AGENCIA TRIBUTARIA VALENCIANA

Proyecto:

GENERALITAT EN RED

PASARELA DE PAGOS POR INTERNET

COMUNICACIONES CON ENTIDADES COLABORADORAS

ABRIL de 2024

Índice

1 Objetivo del documento

El objetivo de este documento es explicar cómo es la comunicación con las entidades financieras. Esta comunicación se realizará mediante la invocación de operativas de un servidor web alojado en la entidad financiera.

Una Entidad Financiera podrá admitir cargos en cuenta, con tarjeta o ambos tipos de cargos.

Para poder realizar cargos en cuenta a través de una entidad financiera, los servicios (operativas) necesarios son los siguientes:

- Pago del importe de una autoliquidación, y obtención del NRC generado por la entidad financiera, en caso de ser satisfactorio el proceso.
- Consulta de un NRC, para poder reanudar el proceso en caso de caída en las comunicaciones durante la generación del mismo.

Para poder realizar cargos con tarjeta (sobre la cuenta asociada o sobre la propia tarjeta) a través de una entidad financiera serán necesarias las mismas operaciones.

- Pago con tarjeta del importe de una autoliquidación, y obtención del NRC generado por la entidad financiera, en caso de ser satisfactorio el proceso. El importe se podrá cargar a la cuenta asociada a la tarjeta o a la propia tarjeta
- Consulta de un NRC de un cargo con tarjeta anterior, para poder reanudar el proceso en caso de caída en las comunicaciones durante la generación del mismo.

No se contempla la anulación de un cargo en cuenta asociado a una autoliquidación telemática.

2 Mecanismo de comunicación con Entidades Financieras colaboradoras

La comunicación se realizará mediante la invocación de un servicio web específico para este cometido, siguiendo una filosofía análoga a la integración actual con el pago de tributos de la AEAT. La diferencia respecto al pago de tributos de la AEAT, donde se utiliza MAC para garantizar la integridad de la comunicación, es que se **cifrarán** los datos tanto de petición como de contestación para garantizar la confidencialidad e integridad de los mismos. Todo el mensaje(en caso de criptografía asimétrica) o todo el mensaje excepto la cabecera(en caso de criptografía simétrica) irá cifrado, dotando a la pasarela de mayor seguridad en las comunicaciones. El resto de las características de la comunicación serán:

- Que se intercambiarán mensajes siguiendo un formato de campos de longitud fija, que viajarán sobre protocolo HTTP o HTTPS. La pasarela soporta que los mensajes se envíen sobre HTTP, pero recomendamos utilizar el canal seguro HTTPS para tener un doble nivel de seguridad.
- Que ni los contribuyentes ni sus representantes tienen por qué ser clientes de banca electrónica.
- Que no existirá firma de las operaciones por parte del usuario de banca electrónica; únicamente comprobación de que su NIF tiene poderes sobre la cuenta de cargo. Ésta será la única comprobación de permisos que se realizará.
- Que se puede reutilizar buena parte de la infraestructura que las Entidades Colaboradoras ya tienen para la integración actual con la AEAT. De esta forma la integración de las entidades financieras al sistema se simplifica considerablemente, objetivo prioritario del proyecto.

3 Formato de los mensajes intercambiados

3.1 Formato para el cargo en cuenta y consulta de cargo en cuenta anterior

A continuación, se presenta la estructura de los mensajes de petición y de respuesta para la orden de cargo en cuenta, correspondientes a una autoliquidación en la entidad financiera.

Debe notarse que tanto la estructura de los mensajes en sí como los códigos y tipos de operación son únicamente una propuesta, abiertos a modificaciones.

Se han respetado en general las especificaciones de la AEAT para la orden de cargo, la consulta de NRC y la respuesta con el NRC (para ambos mensajes), añadiendo los campos que se estiman necesarios en su caso. La modificación más importante es el envío del número de justificante, el cual servirá para generar el NRC, y que se enviará durante la conciliación en los registros de detalle de documentos de la norma 65.

El resto de los mensajes sigue una especificación equivalente a la de dichos mensajes, pero adaptado a las necesidades de cada consulta.

