Anexo I

Pago telemático. Cargo en cuenta

[1 OBJETIVO 3](#_Toc452119605)

[1 CARACTERÍSTICAS DEL SERVICIO 3](#_Toc452119606)

[1.1 Características funcionales 3](#_Toc452119607)

[1.2 Características técnicas 3](#_Toc452119608)

[2 FLUJO DEL PAGO 4](#_Toc452119609)

[2.1 Tratamiento de duplicados 6](#_Toc452119610)

[3 PETICIÓN APLICACIÓN 🡪 ENTIDAD BANCARIA. (TOKEN\_REQUEST) 7](#_Toc452119611)

[3.1 Tratamiento de los datos del sujeto pasivo 8](#_Toc452119612)

[4 RESPUESTA ENTIDAD BANCARIA 🡪 APLICACIÓN (TOKEN\_REPLY). 9](#_Toc452119613)

[5 ANEXO . ESQUEMA DE INTERCAMBIO DE INFORMACIÓN 10](#_Toc452119614)

[6 ANEXO. EJEMPLO TOKEN\_REQUEST 11](#_Toc452119615)

[7 ANEXO. EJEMPLO TOKEN\_REPLY 12](#_Toc452119616)

[8 ANEXO. ALGORITMO DE CIFRADO 12](#_Toc452119617)

[9 ANEXO. CALCULO DE MACODE 13](#_Toc452119618)

[10 ANEXO. CÓDIGO DE CONTROL TRIBUTARIO (CCT) 14](#_Toc452119619)

[10.1 Formato 14](#_Toc452119620)

[10.2 Descripción del MACODE 14](#_Toc452119621)

[10.3 Esquema del algoritmo de construcción 15](#_Toc452119622)

[11 CÓDIGOS DE ERROR 16](#_Toc452119623)

# OBJETIVO

En el presente documento se describe desde un punto de vista técnico los requerimientos del servicio de pago telemático que se debe establecer entre la entidad bancaria y la CARM para proporcionar los servicios de CARGO EN CUENTA.

Este sistema de pago está pensada principalmente para contribuyentes o colaboradores que dispongan de una cuenta corriente en la entidad bancaria, y deseen realizar un cargo en la misma referente a un impuesto de manera inmediata (online), sencilla, y sin necesidad de tener contratados los servicios de Banca Electrónica.

# CARACTERÍSTICAS DEL SERVICIO

## Características funcionales

1. El usuario **no requerirá tener el servicio de banca electrónica**, le bastará con ser titular de una cuenta en la entidad bancaria
2. El cargo en su cuenta y la comunicación del resultado deberá realizarse siempre de manera **ON-LINE**, esto es, el tiempo de respuesta ha de ser pequeño y el usuario quedará bloqueado hasta el procesamiento del cargo.
3. El servicio de pago ha de ser sencillo y para **evitar errores** se deberán proporcionar de manera automática todos los datos del usuario o del cargo conocidos de antemano tanto por la aplicación como por parte de la entidad bancaria. A estos efectos la aplicación y la entidad bancaria intercambiarán la información necesaria.
4. El servicio deberá proveer al usuario de un **justificante de pago** emitido directamente por la entidad bancaria.

## Características técnicas

1. Todas las comunicaciones APLICACION-USUARIO-ENTIDAD.BANCARIA se establecerán **cifradas** bajo protocolo HTTP seguro (HTTPS).
2. La información intercambiada APLICACION-ENTIDAD.BANCARIA incorporará mecanismos de **firma digital (MACODES o similar)** para asegurar la no variación de la misma, así como la autenticidad del emisor. Además, la información sobre la identidad del usuario y los datos del pago viajarán cifrados.
3. En las comunicaciones APLICACION-ENTIDAD.BANCARIA se establecerán **mecanismos extras** de seguridad como la validación de direcciones IP’s.

# FLUJO DEL PAGO

**6.a** Envío de CCT

CIUDADANO

(navegador)

**1.** Solicitud de pago

SERVIDOR ENTIDAD BANCARIA

APLICACIÓN

**3.** Envío de mensaje con **i**nformación  
 de cargo.

**2.** Enlace  
a entidad bancaria

**5.** Introducción de cuenta corriente

**4.** Pantalla de petición de Cuenta Corriente

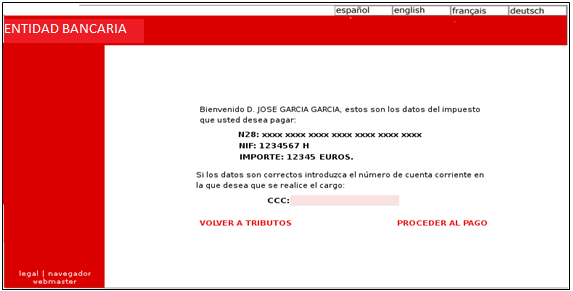
**6.b** Resultado del cargo

**9.** Vuelta a la aplicación para finalizar trámite

**8.** Impresión Justificante de Pago

Los pasos del proceso de pago son:

