



## PASARELA DE PAGOS DE LA ADMINISTRACIÓN VASCA

CÓDIGO:	P.04
DENOMINACIÓN:	Proceso de generación del NRC
VERSIÓN:	01
RESPONSABLE:	Juan Luis Ronco

## PASARELA DE PAGOS DE LA ADMINISTRACIÓN VASCA

PROCESO: P.04 – Proceso de generación del NRC

Página: 2/13

### 1. CONTROL DEL PROCEDIMIENTO

#### 1.1. CONTROL DE MODIFICACIONES

Cualquier modificación en el contenido o estructura del presente procedimiento se recogerá debidamente en la tabla adjunta y supondrá una variación en el número de versión del mismo.

La responsabilidad de la introducción de una modificación se asumirán por el Responsable del proceso.

Versión	Fecha	Capítulo	Modificación	Observaciones
01	08/10/2006	-	-	Versión inicial
02	dd/mm/aaaa	-		

#### 1.2. DIFUSIÓN DEL PROCEDIMIENTO

La difusión del procedimiento se realizará a través de correo electrónico a los responsables de las Entidades Financieras.

## PASARELA DE PAGOS DE LA ADMINISTRACIÓN VASCA

PROCESO: P.04 – Proceso de generación del NRC

Página: 3/13

## 2. PROCEDIMIENTO PARA LA GENERACIÓN DEL NÚMERO DE REFERENCIA COMPLETO (NRC)

### 2.1. PROPÓSITO DEL PROCESO

Definir, establecer y mantener la sistemática y vías de comunicación y el flujo de información del proceso de generación del Número de Referencia Completo (NRC) para las Entidades Financieras adheridas a la Pasarela de Pagos de la Administración Vasca.

### 2.2. ÁMBITO DEL PROCESO

El proceso de generación del NRC para las Entidades Financieras adheridas a la Pasarela de Pagos de la Administración Vasca se circunscribe a los siguientes colectivos:

- Responsables de la OMA
- Profesionales del grupo OMA-EJIE
- Responsables de las Entidades Financieras

### 2.3. DEFINICIONES

- **Responsables de la OMA:** Profesionales de la OMA responsables de la Pasarela de Pagos.
- **Profesionales del grupo OMA-EJIE:** Profesionales de EJIE que prestan servicio y apoyo a la OMA.
- **Responsables de las Entidades Financieras:** Profesionales de las Entidades Financieras responsables de los desarrollos de la Pasarela de Pagos, así como los profesionales de las Entidades Financieras responsables de la recepción de las claves para la generación del NRC.

### 2.4. DESARROLLO DEL PROCESO

## PASARELA DE PAGOS DE LA ADMINISTRACIÓN VASCA

PROCESO: P.04 – Proceso de generación del NRC

Página: 4/13

El proceso de generación del NRC para las Entidades Financieras adheridas a la Pasarela de Pagos de la Administración Vasca se llevará a cabo mediante las siguientes actividades:

<b>Proceso P.02:</b> Incorporación de Entidades Emisoras	1.- Solicitud de incorporación 2.- Acuse de recibo 3.- Necesidades de información 4.- Seguimiento
--	--

### 2.5. MISIONES Y RESPONSABILIDADES

#### 1.- Solicitud de incorporación

El Responsable de la Entidad Emisora realizará una solicitud de incorporación de dicha Entidad Emisora a la Pasarela de Pagos a la siguiente dirección de correo electrónico, [mipago@ej-gv.es](mailto:mipago@ej-gv.es), indicando, al menos, los siguientes datos:

- **Datos necesarios para dar de alta a una Entidad Emisora en la Pasarela de Pagos:**

- Nombre del Responsable o Responsables de la Entidad Emisora
- Correo electrónico del Responsable o Responsables de la Entidad Emisora
- Teléfono del Responsable o Responsables de la Entidad Emisora
- CIF de la Entidad Emisora (p.e. S4833001C)
- Nombre de la Entidad Emisora (euskeria) (p.e. Eusko Jaurlaritza)
- Nombre de la Entidad Emisora (castellano) (p.e. Gobierno Vasco)  
(p.e., en el caso de ofrecer la información bilingüe: Eusko Jaurlaritza-Gobierno Vasco)
- Código de la Entidad Emisora en las Entidades Financieras (p.e. 04833001)
- Nombre del Municipio
- Código Postal
- Domicilio