Cada mensaje de petición tiene una cabecera de tres campos que forman una identificación única de la operación, compuesta de:

1. NIF/CIF originario de la transacción.
2. Fecha de la petición (AAMMDD).
3. Hora de la petición (HHMMSSSSSS), indicando hasta décimas de milisegundo.

A continuación, se presenta la estructura de los mensajes de petición y de respuesta para las órdenes de cargo en cuenta y de consulta, correspondientes a una autoliquidación en la entidad financiera.

Debe notarse que la estructura es idéntica a la utilizada por el applet de la AEAT.

El MAC que aparece en el campo 22 para asegurar la autenticidad de los 128 bytes anteriores no se rellenará, ya que se trata de un mecanismo de control realizado en el modelo original de la AEAT dado que las comunicaciones se realizan desde el PC del usuario. Este mecanismo de control se ha reemplazado por sistemas de seguridad más fuertes y que conciernen al mensaje completo y no sólo a los 128 primeros caracteres del mensaje. Debe notarse que la estructura de este mensaje es multi-impuesto y multioficina tributaria, por lo que algunos de los campos no se utilizarán en las tasas y tributos tramitados en la primera fase del proyecto, aunque deben aparecer en el mensaje para futuras incorporaciones de nuevos impuestos y Consellerias.

En la tabla siguiente se han señalado con negrita las ampliaciones/modificaciones respecto al modelo original de la AEAT.

Petición (orden de cargo y consulta):

Nº	POS.	LONG.	TIPO	DESCRIPCION
1	1	9	An	NIF del contribuyente (XNNNNNNNX) (1)
2	10	6	N	Fecha AAMMDD
3	16	10	N	Hora HHMMSSSSSS
4	26	3	An	Tipo de Operación (001 = Ingresos Autoliquidaciones)
5	29	2	An	Tipo de petición (01=Alta, 02=Consulta)
6	31	3	N	Modelo (MMM, Ej.: 600, 620, 650, ...)
7	34	2	N	Ejercicio fiscal (AA) (2)
8	36	2	An	Período (3)
9	38	1	An	Tipo de moneda de la declaración (valor fijo E)

10	39	1	An	Tipo de autoliquidación (I o D). Sólo ingresos (valor I).
11	40	9	An	N.I.F. del contribuyente (XNNNNNNNX)(1)
12	49	5	N	Código de Administración. C. Valenciana = 77008 (4)
13	54	6	An	Código territorial (5)
14	60	6	N	Fecha de devengo AAMMDD
15	66	12	N	Importe del ingreso / devolución (en euros x 100, ajustado a la derecha y relleno de ceros a la izquierda)
16	78	12	N	Importe total de la deuda (Renta con fraccionamiento)
17	90	1	N	Opción de fraccionamiento según normativa (siempre a 1)
18	91	20	N	Código Cuenta Cliente (6)
19	111	12	N	Importe en la moneda en que esté denominada la Cuenta Restringida del abono o solicitud de devolución.
20	123	9	An	NIF del Representante
21	132	9	An	NIF del Representante 2 o blancos
22	141	16	An	Blancos (7)
23	157	4	An	Anagrama fiscal del contribuyente (letras de etiqueta del contribuyente en personas físicas o blancos). No es obligatorio
24	161	40	An	Apellidos y Nombre o Razón Social del contribuyente
25	201	40	An	Apellidos y Nombre del Representante 1
26	241	40	An	Apellidos y Nombre del Representante 2 o blancos
27	**281**	**13**	**N**	**Número de Justificante generado por la Conselleria** (8)
28a	**294**	**1**	**N**	**Acreditación Pagos por Cuenta de terceros (0 no representante, 1 representante)** (9)
28b	295	15	An	Libre (blancos).
29	**310**	**10**	**An**	**Matrícula. Libre para otros modelos** (10)
30	**320**	**4**	**An**	**Concepto de la autoliquidación. Para distinguir los conceptos asociados al modelo (‘0001’ -TRP, ‘0002’ - AJD, ‘0003’ - OS)** (11)
31	324	82	An	Reservado para posibles ampliaciones (12)

Notas:

(1) Aunque en la autoliquidación existen varios sujetos pasivos, sólo se informará del primero de ellos, que es el contribuyente que realiza la autoliquidación.

