Documento:	Pasarela de Pagos de las Administraciones Vascas
Denominación:	**Certificación de la Asociación Tercero-Número de Cuenta** Especificaciones Técnicas

Elaborado:	
Fdo.:	
Nombre:	Responsables Técnicos Pasarela Pagos
Fecha:	Diciembre 2014

Revisado y aprobado:
Fdo.:
Fecha:

Control de documentación

Título de documento:	Certificación de la Asociación Tercero-Número de Cuenta. Especificaciones Técnicas

Histórico de versiones

Código:

Versión:

Fecha: Septiembre 2010 – Versión Inicial

Diciembre 2014 – Versión Última

Cambios producidos desde la última versión

Primera versión.

Mayo 2011: Revisión de los códigos de retorno. Inclusión de la figura del "Autorizado"

Diciembre 2014: Inclusión de nuevos códigos de retorno ["Cuenta Modificada"] y posibilidad de envió de restricciones.

Control de difusión

Responsable:

Aprobado por:

Firma: Fecha:

Distribución:

Referencias de archivo

Autor:

Nombre archivo:

Localización:

Contenido

1 Introducción y Objeto del Documento

El presente documento es la Especificación Técnica de los servicios de la **Pasarela de Pagos de las Administraciones que facilita la certificación de la asociación de un tercero con un número de cuenta en una Entidad Financiera**.

El documento tiene dos destinatarios:

Destinatario	Objetivo	Puntos de interés
Las **Aplicaciones Departamentales** usuarias de la Pasarela de Pagos	Utilizar en una aplicación Departamental la funcionalidad de certificación de la asociación de un tercero con un número de cuenta	Bastaría con que el desarrollador responsable de la Aplicación Departamental se centre en los puntos: 3.2.4-Funciones expuestas por la Pasarela de Pagos para Aplicaciones Departamentales — Envío de solicitudes de certificación de asociación tercero-número de cuenta 3.2.5-Funciones expuestas por la Aplicación Departamental para la Pasarela de Pagos — Recepción de respuestas a la solicitud de certificación de la asociación tercero-número de cuenta
Las **Entidades Financieras** integradas con la Pasarela de Pagos	Incorporar la certificación de asociación tercero-número de cuenta en el adaptador de la banca electrónica con la Pasarela de Pagos	Bastaría con que el desarrollador responsable de la banca electrónica se centre en los puntos: 3.2.2-Funciones expuestas por la Entidad Financiera para la Validación de Cuentas. — Recepción de las solicitudes de certificación de asociación tercero-número de cuenta 3.2.3-Funciones expuestas por la Pasarela de Pagos para las Entidades Financieras — Recepción de respuestas a la solicitud de certificación de la asociación tercero-número de cuenta

IMPORTANTE

El presente documento en ningún caso debe considerarse como definitivo, el objetivo es básicamente crear un **documento de trabajo** en el que analizar la viabilidad, las ventajas, los inconvenientes, retos, etc. de las nuevas funcionalidades propuestas.
El documento en este sentido está "vivo" de forma que irá recogiendo las sugerencias, puntos a resolver, etc. que vayan apareciendo en las posteriores reuniones.