## PASARELA DE PAGOS DE LA ADMINISTRACIÓN VASCA

PROCESO: P.04 – Proceso de generación del NRC

Página: 5/13

- Código y descripción de las Entidades Financieras Colaboradoras de la Entidad Emisora<sup>1</sup>.
- **Datos necesarios para dar de alta cada uno de los conceptos de pago de una Entidad Emisora en la Pasarela de Pagos:**
  - Código de la Entidad Emisora en las Entidades Financieras (p.e. 04833001)
  - Código de Sufijo o Tributo que identifica el concepto de pago (Cuaderno nº 57, Cuaderno nº 60).
  - Descripción del concepto de pago (euskeria) (p.e. Zaborrak)
  - Descripción del concepto de pago (castellano) (p.e. Basuras)  
(p.e., en el caso de ofrecer la información bilingüe: Zaborrak / Basuras)  
(evitar introducir abreviaturas)
  - Logo de la Entidad Emisora<sup>2</sup>
  - Tipo de formato de Cuaderno bancario
    - 507: Cuaderno nº 57
    - 502: Cuaderno nº 60, modalidad 1 (formato corto)
    - 508: Cuaderno nº 60, modalidad 1 (formato largo)
    - 521: Cuaderno nº 60, modalidad 2 (sin recargo)
    - 522: Cuaderno nº 60, modalidad 2 (con recargo)
  - Código y descripción de las Entidades Financieras Colaboradoras de la Entidad Emisora<sup>3</sup>.

<sup>1</sup> Ver Anexo 1: Relación de Códigos de Entidades Financieras

<sup>2</sup> Ver Anexo 2: Modelo de Justificante de Pago

<sup>3</sup> Ver Anexo 1: Relación de Códigos de Entidades Financieras

## PASARELA DE PAGOS DE LA ADMINISTRACIÓN VASCA

PROCESO: P.04 – Proceso de generación del NRC

Página: 6/13

- Tipo de validación

Se refiere al tipo de validación que se debe aplicar para validar los dígitos de control de la referencia para pagos de este sufijo. De momento tenemos los siguientes casos:

- 0: No se validan los dígitos de control.
- 1: Validación estándar, definida en la documentación de la Asociación Española de Banca sobre los cuadernillos 57 y 60.
- X: Validación no estándar, mediante procedimientos específicos a definir, para casos especiales.

### 2.- Acuse de recibo

El Responsable de la OMA contrastará, con el Responsable del grupo OMA-EJIE, la disponibilidad del conjunto de los Profesionales del grupo OMA-EJIE, y elaborará Acuse de recibo de la solicitud de incorporación a la Pasarela que incluirá, entre otros, los siguientes apartados:

- Profesional del grupo OMA-EJIE asignado al proceso de nueva incorporación.
- Correo electrónico de comunicación ([mipago@ej-gv.es](mailto:mipago@ej-gv.es))
- Código y nombre asignado a la instancia o aplicación.
- Previsión de la planificación de incorporación de la instancia o aplicación.
- Propuesta de calendario de seguimiento.
- Remisión de la documentación técnica de la Pasarela de Pagos, en su caso.

### 3.- Necesidad de información

Todas las necesidades de información de los Responsables de las Entidades Emisoras se dirigirán a la siguiente dirección de correo electrónico, [mipago@ej-gv.es](mailto:mipago@ej-gv.es), indicando en el correo, al menos, la siguiente información:

- Código de la Entidad Emisora.
- Descripción de la Entidad Emisora.
- Objeto de la consulta.

## PASARELA DE PAGOS DE LA ADMINISTRACIÓN VASCA

PROCESO: P.04 – Proceso de generación del NRC

Página: 7/13

Aquellas Entidades Emisoras que ya hayan practicado alguna solicitud de incorporación, procurarán obtener dicho conocimiento en sus respectivas organizaciones previamente a la demanda de información al Responsable de la OMA y/o a los Profesionales del grupo OMA-EJIE.

Esta operativa permitirá liberar al Responsable de la OMA y/o a los Profesionales del grupo OMA-EJIE de consultas ya respondidas, y centrar sus esfuerzos en aspectos de un mayor valor añadido.

### 4.- Seguimiento

El Responsable de la OMA se pondrá en contacto, con el Responsable o Responsables de la Entidad Emisora, de acuerdo con el calendario de seguimiento, al objeto de evaluar los avances del proceso de incorporación, y proponer las medidas oportunas para la consecución de los plazos previstos, en su caso.

