52 nn		Hora de inicio			•	•
	04 18 53 nn		Hora final			•	•
	04 18 55 nn		Lunes			•	•
	04 18 56 nn		Martes			•	•
	04 18 57 nn		Miércoles			•	•
	04 18 58 nn		Jueves			•	•
	04 18 59 nn		Viernes			•	•
	04 18 5A nn		Sábado			•	•
	04 18 5B nn		Domingo			•	•
	04 42 30 nn	Importe	Propietario del titulo			•	•
	04 42 31 nn		Número del titulo			•	•
	04 42 3D nn		Cantidad			•	•
	04 42 3E nn		Signo			•	•
	04 44 3D nn	Fianza	Cantidad			•	•
	04 44 3E nn		Signo			•	•
	04 45 30 nn	Regularización	Propietario del titulo			•	•
	04 45 31 nn		Número del titulo			•	•
	04 45 3D nn		Cantidad			•	•
	04 46 30 nn	Cambio operatividad	Propietario del titulo			•	•
	04 46 31 nn		Número del titulo			•	•
	04 46 36 nn		Operatividad			•	•
	04 47 30 nn	Nuevo trayecto habitual	Propietario del titulo			•	•
	04 47 31 nn		Número del titulo			•	•
	04 47 34 nn		ST-1			•	•
	04 47 35 nn		ST-2			•	•
	04 48 30 nn	Nuevos saltos habituales	Propietario del titulo			•	•
	04 48 31 nn		Número del titulo			•	•
	04 48 34 nn		ST-1			•	•
	04 48 35 nn		ST-2			•	•

- Información de campo de texto.

Byte	Campo	Descripción
0	**T**	**0x09**
1…2	**L**	**longitud = Depende de la longitud del valor**
4	09_CC	Código de campo *Tabla de códigos de campo detallada a continuación.
5…N	09_VALOR	Valor del campo Cada byte representara en formato ASCII un carácter. [2]

TABLA DE CODIGOS DE CAMPOS

La columna **C6_Tipo** indica que el campo será entregado en caso de solicitar dicho tipo de información. En el caso de solicitar información de la tarjeta.

La columna **Opcional** indica que dicho campo NO es esencial y por lo tanto no será devuelto por la función si no existe.

Ámbito	Código HEX	Descripción	C6_Tipo = 1	C6_Tipo = 2	C6_Tipo = 3	Opcional
Identificación de tarjeta	08 01 0D 00	Nombre del usuario	•	•	•	
	08 01 0E 00	Número del documento	•	•	•	

[2] Ver tabla ASCII de caracteres de texto

5.6. RESUMEN DE TIPOS EN "DATA_IN".

Función	TI	Detalles
*	**0xF1**	Cabecera.
Init()	**0xC0**	Registro de datos de situación actual (módulo de validación)
	0xC1	Parámetros de situación (módulo de ventas)
	0xC5	Registro de fecha y hora de operación.
	0xC6	Registro de parámetros auxiliares para el módulo de validación.
	0xC7	Registro de tarificación relacionado con saltos en la tarjeta.
	0xC8	Registro de tarificación origen/destino.
	0xC9	Registro de parámetros de transbordo.
	0xCA	Registro de tipo de información a solicitar en la consulta.
	0xCB	Registro de importe
	0xCC	Registro de pasajeros a anular
Process()	**0xB0**	Información general del TAG presente.
	0xB1	Resultado de una operación efectuada.
	0xB2	Información con las propiedades de la clave maestra.
	0xB3	Información de la versión de claves.
	0xB4	Lista de aplicaciones existentes.
	0xB5	Información de la versión de fabricación.
	0xB6	Lista de archivos existentes en la aplicación actualmente seleccionada.
	0xB7	Información de un archivo especifico.
	0xB8	Información de lectura de archivo estándar.
	0xB9	Información de lectura de archivo de valor.
	0xBA	Información de lectura de archivo de registro.