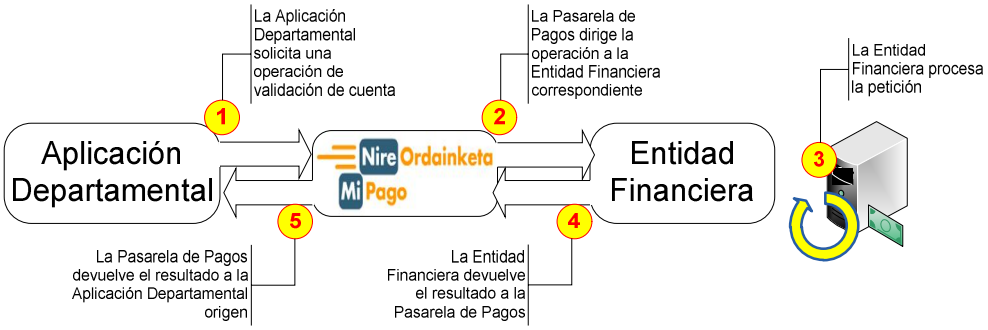
2 Funcionalidades

Descripción	Permite a una Administración solicitar a una Entidad Financiera una certificación de que un número de cuenta pertenece a un tercero (o está asociado como titular/co-titular o autorizado)
Escenarios de uso	• Validación previa del número de cuenta cuando la Administración tiene que realizar un pago a un tercero en un número de cuenta (ej: pago de una ayuda) • Validación previa de varios números de cuenta previo al envío de un lote de órdenes de pago. • Depuración de las bases de datos de terceros
Funcionalidades requeridas	La pregunta que se pretende responder es: ***¿Pertenece la cuenta X a el tercero con DNI Y?*** **NOTA**: El objetivo es validar que el número de cuenta proporcionado por el tercero es correcto de cara a que la Administración haga un ingreso en dicho número de cuenta, por lo tanto, basta con que el tercero sea titular, co-titula o autorizado en la cuenta. Se contemplan tres escenarios de uso:

Validación <u>individual</u> on-line	**Funcionalidad**	**Validar un número de cuenta**
	Escenario de uso	Validación individual por ejemplo de un alta de tercero
	Restricciones de uso	NO hay
Validación <u>múltiple</u> on-line La certificación múltiple on-line implica que **hay una garantía de tiempo máxima de 1 o 2 horas hasta que se recibe la respuesta** de la Entidad Financiera.	**Funcionalidad**	**Validar un lote de números de cuenta**, imponiendo un número máximo de validaciones en el lote (ej: no superior a 1.000)
	Escenario de uso	Remesas de órdenes de pago diarias de una Administración
	Restricciones de uso	NO hay

3 Implementación

La implementación propuesta funcionará **<u>siempre</u>** en **modo asíncrono**, es decir:



IMPORTANTE: Funcionamiento asíncrono

Tanto la aplicación departamental como la Pasarela de Pagos no se quedan a la espera de recibir la respuesta de la Entidad Financiera sino que envían el mensaje con la operación a la Entidad Financiera que lo procesará y cuando termine invocará a una función en la Pasarela de Pagos para informarle del resultado; la Pasarela de Pagos en ese momento pasará el resultado a la Aplicación Departamental.

3.1 Detalles de Funcionamiento

Detalles de Funcionamiento

- La validación **NO tendrá en cuenta la relación del tercero con la cuenta** (propietario, co-propietario o autorizado), simplemente devolverá si se puede realizar un pago en la cuenta para el tercero.
- **La Aplicación Departamental NO tiene que preocuparse de qué Entidad Financiera es la propietaria de una determinada cuenta corriente**, la Pasarela de Pagos recibirá la petición de validación de cuenta y la dirigirá a la Entidad Financiera correspondiente.
- En el caso de **lotes de validación** de números de cuenta, la Pasarela de Pagos en primer lugar "troceará" el lote enviado por la Aplicación Departamental en varios paquetes –uno por cada Entidad Financiera- y enviará a cada una aquellas cuentas de su propiedad.

  Cuando todas las Entidades Financieras devuelvan el resultado de la validación, la Pasarela de Pagos se encargará de volver a "juntar" los paquetes de respuesta de cada Entidad Financiera en uno solo que devolverá a la Aplicación Departamental.
- **La Administración será la responsable de mantener los consentimientos/autorizaciones** para consultar el número de cuenta; en el caso del Gobierno Vasco, estas autorizaciones normalmente se tienen en la forma del Formulario de Alta de Terceros o solicitud donde se recoge la firma del ciudadano/a otorgando este **consentimiento de consulta** a la Administración.

  Los consentimientos / autorizaciones **no se envían a la Entidad Financiera** en el XML de intercambio, simplemente, la Administración **se compromete a custodiar y facilitar estos consentimientos a la Entidad Financiera** cuando esta los solicite.