(2) Actualmente se utilizan únicamente para el modelo 045 correspondiente a Juego y son obligatorios. El resto de los modelos tributarios **no contienen** el dato, por lo que el campo correspondiente de la petición tendrá valor ‘00’. En todos los casos el ejercicio es el año de devengo, que en el mensaje se reflejaría con las dos últimas cifras del mismo.

(3) Actualmente se utilizan únicamente para el modelo 045 correspondiente a Juego y son obligatorios. El resto de los modelos tributarios **no contienen** el dato, por lo que el campo correspondiente de la petición tendrá valor ‘00’. En ambos casos los períodos válidos son 1, 2, 3 y 4 (01, 02, 03 y 04 según el formato del mensaje de petición), que corresponden a trimestres (se pagan a post-trimestre). En el modelo 045 (Tasa fiscal sobre el juego. Máquinas o aparatos automáticos) los períodos válidos son los cuatro anteriores (01, 02, 03 y 04).

Para el ejercicio fiscal y el periodo, puede existir una excepción en los modelos 046 y 047 correspondientes a autoliquidaciones y liquidaciones de tasas respectivamente, ya que cada Conselleria definirá datos propios en estos modelos.

(4) Formado en las dos primeras posiciones por el Código de Comunidades Autónomas (B.O.E. 7-2-89), las dos posiciones siguientes son siempre el valor fijo "00" y la última posición es el dígito de control, siempre fijo para cada Comunidad Autónoma, y calculado según el módulo 11. Este sistema tiene que valer también para otras administraciones y organismos (Ayuntamientos,). El código de administración correspondiente a la Generalitat Valenciana es el 77008.

(5) Código Territorial del documento según aparece en la Norma 65 de la AEB. Servirá para que la Entidad Colaboradora identifique la cuenta restringida donde se realizará el abono. Tanto este campo como el siguiente no aparecen en la estructura utilizada en la AEAT y son necesarios para el pago de impuestos cedidos a las comunidades autónomas. Aparecen en este punto del mensaje y no al final del mismo por compatibilidad con otras CCAA (en la actualidad, Aragón, Castilla y León, Andalucía).

(6) Sobre la cuenta de cargo deberán tener poderes los representantes especificados (pueden ser uno o dos) del contribuyente o el propio contribuyente; siempre se especificará al menos un representante, que podrá coincidir o no con el contribuyente.

(7) El MAC no se utiliza. **Este campo se completará a blancos.**

(8) **Este *Número de Justificante* lo genera el backoffice de la Conselleria e identifica unívocamente la autoliquidación. Los 13 primeros caracteres del NRC serán este número de justificante.**

(9) Campo utilizado para indicar si el representante está acreditado para realizar el pago por cuenta de terceros. Los valores posibles en el momento presente son:

- 0: El Sujeto Pasivo coincide con el representante 1, y tiene poderes (titular o firma solidaria) sobre la cuenta contra la que se realiza el cargo. Es decir: sujeto pasivo = representante 1 = titular o firma solidaria sobre la cuenta donde se realiza el cargo.
- 1: El sujeto pasivo es diferente del Representante 1 y es el representante quien tiene poderes (titular o firma solidaria) sobre la cuenta en la que se realiza el cargo. Es decir: sujeto pasivo <> (representante 1 = titular o firma solidaria sobre la cuenta donde se realiza el cargo)

Si la pasarela admite otro tipo de cargos en el futuro se podrán añadir más valores posibles.

(10) *La Matrícula* se informará si se trata de una tasa fiscal sobre el juego referente a máquinas o aparatos automáticos (045) o se podrá informar si se trata de una liquidación de Transmisiones de Vehículos (620). Si no es así, este campo se podrá utilizar para información adicional de otros modelos o irá a blancos.

(11) El *Concepto* de la autoliquidación es obligatorio para todos los modelos, incluidos aquellos que tengan asociado un único concepto.