1. El ciudadano necesita realizar un pago de algún impuesto o similar gestionado por CARM.
2. En la aplicación que ha generado esa necesidad de pago se le ofrece al ciudadano la posibilidad de proceder al pago telemático, de forma individual, de cada uno de las deudas que tiene pendientes
3. Si el usuario decide proceder con el pago telemático en la modalidad CARGO EN CUENTA, al pulsar sobre la opción correspondiente a un cargo concreto, se abrirá una nueva ventana y se hará una petición a la URL de servicio especificada por la entidad bancaria, enviando de forma transparente al usuario los datos correspondientes al cargo (TOKEN\_REQUEST).
4. La entidad bancaria realiza la validación y descifrado de los datos recibidos.
5. Si la validación es correcta, la entidad bancaria presentará al ciudadano una pantalla, similar a la que aparece a continuación, donde se mostrarán los datos del cargo y una entrada para la introducción del número de cuenta corriente.



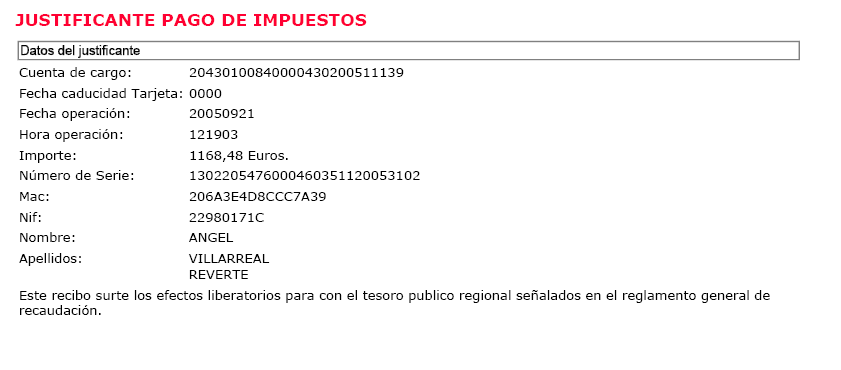
Si se produce algún problema en la validación de los datos en el servidor de la entidad bancaria, se mostrará una pantalla de error indicando las causas del mismo con un enlace en el que se ofrezca la opción de volver al portal de tributos.

1. Para proceder al pago deberá introducir su número de cuenta corriente y pulsar en el enlace '**PROCEDER AL PAGO**'.
2. En caso de que la operación de cargo se procese con éxito, el servidor de la entidad bancaria realizará una petición al servidor de la aplicación comunicando el resultado del cargo (TOKEN\_REPLY), y mostrará al usuario una pantalla con el resultado de la operación:



Si se produce algún error, se informará al usuario pero no al servidor de la aplicación.

1. Opcionalmente el usuario podrá imprimir el justificante de pago con el campo MAC generado por la entidad bancaria, que se utilizaría como justificante electrónico de la operación



Notas:

* El enlace de vuelta a la aplicación que la entidad bancaria proporcionará al usuario en todas las pantallas del servicio se extraerá de la etiqueta <URL\_VUELTA>
* La URL de la aplicación a la que el servidor de la entidad bancaria tendrá que enviar el resultado del cargo (paso **6.a**) se extraerá de la etiqueta <URL\_NOTIFICACION>
* Ambas direcciones vendrán especificadas en la petición inicial (TOKEN\_REQUEST)

## Tratamiento de duplicados

Es posible que al intentar realizar el pago identificado por un N28, ese N28 figure como pagado. Para este tipo de situaciones, el modo de actuar sería el siguiente:

* Con los datos que se envían para realizar el ingreso, se comprueba que no exista ya ese N28 pagado.
* Si ya existe, se comprueba si el NIF y el importe enviados en el detalle de ingreso coinciden con los del N28 que ya está pagado.
* Si los tres datos coinciden, no se trata de un duplicado sino de un intento de pago de algo ya pagado. La entidad bancaria avisará al ciudadano de esta eventualidad y se enviará a la aplicación la información con el resultado del cargo, devolviendo por tanto el CCT que ya se había generado**.**
* Si los datos no coinciden, se trata de un duplicado real. La entidad bancaria mostrará al ciudadano un mensaje de error y enviará a la aplicación el código de error correspondiente a duplicado pero no el CCT.