Tratamiento de los números de cuenta en la Pasarela de Pagos

Un objetivo básico de la Pasarela de Pagos es que **en los servidores de la Pasarela de Pagos no existan números de cuenta o tarjeta.**

En este caso este objetivo **no puede ser mantenido** ya que los números de cuenta han de "pasar" por la Pasarela de Pagos, sin embargo, **los números de cuenta deberán "circular" encriptados por una clave simétrica que idealmente únicamente han de conocer la Administración originaria de la operación y la Entidad Financiera,** nunca la Pasarela de Pagos.

> **Lo anterior implica que cada una de las Administraciones usuarias de esta funcionalidad en la Pasarela de Pagos debería intercambiar una clave de cifrado simétrico con cada una de las Entidades Financieras** con el objeto de encriptar la información de número de cuenta.
>
> Este requisito sin embargo, obligaría a intercambiar claves simétricas entre cada Administración usuaria de la Pasarela de Pagos y cada Entidad Financiera.
>
> Suponiendo que hay 100 Administraciones en la Pasarela y 10 Entidades Financieras habría que intercambiar 100x10=1.000 claves, algo que no es plausble.

Dada la imposibilidad de intercambiar claves para cada Administración-Entidad Financiera, se "relaja" el requerimiento de seguridad y **los números de cuenta o tarjeta serán encriptados utilizando las claves simétricas ya existentes (ya intercambiadas) entre la Pasarela de Pagos y cada una de las Entidades Financieras**.

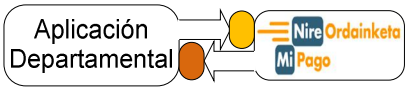
> Esta forma de funcionamiento implica que en teoría, desde la Pasarela de Pagos y conociendo las claves simétricas de cada Entidad Financiera, es posible desencriptar los números de cuenta.
>
> Desde la Pasarela de Pagos se asume este riesgo ya que se considera mínimo al estar las claves de cifrado simétrico con cada Entidad Financiera debidamente custodiadas en un contenedor seguro.

Para facilitar el uso y la gestión de estas claves, las librerías de la Pasarela de Pagos (p12) incluirán las funcionalidades necesarias para encriptación / desencriptación y generado de claves.

3.2 Resumen de los Interfaces

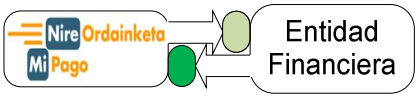
A continuación se describen las interfaces que exponen:

Interfaz entre las Aplicaciones Departamentales y la Pasarela de Pagos



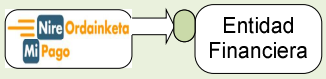
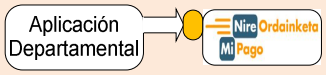
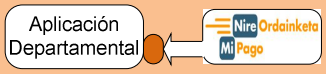
- La Pasarela de Pagos para que las Aplicaciones Departamentales **envíen** los mensajes de solicitud de certificación de asociación tercero-número de cuenta a realizar en las Entidades Financieras
- Las Aplicaciones Departamentales para que la Pasarela de pagos **devuelva** las respuestas a los mensajes de solicitud de certificación

Interfaz entre la Pasarela de Pagos y las Entidades Financieras



- La Entidad Financiera para que la Pasarela de Pagos le **envíe** los mensajes de solicitud de certificación de asociación tercero-número de cuenta
- La Pasarela de Pagos para que la Entidad Financiera **devuelva** las respuestas a los mensajes de solicitud de certificación

Por lo tanto hay cuatro interfaces a implementar:

Interfaz	Quién lo tiene que implementar	Ideograma	Funciones
Funciones expuestas por la Entidad Financiera para la Validación de Cuentas	Entidad Financiera		• Certificar asociación tercero-número de cuenta • Certificar un lote de terceros-números de cuenta
Funciones expuestas por la Pasarela de Pagos para las Entidades Financieras (en la URL de callback)	Pasarela de Pagos		• Recibir la certificación de la asociación de un tercero con un número de cuenta • Recibir Lote de certificaciones de asociación tercero-números de cuenta certificados
Funciones expuestas por la Pasarela de Pagos para Aplicaciones Departamentales	Pasarela de Pagos		• Certificar la asociación tercero-número de cuenta • Certificar un lote de asociaciones tercero-números de cuenta
Funciones expuestas por la Aplicación Departamental para la Pasarela de Pagos (en la URL de callback)	Aplicaciones Departamentales		• Recibir la certificación de la asociación de un tercero con un número de cuenta • Recibir Lote de certificaciones de asociación tercero-número de cuenta

Como se puede observar hay tres partes implicadas a las cuales “interesan” las presentes Especificaciones Técnicas:

Entidades Financieras	Ofrecen los servicios
Pasarela de Pagos	Hace de “intermediario” entre las aplicaciones departamentales “usuarias” de los servicios y las Entidades Financieras
Aplicaciones Departamentales	Usuarias de los servicios

De cara a la implementación de los servicios, cada entidad (Entidad Financiera / Pasarela de Pagos / Aplicación Departamental) deberá atenerse a las especificaciones del interfaz que le atañe de los anteriores.

3.2.1 Nomenclatura de los Servicios

La Pasarela de Pagos desde su concepción inicial (año 2000) utiliza una filosofía de exposición de servicios técnicamente cercana a la filosofía REST (*Respresentational State Transfer*) en el sentido que se definió un interfaz simple por el que se intercambian mensajes XML.
El desarrollo de las funcionalidades de certificación de la asociación de terceros-número de cuenta se propone que siga el mismo sistema que las funciones desarrolladas hasta el momento en la Pasarela de Pagos

Este interfaz de exposición de servicios de la Pasarela de Pagos se basa en estandarizar una nomenclatura común para el acceso a los servicios cuyas URLs seguirán la siguiente **nomenclatura:**

`http(s)://sitio:puerto/[URL del servicio]`	URL de acceso al servicio de Pasarela.

Ejemplos:

https://site/xWar/yServlet
https://site/pasarela/x.asp
https://site/x.cgi
https://site/x.php

Estos servicios web recibirán pasarán una serie de **parámetros normalizados** que identifican la **función** requerida en la forma:

```
http://[urlServicio]?module=X&function=Y&[resto de parametros]
```

En todos los casos:

- **Los parámetros se enviarán en formato XML**
- **El resultado de la llamada a la función se devolverá en formato XML.**

En la siguiente tabla se detallan cada uno de estos parámetros:

module — Módulo de la pasarela

Descripción	→	Permite dividir la pasarela de la Administración o Entidades Financieras en módulos (si se considera necesario) para agrupar funciones lógicas.
Valor	→	Un nombre identificador del módulo de la pasarela donde se encuentran las funciones.
Ejemplo	→	*module="certGateway"*

function — Función/procedimiento específico dentro del módulo correspondiente

Descripción	→	Identifica una funcionalidad invocable remotamente
Valor	→	Nombre identificador de la función
Ejemplo	→	*function="holderCert"*

Otros parámetros — Los nombres de los parámetros enviados al servicio accesible vía web pueden ser:

Parámetro	Descripción
`holderCertData`	XML con la solicitud de certificación
`holderCertDataList`	Lista de XMLs de solicitud de certificación
`holderCertCertifiedData`	XML con datos de respuesta de una solicitud de certificación
`holderCertCertifiedDataList`	Lista de XMLs con datos de respuesta de una solicitud de certificación
`protocolData`	Datos de protocolo de una invocación de servicio
`operationResult`	Resultado de la operación (de la invocación del servicio)

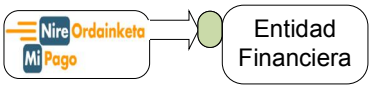
Importante:

Adicionalmente y en base a las necesidades específicas de cada pasarela (Administración o Entidad Financiera), podrán existir aquellos parámetros que cada uno considere necesarios.