5.7. RESUMEN DE TIPOS EN "DATA_OUT"

Función	TI	Detalles
*	**0xF1**	Cabecera.
	0xF2	Tiempo de consumo de la función ejecutada
Version()	**0x01**	Versión del núcleo.
	0x02	Versión del módulo de venta.
	0x03	Versión del módulo de validación.

	0x04	Versión del módulo de inspección.
	0x05	Información al desarrollador.
Process()	**0x99**	Información de error de sistema.
	0x10	Autentificación.
	0x11	Propiedades de la clave maestra.
	0x12	Leer versión de una clave.
	0x13	Listar aplicaciones existentes en la tarjeta.
	0x14	Seleccionar una aplicación.
	0x15	Obtener información de fabricación.
	0x16	Listar archivos de la aplicación actualmente seleccionada.
	0x17	Obtener información de un archivo.
	0x18	Leer información de un archivo estándar de datos.
	0x19	Escribir información en un archivo estándar de datos.
	0x1A	Leer información de un archivo de valor.
	0x1B	Incremento de valor de un archivo de valor.
	0x1C	Decremento de valor de un archivo de valor.
	0x1D	Incremento del valor limitado por el crédito establecido.
	0x1E	Escribir información de un registro en un archivo de registros.
	0x1F	Leer información de un registro de un archivo de registros.
	0x20	Borrar completamente un archivo de registros.
	0x21	Confirmar transacción.
	0x22	Invalidar transacción.
	0x30	Operativa con el centro autorizador
LastError()	**0x06**	Información del último error de sistema.
GetInfo()	**0x07**	Detalles de la Información al viajero.