## PASARELA DE PAGOS DE LA ADMINISTRACIÓN VASCA

PROCESO: P.04 – Proceso de generación del NRC

Página: 8/13

### Anexo 1: Número de Referencia Completo (NRC)

#### A. GENERACIÓN NRC

- El NRC se generará a partir de 64 caracteres obtenidos a partir de los siguientes datos:

Código Identificador	1 carácter x	Identificador del tipo de NRC en función de la operación
Tipo de liquidación	3 caracteres xxx	Según cuadernillo utilizado
Identificador de la entidad emisora de la liquidación	11 caracteres xxxxxxxxxxxx	Código que identifica a la administración emisora de la liquidación
Identificador Liquidación	14 caracteres xxxxxxxxxxxxxx	Código emitido por la Administración que permite identificar la liquidación
Importe consignado en la liquidación	12 caracteres xxxxxxxxxxxx	Importe ingresado en la entidad que ha de corresponder con el importe a pagar para el periodo indicado en la liquidación
Fecha de ingreso	8 caracteres xxxxxxxx	Fecha en la que la entidad de crédito ingresa el importe. Debe coincidir con los periodos de pago señalados en la liquidación Formato: ddMMyyyy
Código entidad de	4 caracteres	Código asignado por el

## PASARELA DE PAGOS DE LA ADMINISTRACIÓN VASCA

PROCESO: P.04 – Proceso de generación del NRC

Página: 9/13

crédito	xxxx	Banco de España a la entidad
Identificación justificante de pago	6 caracteres xxxxxx	De utilización opcional para las entidades de crédito. En caso de no ser utilizado, se enviarán cinco ceros (00000)
Identificación del justificante de pago para la Entidad Financiera	11 caracteres xxxxxxxxxxxx	De utilización opcional para las entidades financieras. Les permite identificar el justificante de pago en sus sistemas

2. A partir de los 64 caracteres se genera una firma utilizando la función MAC (Message Authentication Code) del algoritmo DES (Data Encryption Standard) según norma ANSI X9.9
3. El NRC final se compone de la identificación de la liquidación (25 caracteres) y la firma generada según lo dispuesto en el punto 2 (8 caracteres). Total: 33 caracteres

### **B. GENERACIÓN DE CLAVES DE CIFRADO POR EL DEPARTAMENTO COMPETENTE EN MATERIA DE TESORERIA Y DE LAS ENTIDADEADES COLABORADORAS**

1. La firma que forma parte del NRC se obtiene mediante un algoritmo basado en una función MAC (*Message Authentication Code*) del algoritmo DES, utilizando una clave simétrica (la clave de la Administración es la misma que la de la Entidad Financiera).
2. Esta clave de firma debe ser secreta y no conocida por ninguna entidad, ni por la Administración ni por las Entidades Financieras.  
Se divide la clave en dos partes que nunca se juntarán salvo en el interior de un sistema informático para construir y almacenar la clave completa:

## PASARELA DE PAGOS DE LA ADMINISTRACIÓN VASCA

PROCESO: P.04 – Proceso de generación del NRC

Página: 10/13

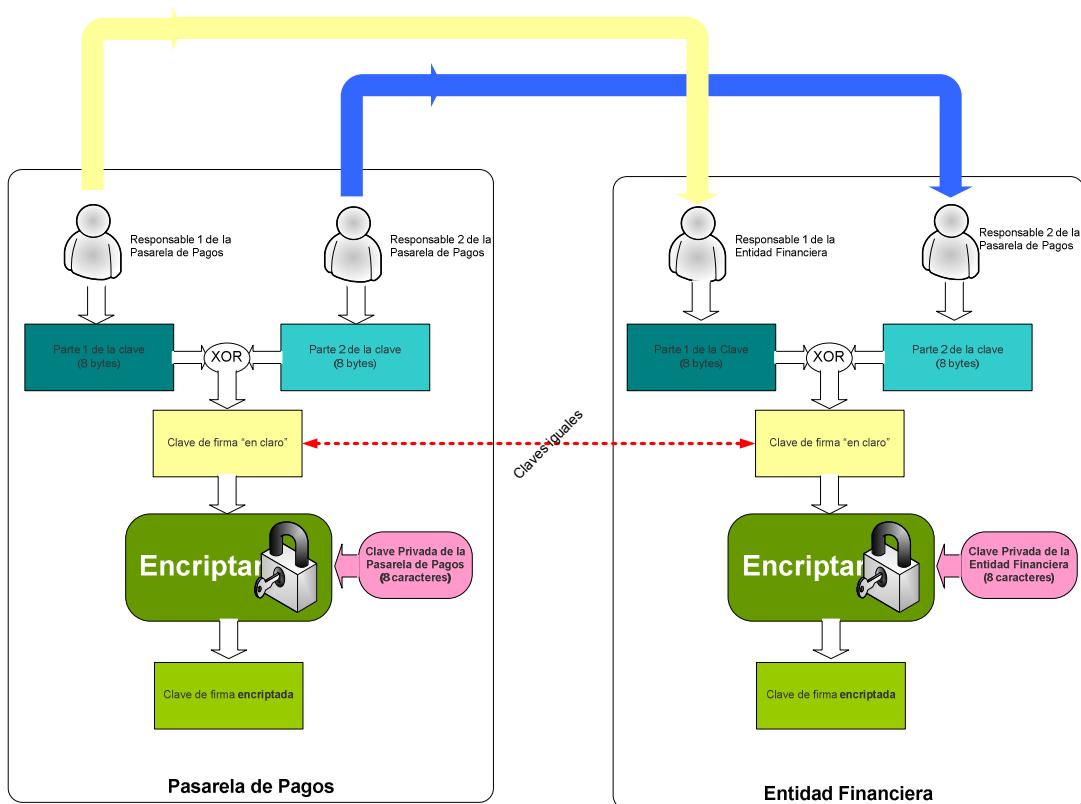
- o Dos responsables de la Pasarela de Pagos generarán dos partes de la clave de firma del NRC.
- o Cada uno de los dos responsables de la Pasarela de Pago introducirán su parte de la clave en un sistema informático donde se utilizará una función XOR para obtener la clave de firma final (en limpio) de generación del NRC.
- o La clave se guardará encriptada por otra clave privada que solo conocerán los responsables de la Pasarela de Pagos.
- o La Pasarela de Pagos enviará por separado su parte de la clave a su homólogo en la Entidad Financiera.
- o Cada Entidad Financiera, utilizando una función XOR, se volverá a construir la clave a partir de las dos partes recibidas y se custodiará en sus sistemas encriptada utilizando una clave privada de cada Entidad Financiera generada por la propia Entidad Financiera.