A continuación se resumen las funciones y los parámetros de cada uno de estos interfaces:

3.2.2 Funciones expuestas por la Entidad Financiera para la Validación de Cuentas.

3.2.2.1 Resumen



Funciones expuestas por la Entidad Financiera para la Validación de Cuentas

Función	Descripción	Parámetros de Entrada	Parámetros de Vuelta (se envían a la URL callback indicada por la Pasarela de Pagos)
Certificar on-line la asociación de un tercero con un *único* número de cuenta	Certifica si un número de cuenta individual está asociada con un tercero dado	• DNI del tercero • Número de cuenta (encriptado) • Timestamp • URL callback de la Pasarela de Pagos	• DNI del tercero • Número de cuenta (encriptado) • Resultado (OK/NOK/Error) • NRC • Timestamp
Certificar on-line un lote de asociaciones tercero-número de cuenta La certificación múltiple on-line implica **que hay una garantía de tiempo máxima de 1 o 2 horas hasta que se recibe la respuesta** de la Entidad Financiera.	Certifica de forma on-line un lote de múltiples asociaciones tercero-número de cuenta La pasarela de Pagos se encargará de "trocear" el lote con los paquetes de certificación para cada Entidad Financiera así que **únicamente llegarán peticiones de certificación de números de cuenta de la Entidad Financiera**	• Una lista de registros con: ▪ DNI del tercero ▪ Número de cuenta (encriptado) • Timestamp • URL callback de la Pasarela de Pagos	• Una lista de registros con: ▪ DNI del tercero ▪ Número de cuenta (encriptado) ▪ Resultado (OK/NOK/Error) ▪ NRC • Timestamp

3.2.2.2 Función: Certificar on-line Asociación Tercero-Número de Cuenta

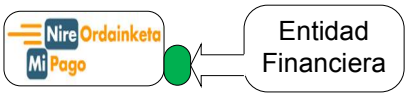
Características	Certifica **una única asociación tercero-número de cuenta** La certificación on-line implica que la respuesta a la solicitud de certificación es inmediata o prácticamente inmediata (unos minutos max)
Origen	**Pasarela de Pagos**
Destino	**Servicio** de la Pasarela de la Entidad Financiera
Método HTTP	GET (preferiblemente) / POST
Función	**module=***certGateway* **function=***holderCert* ***Parámetros***: **`holderCertData`**: Datos a certificar (asociación tercero-número de cuenta) o DNI del tercero o Número de cuenta encriptado con las claves simétricas intercambiadas entre la Pasarela de Pagos y la Entidad Financiera **`protocolData`** Datos de protocolo. El dato más relevante es la ***URL de callback*** **en la Pasarela de Pagos donde la Entidad Financiera "notificará" de forma asíncrona el resultado de la operación**
Respuesta	El resultado de la certificación de la asociación tercero-número de cuenta se devuelve de forma asíncrona a la URL de callback en la Pasarela de Pagos incluida en el parámetro *`protocolData`* Como respuesta a la invocación HTTP a la función *`holderCert`* se devuelve una estructura **`operationResult`** que indica si el mensaje con la solicitud de certificación de asociación tercero-número de cuenta ha sido recibido y va a ser procesado. **NOTA**: En el caso de la solicitud de certificación de una única asociación tercero-número de cuenta (esta función), la Entidad Financiera puede opcionalmente devolver de forma **síncrona** el resultado de la certificación en la estructura operationResult. En cualquier caso, también se devolverá el resultado de forma asíncrona a la URL de callback indicada en el parámetro de entrada *`protocolData`*