(12) Se podrá utilizar para información adicional de otros modelos en caso de que el campo 29 no sea suficiente para reflejar dicha información adicional o irá a blancos. Hay que tener en cuenta que las EECC pueden tener disponible, para incluir y devolver datos adicionales en el CSB65, una longitud inferior a la suma de las longitudes de los campos 29 y 31 del mensaje de petición.

Respuesta:

Nº	POS.	LONG.	TIPO	DESCRIPCION
1	1	3	An	Tipo de Operación (001 = Ingresos Autoliquidaciones)
2	4	2	An	Tipo de petición (01=Alta, 02=Consulta)
3	6	3	N	Modelo (MMM, Ej.: 600, 610, ...)
4	9	2	N	Ejercicio fiscal (AA)
5	11	2	An	Período (Ej.: 0A, 1T, 01, ...)
6	13	1	An	Tipo de moneda de la declaración (P o E)
7	14	1	An	Tipo de autoliquidación (I o D)
8	15	9	An	N.I.F. del contribuyente(XNNNNNNNX)
9	24	4	An	Letras de etiqueta en personas físicas
10	28	5	N	Código de Administración
11	33	12	N	Importe del ingreso / devolución (en euros x 100, ajustado a la derecha y relleno de ceros a la izquierda)
12	45	12	N	Importe total de la deuda (Renta con fraccionamiento)
13	57	1	N	Opción de fraccionamiento según normativa (Ej.:1,2 ó 3)
14	58	20	N	Código Cuenta Cliente
15	78	12	N	Importe en la moneda en que esté denominada la Cuenta Restringida del abono o solicitud de devolución. (No se pide al ciudadano. Es calculado)
16	90	8	N	Fecha de la operación (AAAAMMDD)
17	98	22	An	**Número de Referencia Completo (NRC)** (MMMVNNNNNNNNDCXXXXXXXX)
18	120	2	An	Código de retorno
19	122	89	An	Reservado para posibles ampliaciones
20	211	190	An	Libre. Actualmente la pasarela de pagos no trata este campo. Para el caso de código de error 86 no se tiene en cuenta la explicación opcional sobre horario de servicio.

Notas que deben tenerse en cuenta sobre los tratamientos y las respuestas:

- Rechazo del doble cargo: No se debe generar un cargo en cuenta duplicado; es decir, si la solicitud de cargo en cuenta corresponde a los mismos datos que en otra solicitud por esta o cualquier otra vía (comprobando, según el supuesto, la tupla “NIF, Modelo, Ejercicio, Período, e Importe” o bien “NIF, número de justificante e importe”) se debe responder con el error 70 (Petición duplicada). Para las tasas y tributos cedidos actualmente a las Comunidades Autónomas, como rechazo del doble cargo no vale la primera comprobación (NIF, Modelo, Ejercicio, ...); la entidad financiera deberá comprobar la terna propuesta en segundo lugar (NIF, nº de justificante e importe).

Códigos de error posibles:

A continuación, se enumeran los posibles códigos de error devueltos como resultado de la petición de cargo en cuenta, tal y como se establece por la AEAT. Puede que alguno de los códigos de error descritos carezca de sentido; además el sistema está abierto a añadir nuevos códigos de error:

Código	Descripción
00	Operación finalizada OK
10	Concepto o modelo erróneo
11	Falta concepto o modelo
12	Ejercicio fiscal erróneo
13	Falta ejercicio fiscal
14	Período erróneo
15	Falta período
16	Tipo de moneda erróneo (distinto de E)
17	NIF/CIF incorrecto para este modelo
18	Falta tipo de moneda
19	Importe ingreso erróneo
20	Falta importe de ingreso
21	NIF contribuyente erróneo
22	Falta NIF del contribuyente
23	NIF del primer representante erróneo
24	Falta NIF del representante
25	Sobra NIF del representante
26	Falta nombre del contribuyente
27	Falta nombre del representante
28	Sobra nombre del representante
29	Código administración erróneo
30	Falta código administración
31	Anagrama erróneo
32	Falta anagrama
33	Sobra anagrama
34	Importe total y parcial no cuadra
35	Falta importe total
36	Sobra importe total
37	Opción fraccionamiento errónea
38	Falta opción fraccionamiento
39	C.C.C. (Código Cuenta Cliente) erróneo
40	Falta C.C.C. (Código Cuenta Cliente)
41	Falta importe redenominación erróneo
42	Falta importe redenominación
43	Tipo de operación erróneo
44	Falta tipo de operación
45	Tipo de petición erróneo (distinto de 01 o 02)
46	Falta tipo de petición
47	Tipo de autoliquidación erróneo (distinto de I o D)
48	Falta tipo de autoliquidación