Grafico de generación, custodia y transferencia de la clave de firma de NRC

## PASARELA DE PAGOS DE LA ADMINISTRACIÓN VASCA

PROCESO: P.04 – Proceso de generación del NRC

Página: 11/13



## PASARELA DE PAGOS DE LA ADMINISTRACIÓN VASCA

PROCESO: P.04 – Proceso de generación del NRC

Página: 12/13

El NRC se calcula en base a los siguientes campos:

Entidad Emisora	Identificador de la <b>Entidad Emisora</b> de la liquidación  <b>11</b> caracteres (se rellena con ceros a la izquierda hasta la longitud del campo)	Código que <b>identifica a la Administración emisora</b> de la liquidación.  Normalmente el <b>emisor</b> incluido en alguno de los formatos de la carta de pago detallados el punto <i>5.6 Formato de la Carta de Pago en cada uno de los cuadernillos</i>
	Identificador de la liquidación  <b>14</b> caracteres (se rellena con ceros a la izquierda hasta la longitud del campo)	Código <b>emitido por la Administración</b> y que permite identificar la liquidación (carta de pago).  Este será la <b>referencia</b> (incluidos los dígitos de control) de la liquidación en alguno de los formatos de carta de pago detallados en el punto <i>5.6 Formato de la Carta de Pago en cada uno de los cuadernillos</i> .
	Importe consignado en la liquidación  <b>11</b> caracteres (se rellena con ceros a la izquierda hasta la longitud del campo)	Importe que se ha ingresado en la Entidad Financiera y que ha corresponder al importe a pagar para el periodo indicado en la liquidación al que pertenece la fecha de pago.  Importe en centeuros rellenando con ceros a la izquierda hasta la longitud del campo.

Entidad Financiera	Identificador de la <b>Entidad Financiera</b>  <b>4</b> caracteres	Código de 4 caracteres asignado por el Banco de España a la Entidad Financiera
	Identificador del Justificante de Pago para la Entidad Financiera  <b>10</b> caracteres (se rellena con ceros a la izquierda hasta la longitud del campo)	Identificador interno del pago para la Entidad Financiera y que permite identificarlo en sus sistemas.  En el caso de que la Entidad Financiera genere identificadores de menor longitud, el campo se rellena con ceros hasta la izquierda hasta la longitud del campo.

## PASARELA DE PAGOS DE LA ADMINISTRACIÓN VASCA

PROCESO: P.04 – Proceso de generación del NRC

Página: 13/13

A partir de estos **50 caracteres** se genera una firma utilizando la **función MAC** (*Message Authentication Code*) del algoritmo **DES** (*Data Encryption Standard*) según norma **ANSI X9.9**

ANSI X9.9 es un standard USA para la autenticación de las transacciones financieras que cubre dos aspectos:

- Formatea del mensaje
- Algoritmo de autenticación del mensaje.

El algoritmo definido por ANSI X9.9 es conocido por DES-MAC y está basado en DES (Data Encryption Standard) que es un algoritmo de firma simétrica en la cual la clave de cifrado es conocida por ambas partes: sirve tanto para encriptar como para desencriptar.

El NRC final se compone a partir de la identificación de la liquidación asignada por la Entidad Financiera (14 caracteres) y la firma (8 caracteres), en total 22 caracteres:

NRC (22) =	Identificación del justificante (14)		+	firma (8)
	Código de la Entidad Financiera	Identificador del Justificante para la Entidad Financiera	+	firma
22	4	10		8