# PETICIÓN APLICACIÓN 🡪 ENTIDAD BANCARIA. (TOKEN\_REQUEST)

Para el envío de la información del cargo que se describe en el paso 3 del apartado flujo del pago se invocará a la URL de servicio que proporcionará la entidad bancaria mediante una petición HTTPS POST con un campo HIDDEN llamado TOKEN\_REQUEST en el que viajará la estructura XML cifrada mediante algoritmo de clave privada.

Este fichero XML deberá ajustarse al nodo <REQUEST> del esquema descrito en el fichero “CargoCuentaTelematica.xsd” que se adjunta con la documentación del servicio. (ver [ANEXO . ESQUEMA DE INTERCAMBIO DE INFORMACIÓN](#_ANEXO_._ESQUEMA)”),

Se describen a continuación los principales campos contenidos en la petición:

1. Identificador de comunicación único (etiqueta <ID\_COMUNICACION>), parámetro que deberá insertarse en la etiqueta del mismo nombre que viajará en el TOKEN\_REPLY de respuesta.
2. Identificador de aplicación (etiqueta <APLICACIÓN>).
3. Fecha de la operación (AAAAMMDD) (etiqueta <FECHA>).
4. Hora de la operación (HH:MM:SS) (etiqueta <HORA>).
5. Emisor del mensaje (etiqueta <EMISOR>).
6. Receptor del mensaje (etiqueta <RECEPTOR>).
7. La URL de vuelta al servicio de la aplicación que aparecerá en las pantallas de respuesta de la entidad bancaria (etiqueta <URL\_VUELTA>).
8. La URL de notificación (etiqueta <URL\_NOTIFICACION>) al servicio de la aplicación que se invocará por parte del servidor de la entidad bancaria (punto 6 del flujo de operaciones) con el parámetro TOKEN\_REPLY.
9. Tipo de servicio, valor 02 para ‘Servicio de Caja’, valor 03 para ‘Servicio de Entidad Colaboradora’ (etiqueta <TIPO\_SERVICIO>).
10. Código de la entidad en la que se realiza el ingreso <ENTIDAD>.
11. NIF del titular de la cuenta (etiqueta <TITULAR\_CUENTA>).
12. Sujeto Pasivo, obligatorio sólo para servicio de caja.
13. Código N28 del ingreso (etiqueta <ID\_UNICO>).
14. Importe del ingreso, en el formato de céntimos de euro (etiqueta <IMPORTE\_INGRESO>).
15. Código del hecho imponible (etiqueta <HECHO\_IMP>), obligatoria sólo para servicio de caja.
16. Oficina liquidadora .(etiqueta <OLDH>), obligatoria sólo para servicio de caja
17. Un MACODE obtenido a partir de la información de los campos:

* TITULAR\_CUENTA
* ID\_UNICO
* IMPORTE\_INGRESO
* SUJETO\_PASIVO
* OLDH
* HECHO\_IMP

Ver ANEXO. CALCULO DE MACODE

## Tratamiento de los datos del sujeto pasivo

Para el correcto tratamiento de la petición enviada, hay que tener en cuenta unas pequeñas consideraciones a la hora de tratar los datos del sujeto pasivo.

Debido a que desde las distintas aplicaciones se recibe la información desde diferentes sistemas en formatos distintos, no siempre se pueden enviar los datos de nombre y apellidos del sujeto pasivo por separado, tal y como se definen en el esquema de intercambio. Por este motivo, el modo de actuación será el siguiente:

* Si el identificador del sujeto pasivo (<NIF\_CIF>) es un **NIF**.
  + Se comprobará que la etiqueta <RAZON\_SOCIAL> está y tiene datos. Si es así, estos son los datos a mostrar en pantalla, independientemente de los datos enviados en las etiquetas <NOMBRE>, <APELLIDO\_1> y <APELLIDO\_2>.

Si no está o no tiene datos, lo que se mostrará en pantalla será el contenido de las etiquetas <NOMBRE>, <APELLIDO\_1> y <APELLIDO\_2>.

* Si el identificador del sujeto pasivo es un **CIF**.
  + La información a mostrar en pantalla será el contenido de la etiqueta <RAZON\_SOCIAL>.