49	NIF del segundo representante erróneo
50	Concepto o modelo no permitidos
51	Ejercicio fiscal no permitido
52	Período no permitido
53	Ingreso no fraccionable por estar fuera del período voluntario
54	Ingreso fuera de período
55	Movimiento distinto de 01 y 02
56	NIF certificado distinto a NIF tecleado
57	NIF primer certificado distinto a NIF tecleado
58	NIF segundo certificado distinto a NIF tecleado
59	El horario de servicio es desde las 2:00 h. hasta las 23:00 h. diariamente

60	Fecha de presentación fuera de plazo
61	Importe total de la deuda erróneo
62	Autoridad certificadora errónea
63	Certificado caducado
64	Certificado revocado
65	Presentador no autorizado en nombre de terceras personas
66	Ha firmado dos veces con el mismo representante
67	Período impositivo concluido errónea
68	Fecha de conclusión período impositivo errónea
69	Error de formato en los datos de la petición
70	Petición duplicada
71	No existe cargo con los datos consultados
72	C.C.C. cancelado
73	C.C.C. bloqueado (judicialmente)
74	C.C.C. con saldo no disponible
75	C.C.C. con saldo insuficiente
76	C.C.C. cuenta no es de ahorro a la vista
77	C.C.C. inexistente
78	C.C.C. inoperante
79	NIF del contribuyente no titular a la cuenta
80	NIF representante no apoderado de la cuenta
81	Contribuyente no persona jurídica (e informa representante)
82	Falta segundo NIF por se cuenta conjunta
83	El segundo NIF no corresponde a titular de la cuenta
84	MAC erróneo
85	No hay suficientes apoderados
86	Esta entidad no atiende la solicitud de cargo por esta vía en este rango horario (y se le añade opcionalmente explicación de horario de servicio que puede venir en la cadena de respuesta desde la posición 211 hasta la 400)
87	Texto de la Entidad Colaboradora en la cadena de respuesta desde la posición 211 hasta la 400 con explicación amplia sobre la incidencia y teléfono de atención al cliente.
88	Contribuyente no identificado
89	Fecha de validez/caducidad de la tarjeta excedida, errónea o ausente
90	No está autorizado para realizar el pago por personas ajenas
91	Número de tarjeta no válido, erróneo o ausente
92	El titular del certificado con que se ha firmado no es titular de la tarjeta

93	Se ha excedido el límite de la operación
94	Tipo de tarjeta no soportado
95	Sólo se aceptan tarjetas emitidas por la propia entidad
99	Error técnico
95	Sólo se aceptan tarjetas emitidas por la propia entidad
99	Error técnico
A4	NRC no existe
A6	NIF no existe
A7	NRC ya constituido. Inténtelo por consulta
A8	NRC no preconstituido. Inténtelo por consulta
A9	NRC ya existe
B6	NRC no disponible para devolución
B8	NRC ya liberado
C1	Incoherencia de datos
C2	NRC de operación ya existe
F2	NRC no disponible para devolución, ya devuelto
H4	Imposible cobro, NRC ya cobrado
I3	Dígito de control erróneo.
I4	Carácter de control erróneo.
I6	Error en el modelo de operación.
I7	Error en el código del Banco de España.
C1	Incoherencia de datos

Vista la tabla de errores, y la descripción de los mensajes que se envía hay algunos errores que no se deben producir nunca, o que sólo deberían producirse en casos concretos, pero los mantenemos por homogeneizar la petición la tabla de errores con la de la AEAT. Resaltamos cosas que se deben tener en cuenta:

- Actualmente el Ejercicio Fiscal y el Periodo son obligatorios únicamente para el modelo 045 correspondiente a Juego. Los mensajes de error 12, 13, 14, 15, 51 y 52 solo se deberán producir con dicho modelo. En el resto de los modelos irá a blancos.
- El campo Anagrama Fiscal del contribuyente no es obligatorio en ningún modelo. Del sujeto pasivo se envía su NIF y su nombre. Por tanto, el error 32 no debe producirse en ningún caso.