6. TABLA ASCII DE CARACTERES DE TEXTO.

Car	Dec	Hex	Car	Dec	Hex	Car	Dec	Hex	Car	Dec	Hex	Car	Dec	Hex
Espacio	32	0x20	Q	81	0x51	é	130	0x82	│	179	0xB3	Σ	228	0xE4
!	33	0x21	R	82	0x52	â	131	0x83	┤	180	0xB4	σ	229	0xE5
”	34	0x22	S	83	0x53	ä	132	0x84	╡	181	0xB5	µ	230	0xE6
#	35	0x23	T	84	0x54	à	133	0x85	╢	182	0xB6	τ	231	0xE7
$	36	0x24	U	85	0x55	å	134	0x86	╖	183	0xB7	Φ	232	0xE8
%	37	0x25	V	86	0x56	ç	135	0x87	╕	184	0xB8		233	0xE9
&	38	0x26	W	87	0x57	ê	136	0x88	╣	185	0xB9	Ω	234	0xEA
‘	39	0x27	X	88	0x58	ë	137	0x89	║	186	0xBA	δ	235	0xEB
(	40	0x28	Y	89	0x59	è	138	0x8A	╗	187	0xBB	∞	236	0xEC
)	41	0x29	Z	90	0x5A	ï	139	0x8B	╝	188	0xBC	ø	237	0xED
*	42	0x2A	[	91	0x5B	î	140	0x8C	╜	189	0xBD	ε	238	0xEE
+	43	0x2B	\	92	0x5C	ì	141	0x8D	╛	190	0xBE	∩	239	0xEF
,	44	0x2C	]	93	0x5D	Ä	142	0x8E	┐	191	0xBF	■	240	0xF0
-	45	0x2D	^	94	0x5E	Å	143	0x8F	└	192	0xC0	±	241	0xF1
.	46	0x2E	_	95	0x5F	É	144	0x90	┴	193	0xC1	≥	242	0xF2
/	47	0x2F	`	96	0x60	æ	145	0x91	┬	194	0xC2	≤	243	0xF3
0	48	0x30	a	97	0x61	Æ	146	0x92	├	195	0xC3	⌠	244	0xF4
1	49	0x31	b	98	0x62	ô	147	0x93	─	196	0xC4	⌡	245	0xF5
2	50	0x32	c	99	0x63	ö	148	0x94	┼	197	0xC5	÷	246	0xF6
3	51	0x33	d	100	0x64	ò	149	0x95	╞	198	0xC6	≈	247	0xF7
4	52	0x34	e	101	0x65	û	150	0x96	╟	199	0xC7	°	248	0xF8
5	53	0x35	f	102	0x66	ù	151	0x97	╚	200	0xC8	¨	249	0xF9
6	54	0x36	g	103	0x67	ÿ	152	0x98	╔	201	0xC9	·	250	0xFA
7	55	0x37	h	104	0x68	Ö	153	0x99	╩	202	0xCA	√	251	0xFB
8	56	0x38	i	105	0x69	Ü	154	0x9A	╦	203	0xCB		252	0xFC
9	57	0x39	j	106	0x6A	¢	155	0x9B	╠	204	0xCC	²	253	0xFD
:	58	0x3A	k	107	0x6B	£	156	0x9C	═	205	0xCD	·	254	0xFE
;	59	0x3B	l	108	0x6C	¥	157	0x9D	╬	206	0xCE		255	0xFF
<	60	0x3C	m	109	0x6D	₧	158	0x9E	╧	207	0xCF			
=	61	0x3D	n	110	0x6E	ƒ	159	0x9F	╨	208	0xD0			
>	62	0x3E	o	111	0x6F	á	160	0xA0	╤	209	0xD1			
?	63	0x3F	p	112	0x70	í	161	0xA1	╥	210	0xD2			
@	64	0x40	q	113	0x71	ó	162	0xA2	╙	211	0xD3			
A	65	0x41	r	114	0x72	ú	163	0xA3	╘	212	0xD4			
B	66	0x42	s	115	0x73	ñ	164	0xA4	╒	213	0xD5			
C	67	0x43	t	116	0x74	Ñ	165	0xA5	╓	214	0xD6			
D	68	0x44	u	117	0x75	ª	166	0xA6	╫	215	0xD7			
E	69	0x45	v	118	0x76	º	167	0xA7	╪	216	0xD8			
F	70	0x46	w	119	0x77	¿	168	0xA8	┘	217	0xD9			
G	71	0x47	x	120	0x78	®	169	0xA9	┌	218	0xDA			
H	72	0x48	y	121	0x79	¬	170	0xAA	│	219	0xDB			
I	73	0x49	z	122	0x7A	½	171	0xAB	▄	220	0xDC			
J	74	0x4A	{	123	0x7B	¼	172	0xAC	▌	221	0xDD			
K	75	0x4B	|	124	0x7C	¡	173	0xAD	▐	222	0xDE			
L	76	0x4C	}	125	0x7D	«	174	0xAE	▀	223	0xDF			
M	77	0x4D	~	126	0x7E	»	175	0xAF	α	224	0xE0			
N	78	0x4E	*delete*	127	0x7F	░	176	0xB0	ß	225	0xE1			
O	79	0x4F	€	128	0x80	▒	177	0xB1	Γ	226	0xE2			
P	80	0x50	ü	129	0x81	▓	178	0xB2	π	227	0xE3			

7. TABLA DE CARACTERES DE TRATAMIENTO ESPECIAL.

Dec	Hex	Ctrl
0	0x00	NUL nulo
1	0x01	SO comienzo cabecera
2	0x02	STX comienzo texto
3	0x03	ETX final texto
4	0x04	EOT fin transmisión
5	0x05	ENQ pregunta
6	0x06	ACK respuesta
7	0x07	BEL sonido
8	0x08	BS retroceso
9	0x09	T tabulador horizontal
10	0x0A	LF avance línea
11	0x0B	VT tabulador vertical
12	0x0C	FF avance pagina
13	0x0D	CR retorno carro
14	0x0E	SO despl. inactivo
15	0x0F	SI despl. activo