# RESPUESTA ENTIDAD BANCARIA 🡪 APLICACIÓN (TOKEN\_REPLY).

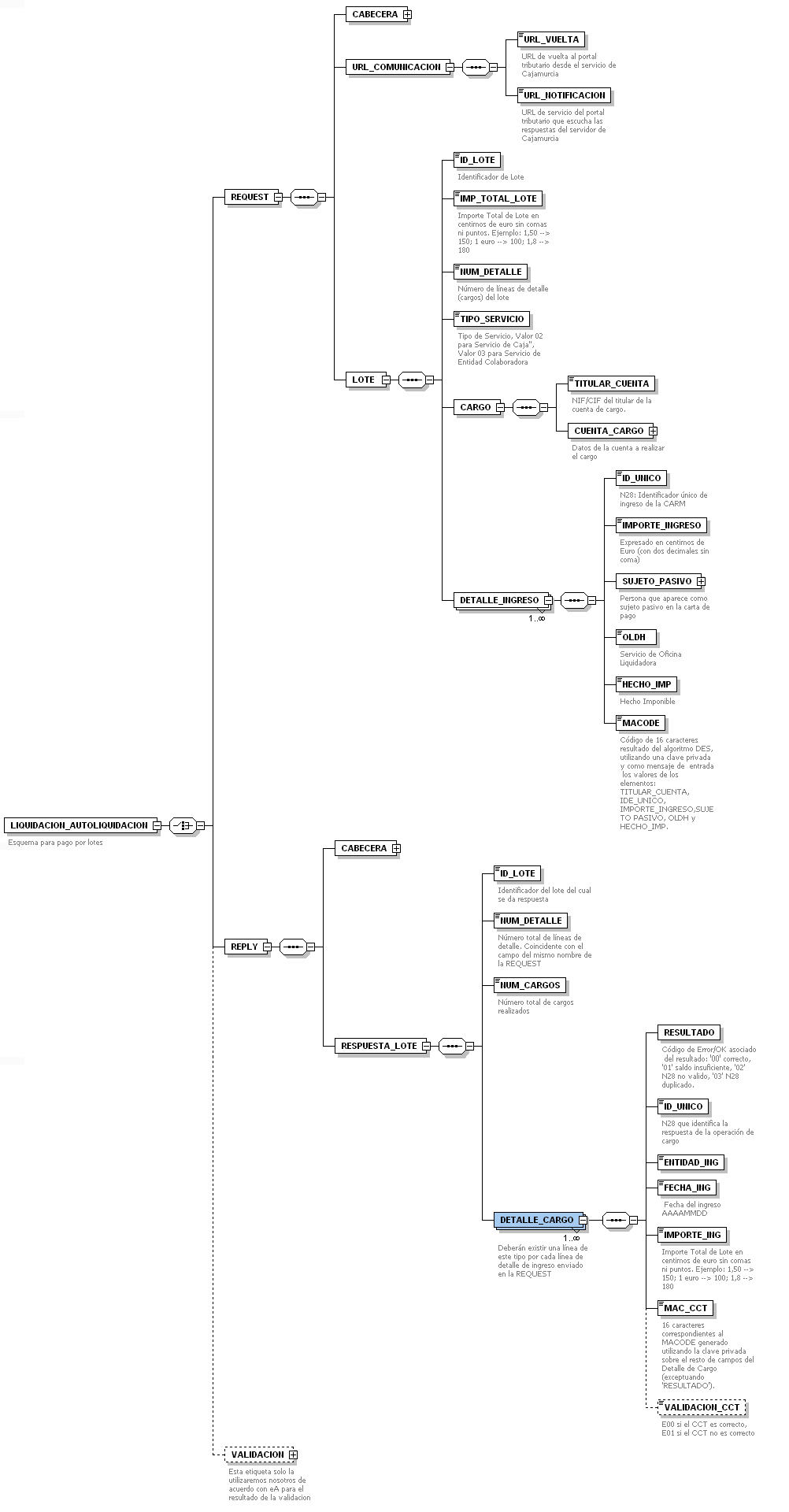
Para el envío de la información de pago que se describe en el **paso 6** del flujo de operaciones se invocará la URL de servicio que viajará en la etiqueta <URL\_NOTIFICACION> del TOKEN\_REQUEST mediante una petición HTTPS POST con un campo HIDDEN llamado TOKEN\_REPLY en el que viajará la estructura XML de respuesta de la entidad bancaria cifrada.