3.2 Modificaciones en los mensajes intercambiados para el cargo con tarjeta y consulta de cargo con tarjeta anterior

El formato de los mensajes es el mismo, admitiendo otro significado y formato para los campos que transportan el CCC (código cuenta cliente) de la cuenta sobre la que se realizará el cargo.

En este campo, de 20 posiciones, podrá viajar:

- El CCC de la cuenta (20 posiciones numéricas completadas a cero por la izquierda).
- Un prefijo “T”, tipo de cargo (valor “CCC” para cargo en la cuenta asociada a la tarjeta o “TAR” para el cargo en la tarjeta) y el número de tarjeta (16 posiciones numéricas completadas a cero por la izquierda), y completado a espacios por la derecha hasta alcanzar el tamaño de 20 posiciones. Por ejemplo, para el número de tarjeta “0083 2136 8411 3016”, el valor que viajará será: “TCCC0083213684113016” para un cargo directo en cuenta o “TTAR0083213684113016” para un cargo sobre la propia tarjeta. En el caso de enviar un número de tarjeta con cargo en cuenta, la Entidad Financiera efectuará un cargo **directo** sobre la cuenta asociada a esa tarjeta. Sobre esa cuenta de cargo deberán tener poderes los representantes especificados (pueden ser uno o dos) del contribuyente; siempre se especificará al menos un representante, que podrá coincidir o no con el contribuyente.
- En caso de ser un cargo sobre la propia tarjeta, deberán tener poderes sobre ella el representante del contribuyente (representante 1); siempre se especificará al menos un representante, que podrá coincidir o no con el contribuyente.

En el campo 22 de 16 posiciones, se incluirá si procede en la petición la fecha de caducidad de la tarjeta (en formato MMAA) seguida de espacios en blanco hasta completar la longitud del campo. Si no procede el campo se seguirá rellenando de espacios en blanco en su totalidad.

A continuación, no se incluyen los contenidos completos de los mensajes de petición y de respuesta (tanto en el mensaje de Orden de Cargo como en el mensaje de Consulta), sino que únicamente se indican los cambios cuyo significado varía:

Petición (tanto en Orden de cargo como en Consulta):

Especificación original:

Nº	POS.	LONG.	TIPO	DESCRIPCION
18	91	20	N	Código Cuenta Cliente
22	141	16	An	Blancos

Nueva especificación:

Nº	POS.	LONG.	TIPO	DESCRIPCION

18	91	20	An	Código Cuenta Cliente o Número de Tarjeta asociada (formato TCCCXXXXXXXXXXXXXXXX para cargo directo en la cuenta asociada a la tarjeta ó TTAR XXXXXXXXXXXXXXXX para cargo sobre la propia tarjeta, siendo XXXXXXXXXXXXXXXX el número de tarjeta de 16 posiciones)
22	141	16	An	Blancos o Fecha de Caducidad Tarjeta formato MMAA (si procede) seguida de blancos a la derecha hasta completar la longitud 16

Respuesta:

No se modifica la especificación de la respuesta. En el campo 14 viajará el CCC de la cuenta donde se ha efectuado el cargo. En caso de ser cargo sobre una tarjeta viajará el mismo código que en mensaje de ida

Códigos de error posibles:

Los códigos de error posibles serán en principio los mismos que en las peticiones de cargo y consulta en cuenta.