Este fichero XML deberá ajustarse al nodo <REPLY> del esquema descrito en el fichero “CargoCuentaTelematica.xsd” que se adjunta con la documentación del servicio. (ver [ANEXO . ESQUEMA DE INTERCAMBIO DE INFORMACIÓN](#_ANEXO_._ESQUEMA)”),

Se describen a continuación los principales campos contenidos en la respuesta:

1. Identificador de comunicación único (etiqueta <ID\_COMUNICACION>), parámetro que deberá ser de idéntico valor al recibido en la etiqueta del mismo nombre incrustada en el TOKEN\_REQUEST correspondiente a la petición en proceso.
2. Identificador de aplicación (etiqueta <APLICACIÓN>).
3. Fecha de la operación (AAAAMMDD) (etiqueta <FECHA> del elemento <CABECERA>).
4. Hora de la operación (HH:MM:SS) (etiqueta <HORA>).
5. Emisor del mensaje (etiqueta <EMISOR>).
6. Receptor del mensaje (etiqueta <RECEPTOR>).
7. Código N28 del ingreso (etiqueta <ID\_UNICO>).
8. Fecha de ingreso (etiqueta <FECHA> del elemento <DETALLE\_CARGO>).
9. Entidad de ingreso (etiqueta <ENTIDAD\_ING>).
10. Importe del ingreso en el formato que se determine (etiqueta <IMPORTE\_INGRESO>).
11. Un MACODE con la información de los 4 puntos anteriores (Etiqueta <MAC\_CCT>).