4 Construcción mensajes utilizando cifrado simétrico Triple DES

En el caso de utilizar criptografía simétrica, todos los mensajes intercambiados tienen una cabecera común formada por tres campos, lo cuales se describen anteriormente:

- NIF/CIF (XNNNNNNNX)
- Fecha (AAMMDD)
- Hora (HHMMSSSSSS)

Estos tres primeros campos de cada mensaje (NIF, fecha y hora) viajarán sin más cifrado que el del propio canal SSL, mientras que el resto de los datos viajarán doblemente cifrados utilizando criptografía simétrica, con las siguientes características:

- Algoritmo: 3DES (DESede) • Modo de cifrado: CBC
- Padding: PKCS5PADDING
- Vector de inicialización para el cifrado: será único para cada entidad financiera y estará compartido entre la Pasarela de Pagos y la entidad a que corresponda.
- Clave de cifrado: constará de una parte fija y otra variable. La parte fija será única para cada entidad financiera y estará compartida entre la Pasarela de Pagos y la entidad a que corresponda. La parte variable dependerá de la información que viaja en los campos de cabecera. La clave tendrá 24 bytes el siguiente formato: *PPPPSSSS.AMMD.NNNXFFFFFF*, donde:
    - PPPP: El prefijo (parte fija de la clave) acordado entre la Oficina Tributaria y la Entidad Financiera.
    - SSSS: Cuatro caracteres centrales de los milisegundos del campo hora. ○ Punto separador.
    - AMMD: Cuatro caracteres centrales de la fecha.
    - Punto separador. ○ NNNX: Últimos cuatro caracteres del NIF/CIF.
    - FFFFFF: El sufijo (parte fija de la clave) acordado entre la Oficina Tributaria y la Entidad Financiera.
- La clave de cifrado, el vector de inicialización y los mensajes a cifrar estarán codificados según la norma ISO-8859-1.
- El contenido del mensaje cifrado (según las anteriores características) viajará codificado en una cadena que sea una representación en modo texto de los caracteres hexadecimales fruto del cifrado realizado (utilizando los caracteres ‘0’-‘9’ y ‘A’-‘F’).

La petición HTTP/HTTPS se realizará mediante un POST o un GET (parametrizable por entidad), con tres campos:

- Campo “ORIGEN”, con valor fijo “GVA”, utilizado por la entidad financiera para identificar el sistema origen de la petición.
- Campo “PETICION” (este nombre de campo es parametrizable), que contendrá el mensaje enviado según la codificación y cifrado descritos.
- Campo “NIVEL”, campo adicional identificativo del tipo de criptografía utilizado (o nivel de seguridad), con valor “10”.

La respuesta a esta petición será un contenido de tipo “text/plain” que contiene directamente la cadena de respuesta, cifrada y codificada según lo especificado en la propuesta original.

5 Construcción mensajes utilizando certificado digital

En caso de utilizar criptografía asimétrica, y a diferencia del caso anterior, todo el contenido del mensaje viajará firmado digitalmente por el origen y cifrado para el destinatario.

Para ello, tanto en origen como en destino se utilizarán certificados digitales emitidos por la Generalitat Valenciana, no estando contemplado la ampliación del sistema para su soporte "multi CA", es decir, el uso de certificados de otras Autoridades de Certificación por parte de alguna de las Entidades Colaboradoras.

El mensaje a firmar y cifrar estará codificado según la norma ISO-8859-1, y el contenido del mensaje una vez firmado y cifrado será un bloque PKCS #7 codificado en Base64.

Contrariamente a la criptografía simétrica aquí firmaremos y cifraremos todo el contenido del mensaje, no enviando ningún carácter sin cifrar. Una vez construido la cadena de pago o consulta para enviar a la Entidad Financiera se firmará y cifrará:

1. Se firma el mensaje con el certificado de la Pasarela de Pagos emitido por la Generalitat Valenciana. Se utiliza el algoritmo SHA-1. El resultado es un bloque PKCS #7 denominado CMS Signed Data, que contiene el certificado, la firma y el mensaje.
2. Se cifra el mensaje firmado, utilizando la información pública del certificado emitido por la GV para la Entidad Financiera a la que va dirigido el mensaje. Obtenemos un CMS Enveloped Data, conteniendo lo siguiente:
   - Mensaje cifrado utilizando Triple DES con una clave que ha generado con un algoritmo aleatorio, siendo el mensaje lo que hemos firmado: el PKCS #7 obtenido en el punto anterior.
   - La clave aleatoria generada cifrada con el algoritmo asimétrico SHA-1, para que únicamente la pueda descifrar la Entidad Financiera a la cual va dirigida.
3. Codificamos el bloque PKCS #7, el cual codificamos en Base64, y será lo que se envíe en el campo PETICION. Se incluirá un salto de línea cada 76 caracteres, como en el estándar RFC 1521 (*MIME (Multipurpose Internet Mail Extensions, Extensiones de correo de internet multipropósito)*