# ANEXO . ESQUEMA DE INTERCAMBIO DE INFORMACIÓN



|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Campo | | | | | Tipo | Tamaño | Descripción |
| REQUEST | | | | |  |  |  |
|  | CABECERA | | | |  |  | Datos de la cabecera |
|  |  | ID\_COMUNICACION | | | string |  | Identificador de la comunicación, el mismo en la REPLY y en la REQUEST |
|  |  | APLICACIÓN | | | string |  | Aplicación implicada en el tratamiento del mensaje |
|  |  | FECHA | | | string | 8 | Fecha de generación del mensaje AAAAMMDD |
|  |  | HORA | | | string | 8 | Hora de generación del mensaje HH:MM:SS |
|  |  | EMISOR | | | string |  | Servidor emisor del mensaje. |
|  |  | RECEPTOR | | | string |  | Servidor receptor del mensaje. |
|  | URL\_COMUNICACION | | | |  |  |  |
|  |  | URL\_VUELTA | | | string |  | URL de vuelta al portal tributario desde el servicio |
|  |  | URL\_NOTIFICACION | | | string |  | URL de servicio del portal tributario que escucha las respuestas del servidor |
|  | LOTE | | | |  |  |  |
|  |  | ID\_LOTE | | | string |  | Identificador de Lote |
|  |  | IM\_TOTAL\_LOTE | | | string | 13 | Importe Total de Lote en centimos de euro sin comas ni puntos. Ejemplo: 1,50 --> 150; 1 euro --> 100; 1,8 --> 180 |
|  |  | NUM\_DETALLE | | | string |  | Número de líneas de detalle (cargos) del lote |
|  |  | TIPO\_SERVICIO | | | string | 2 | Tipo de Servicio, Valor 02 para Servicio de Caja", Valor 03 para Servicio de Entidad Colaboradora |
|  |  | CARGO | | |  |  |  |
|  |  |  | TITULAR\_CUENTA | | string | 9 | NIF/CIF del titular de la cuenta de cargo. |
|  |  |  | CUENTA\_CARGO | |  |  |  |
|  |  |  |  | ENTIDAD | string | 4 | Código de la entidad |
|  |  |  |  | SUCURSAL | string |  | Código de la sucursal |
|  |  |  |  | D\_C | string | 2 | Dígitos de control |
|  |  |  |  | CUENTA | string | 10 | Número de cuenta |
|  |  | DETALLE\_INGRESO | | |  |  |  |
|  |  |  | ID\_UNICO | | string | 28 | N28: Identificador único de ingreso de la CARM |
|  |  |  | IMPORTE\_INGRESO | | string | 13 | Expresado en centimos de Euro (con dos decimales sin coma) |
|  |  |  | OLDH | | string |  | Servicio de Oficina Liquidadora |
|  |  |  | HECHO\_IMP | | string | 60 | Hecho imponible |
|  |  |  | MACODE | | string | 16 | Código de 16 caracteres resultado del algoritmo DES, utilizando una clave privada y como mensaje de entrada los valores de los elementos: TITULAR\_CUENTA, IDE\_UNICO, IMPORTE\_INGRESO, SUJETO PASIVO, OLDH y HECHO\_IMP. |
|  |  |  | SUJETO\_PASIVO | |  |  | Persona que aparece como sujeto pasivo en la carta de pago |
|  |  |  |  | NIF\_CIF | string | 9 | NIF/CIF del sujeto pasivo |
|  |  |  |  | NOMBRE | string | 20 | Nombre |
|  |  |  |  | APELLIDO\_1 | string | 20 | Primer apellido |
|  |  |  |  | APELLIDO\_2 | string | 20 | Segundo apellido |
|  |  |  |  | RAZON\_SOCIAL | string | 60 | Razón social, en caso de CIF |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Campo | | | | Tipo | Tamaño | Descripción |
| REPLY | | | |  |  |  |
|  | CABECERA | | |  |  | Datos de la cabecera |
|  |  | ID\_COMUNICACION | | string |  | Identificador de la comunicación, el mismo en la REPLY y en la REQUEST |
|  |  | APLICACIÓN | | string |  | Aplicación implicada en el tratamiento del mensaje |
|  |  | FECHA | | string | 8 | Fecha de generación del mensaje AAAAMMDD |
|  |  | HORA | | string | 8 | Hora de generación del mensaje HH:MM:SS |
|  |  | EMISOR | | string |  | Servidor emisor del mensaje. |
|  |  | RECEPTOR | | string |  | Servidor receptor del mensaje. |
|  | RESPUESTA\_LOTE | | |  |  |  |
|  |  | ID\_LOTE | | string |  | Identificador del lote del cual se da respuesta |
|  |  | NUM\_DETALLE | | numérico |  | Número total de líneas de detalle. Coincidente con el campo del mismo nombre de la REQUEST |
|  |  | NUM\_CARGOS | | numérico |  | Número total de cargos realizados |
|  |  | DETALLE\_CARGO | |  |  | Deberán existir una línea de este tipo por cada línea de detalle de ingreso enviado en la REQUEST |
|  |  |  | RESULTADO | string |  | Código de Error/OK asociado del resultado: '00' correcto, '01' saldo insuficiente, '02' N28 no valido, '03' N28 duplicado. |
|  |  |  | ID\_UNICO | string | 28 | N28 que identifica la respuesta de la operación de cargo |
|  |  |  | ENTIDAD\_ING | string | 4 | Código de la entidad del ingreso |
|  |  |  | FECHA\_ING | string | 8 | Fecha del ingreso AAAAMMDD |
|  |  |  | IMPORTE\_ING | string | 13 | Importe Total de Lote en centimos de euro sin comas ni puntos. Ejemplo: 1,50 --> 150; 1 euro --> 100; 1,8 --> 180 |
|  |  |  | MAC\_CCT | string |  | 16 caracteres correspondientes al MACODE generado utilizando la clave privada sobre el resto de campos del Detalle de Cargo (exceptuando 'RESULTADO'). |
|  |  |  | VALIDACION\_CCT | string |  | E00 si el CCT es correcto, E01 si el CCT no es correcto |
| VALIDACION | | | |  |  | Esta etiqueta solo la usamos nosotros de acuerdo con eA para el resultado de la validación. |
|  | CODIGO\_ERROR | | | string |  | E00: Ok, E01: No se ha podido validar el XML contra el esquema. |
|  | TEXTO\_ERROR | | | string |  | Texto del error |

# ANEXO. EJEMPLO TOKEN\_REQUEST

<?xml version="1.0" encoding="ISO-8859-1"?>

<LIQUIDACION\_AUTOLIQUIDACION xmlns="http://ea.carm.es/schemas/basicos/seguridad/pagoBanco/CargoCuentaTelematica.xsd">