La petición HTTP/HTTPS se realizará mediante un POST (debido al mayor tamaño del mensaje firmado que supera el máximo permitido para GET), con tres campos:

- Campo "ORIGEN", con valor fijo "GVA", utilizado por la entidad financiera para identificar el sistema origen de la petición.
- Campo "PETICION" (este nombre de campo es parametrizable), que contendrá el mensaje enviado según la codificación y cifrado descritos.
- Campo "NIVEL", campo adicional identificativo del tipo de criptografía utilizado (o nivel de seguridad), con valor "20".

La respuesta a esta petición será un contenido de tipo “text/plain” que contiene directamente la cadena de respuesta, firmada, cifrada y codificada según lo indicado anteriormente. Utilizando los mismo mecanismos y algoritmos que la pasarela, la Entidad Financiera firmará con su certificado, cifrará con el certificado de la Pasarela de Pagos y codificará el resultado en Base64 de la misma forma que el mensaje de petición. Esa respuesta será la que envíe a la Pasarela.

6 Integración de Entidad Colaboradora en la Pasarela de Pagos GV

Para la integración de una Entidad Financiera colaboradora con la Pasarela de Pagos, se definirán en ambos extremos de la comunicación una serie de parámetros. Habrá valores que dependerán del tipo de criptografía elegido, mientras que habrá otros que se fijarán en ambos tipos de criptografía.

6.1 Parámetros comunes para ambas criptografías a proporcionar por las EECC

- **URL de Conexión:** Dirección del servicio que ofrece la Entidad Financiera, y que deberá proporcionar a la Pasarela de Pagos
- **Método de Conexión:** Método por el cual se conectará la oficina tributaria con la entidad bancaria. Los valores posibles son GET o POST, si bien en criptografía asimétrica deberá ser siempre POST
- **Atributo de petición:** Atributo de la petición en el que irá el mensaje de pago o consulta que la pasarela envía a la Entidad Financiera.
- **Cociente Carácter de Control:** Cociente para calcular el carácter de control del justificante, necesario para el cálculo del NRC
- **Tabla de conversión:** Tabla de conversión entre las letras y el resultado de dividir por el cociente, tras aplicar la operación pertinente sobre el número de justificante. Tendrá tantas letras como vale el cociente
- **Nivel de seguridad:** Tipo de criptografía que se utilizará para el intercambio de mensajes. Valores posibles: “10”(criptografía simétrica Triple DES), “20”(criptografía asimétrica utilizando certificados digitales)
- **Tipos de pago admitidos:** Para indicar qué tipos de pago permite la Entidad Financiera. Valores posibles: “CCC” si únicamente admite cargos contra un número de cuenta, “TARJETA” si únicamente admite pagos mediante tarjeta y “AMBOS” si admite ambos tipos de cargos.

6.2 Parámetros necesarios para criptografía simétrica

- **Prefijo Clave:** Prefijo de la clave de cifrado/descifrado de los mensajes intercambiados en caso de utilizar Triple DES. Será una cadena de 4 caracteres

- **Sufijo Clave:** Sufijo de la clave de cifrado/descifrado de los mensajes intercambiados en caso de utilizar Triple DES. Será una cadena de 6 caracteres
- **Vector de inicialización:** Vector de inicialización para el cifrado/descifrado de los mensajes intercambiados en caso de utilizar Triple DES. Será una cadena de 8 caracteres

6.3 Parámetros necesarios para criptografía asimétrica

- **Certificado:** La GV emitirá un certificado, que tendrá la entidad financiera, mientras que a la Pasarela se le proporcionará el fichero con la información pública de ese certificado. Así, en los mensajes intercambiados, la pasarela cifrará los mensajes que envíe a dicha entidad con la clave pública del certificado y la Entidad lo descifrará con su clave privada.