<REQUEST>

<CABECERA>

<ID\_COMUNICACION>1234567890123456789012345678</ID\_COMUNICACION>

<APLICACIÓN>PORTAL-TRIBUTARIO</APLICACIÓN>

<FECHA>20051009</FECHA>

<HORA>23:54:01</HORA>

<EMISOR>CARM</EMISOR>

<RECEPTOR>CAJAMURCIA</RECEPTOR>

</CABECERA>

<URL\_COMUNICACION>

<URL\_VUELTA>

<https://etributos.carm.es/etributos/Modeloxxx>

</URL\_VUELTA>

<URL\_NOTIFICACION>

<https://etributos.carm.es/etributos/NotificacionModeloxxx>

</URL\_NOTIFICACION>

</URL\_COMUNICACION>

<LOTE>

<ID\_LOTE/>

<IMP\_TOTAL\_LOTE/>

<NUM\_DETALLE/>

<TIPO\_SERVICIO>02<TIPO\_SERVICIO>

<CARGO>

<TITULAR\_CUENTA>45678765K</TITULAR\_CUENTA>

<CUENTA\_CARGO></CUENTA\_CARGO>

</CARGO>

<DETALLE\_INGRESO>

<ID\_UNICO>2222022220222202222022220</ID\_UNICO>

<IMPORTE\_INGRESO>12324</IMPORTE\_INGRESO>

<SUJETO\_PASIVO>

<NIF\_CIF>123456789H</NIF>

<NOMBRE>JOSE</NOMBRE>

<APELLIDO\_1>GARCIA</APELLIDO\_1>

<APELLIDO\_2>GARCIA</APELLIDO\_2>

<RAZON\_SOCIAL/>

</SUJETO\_PASIVO>

<OLDH/>

<HECHO\_IMP>4569787</HECHO\_IMP>

<MACODE>126446ABCD298BDD</MACODE>

</DETALLE\_INGRESO>

</LOTE>

</REQUEST>

</LIQUIDACION\_AUTOLIQUIDACION>

# ANEXO. EJEMPLO TOKEN\_REPLY

<?xml version='1.0' encoding='ISO-8859-1'?>

<LIQUIDACION\_AUTOLIQUIDACION xmlns="http://ea.carm.es/schemas/basicos/seguridad/pagoBanco/CargoCuentaTelematica.xsd">

<REPLY>

<CABECERA>

<ID\_COMUNICACION>1234567890</ID\_COMUNICACION>

<APLICACIÓN>PORTAL-TRIBUTARIO</APLICACIÓN>

<FECHA>20051008</FECHA>

<HORA>23:15:03</HORA>

<EMISOR>CAJAMURCIA</EMISOR>

<RECEPTOR>CARM</RECEPTOR>

</CABECERA>

<RESPUESTA\_LOTE>

<ID\_LOTE/>

<NUM\_DETALLE/>

<NUM\_CARGOS/>

<DETALLE\_CARGO>

<ID\_UNICO>2222022220222202222022220</ID\_UNICO>

<ENTIDAD\_ING>2043</ENTIDAD\_ING>

<FECHA\_ING>20051008</FECHA\_ING>

<IMPORTE\_ING>1232422</IMPORTE\_ING>

<MAC\_CCT>1234567890123456</MAC\_CCT>

</DETALLE\_CARGO>

</RESPUESTA\_LOTE>

</REPLY>

</LIQUIDACION\_AUTOLIQUIDACION>

# ANEXO. ALGORITMO DE CIFRADO

La información que se envía tanto en el TOKEN\_REQUEST como en el TOKEN\_REPLY está cifrada mediante el algoritmo TripleDES en modo CBC.

Se establecerán los parámetros de cifrado del algoritmo entre la aplicación de la CARM y la entidad bancaria.

# ANEXO. CALCULO DE MACODE

El macode se calcula utilizando la clave privada asignada a la entidad bancaria, aplicando el algoritmo DES a una cadena formada por la concatenación de los siguientes campos, extraidos del XML de comunicación:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CAMPOS PARA CALCULO MACODE** | | | | | | |
| NUM | POS | LON | TIPO | DESCRIPCION | Campo Fichero XML | VALORES |
| 1 | 1 | 9 | An | NIF/CIF del Titular de la cuenta de cargo | <TITULAR\_CUENTA> |  |
| 2 | 10 | 28 | N | Número de Serie N28 | <ID\_UNICO> |  |
| 3 | 38 | 13 | N | Importe del ingreso en céntimos de euro | <IMPORTE\_INGRESO> |  |
| 4 | 51 | 9 | An | NIF/CIF del contribuyente | <SUJETO\_PASIVO>  <NIF\_CIF> |  |
| 5 | 60 | 50 | An | Nombre o razón social del contribuyente | <SUJETO\_PASIVO>  <NOMBRE> ó  <RAZON\_SOCIAL> |  |
| 6 | 110 | 20 | An | Apellido 1 | <SUJETO\_PASIVO>  <APELLIDO1> |  |
| 7 | 130 | 20 | An | Apellido 2 | <SUJETO\_PASIVO>  <APELLIDO2> |  |
| 8 | 150 | 3 | N | Oficina liquidadora | <OLDH> | ‘000’ |
| 9 | 153 | 6 | An | Hecho Imponible  ( También se conoce como Expresión Abreviada) | <HECHO\_IMP> |  |
| 10 | 159 | 16 | An | Código MAC resultante de los campos anteriores | <MACODE> |  |

# ANEXO. CÓDIGO DE CONTROL TRIBUTARIO (CCT)

El código de control tributario (CCT) es un campo de validación de la liquidación realizada por el cliente en oficinas de las entidades colaboradoras y constituye el justificante del pago de un impuesto gestionado por la CARM.

## Formato

El CCT se forma por concatenación de los siguientes campos:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Campo** | **Formato** | **Tamaño** | **Descripción** | |
|  |  |  |  |
| N28 | Numérico | 28 | Número de serie 28 dígitos | |
| Importe Ingresado | Numérico | 13 | Expresado en céntimos de euro. | |
| Fecha de Ingreso | Numérico | 8 | Formato: AAAAMMDD | |
| Código Entidad Bancaria | Numérico | 4 | Código de entidad | |
| MACODE | Alfanumérico | 16 | Numérico hexadecimal. | |

Ejemplo:

130220962600102000052009199500000009126232009063020431F54393D7E5F4527

**130220962600102000052009199500000009126232009063020431F54393D7E5F4527**

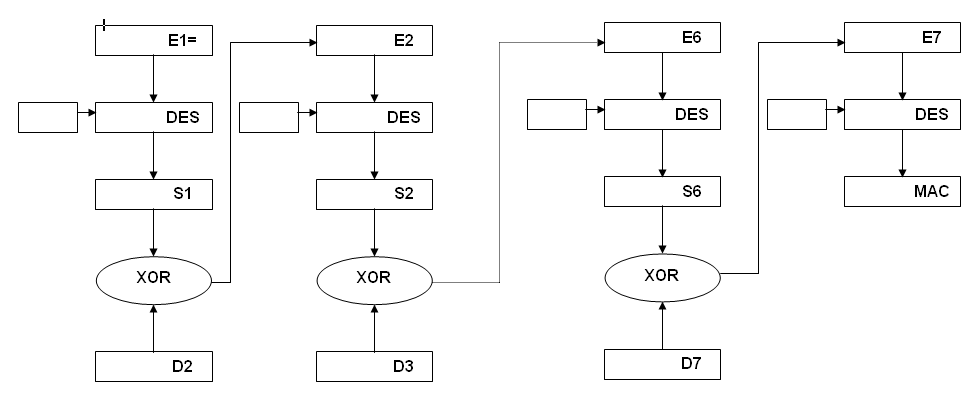
**N28** **Importe** **Fecha** **Entidad** **MACODE**

## Descripción del MACODE

El MACODE se forma a partir de los 53 primeros bytes del campo (compuestos por el N28, el importe, la fecha de ingreso y el código de la entidad bancaria) y de la clave privada de 8 bytes según las normas internacionales ISO8730/ISO8731 y estadounidense ANSI X9.9. Para generar el CCT es imprescindible que todos los datos que componen el campo estén en código EBCDIC y debidamente informados.

Los datos fuente compuestos por los cuatro primeros campos se agrupan en grupos de 64 bits (D1, D2,... D7), el último grupo (el 7º) no tendrá disponibles los 64 bits (solamente 40) por lo que se deberá ajustar a la izquierda y rellenar los 24 bits restantes con ceros binarios hasta completar los 64. Como se muestra en la figura explicativa, se inicializa el registro de entrada E1 con D1, este registro se pasa por el algoritmo DES utilizándose la correspondiente clave de macode CM y se obtiene como resultado los 64 bits del registro de salida S1. El grupo D2 junto con S1 son sometidos a una XOR (OR exclusiva) cargándose el resultado en el registro de entrada E2. Este proceso continúa con los siete grupos de 64 bits. El último registro de entrada obtenido se pasa por el algoritmo DES produciendo una salida de 64 bits (equivalente a 16 caracteres hexadecimales) que forman el MACODE a incorporar al CCT.

## Esquema del algoritmo de construcción



# CÓDIGOS DE ERROR

En los mensajes de respuesta se contemplan los siguientes códigos de error:

|  |  |
| --- | --- |
| Código | Descripción |
| 00 | Correcto |
| 01 | Saldo insuficiente |
| 02 | N28 no válido |
| 03 | N28 duplicado |
| 04 | CCC no existente |
| 05 | No existe relación NIF y CCC. El NIF no es titular la cuenta. |
| 88 | Error de verificación del MAC |
| 99 | Resto de errores |