3.2.2.3 Función: Certificar on-line un lote de asociaciones tercero-número de cuenta

Características	Certifica un lote (múltiples) asociaciones tercero-número de cuenta. La certificación múltiple **on-line** implica que: • Únicamente se enviarán a la Entidad Financiera las solicitudes de certificación de **aquellos números de cuenta pertenecientes a la Entidad Financiera**. La Pasarela de Pagos se encargará de **"trocear" los lotes de solicitudes de certificación en múltiples lotes para enviar a cada Entidad Financiera** y de "juntar" de vuelta las respuestas de cada una de ellas para devolver el resultado a la Aplicación Departamental solicitante. • **Hay un límite** (por definir) **en el número de asociaciones tercero-número de cuenta** que se puede solicitar certificar • El límite en el número de asociaciones tercero-número de cuenta se impone para **garantizar que hay un tiempo máximo** (1/2 horas) en que la petición de certificación va a ser procesada.
Origen	**Pasarela de Pagos**
Destino	**Servicio** de la Pasarela de la Entidad Financiera
Método HTTP	POST
Función	**module=***certGateway* **function=***multiple*HolderCert ***Parámetros***: **holderCertDataList**: Lista de estructuras holderCertData cada una de las cuales contiene un registro de datos a certificar (asociación tercero-número de cuenta) ▪ DNI del tercero ▪ Número de cuenta encriptado con las claves simétricas intercambiadas entre la Pasarela de Pagos y la Entidad Financiera NOTA: Dado que el número de registros a certificar puede ser muy grande, este parámetro con la lista de registros a certificar se enviará comprimido en formato ZIP **protocolData** Datos de protocolo. El dato más relevante es la ***URL de callback* en la Pasarela de Pagos donde la Entidad Financiera "notificará" de forma asíncrona el resultado de la operación**
Respuesta	El resultado de la certificación de múltiples asociaciones tercero-número de cuenta se devuelve de forma asíncrona a la URL de callback en la Pasarela de Pagos incluida en el parámetro *protocolData* Como respuesta a la invocación HTTP a la función *holderCert* se devuelve una estructura **operationResult** que indica si el mensaje con la solicitud de certificación de múltiples asociaciones tercero-número de cuenta ha sido recibido y va a ser procesado.

3.2.3 Funciones expuestas por la Pasarela de Pagos para las Entidades Financieras

3.2.3.1 Resumen



Funciones expuestas por la Pasarela de Pagos para las Entidades Financieras (en la URL de callback)

Función	Descripción	Parámetros de Entrada	Parámetros de Vuelta (se envían de forma síncrona como respuesta a la llamada)
Asociación tercero-número de cuenta certificado	Recibe el resultado de la certificación de la asociación de un tercero con un número de cuenta	• DNI del tercero • Número de cuenta (encriptado) • Resultado (OK/NOK) • Timestamp	• Resultado (OK/NOK/Error) • Timestamp
Lote de asociaciones tercero-número de cuenta certificados	Recibe el resultado de la certificación de un lote de asociaciones tercero-número de cuenta	• Una lista de registros con: ▪ DNI del tercero ▪ Número de cuenta (encriptado) • Timestamp	• Resultado (OK/NOK/Error) • Timestamp

3.2.3.2 Función: Asociación Tercero - Número de Cuenta Certificado

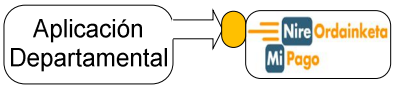
Características	Función de Callback en la Pasarela de Pagos que recibe desde la Entidad Financiera la certificación de **una única asociación tercero-número de cuenta**
Origen	**Servicio** de la Pasarela de la Entidad Financiera
Destino	**Pasarela de Pagos**
Método HTTP	GET (preferiblemente) / POST
Función	**module=***certGateway* **function=***holderCertified* ***Parámetros**:* **`holderCertCertifiedData`**: Datos enviados previamente desde la Pasarela de Pagos (asociación tercero-número de cuenta) certificados por la Entidad Financiera o DNI del tercero o Número de cuenta encriptado con las claves simétricas intercambiadas entre la Pasarela de Pagos y la Entidad Financiera o Resultado de la certificación: **OK** • El tercero está asociado al número de cuenta de alguna forma (titular, autorizado, co-titular, etc) En este caso, la Entidad Financiera incluirá un **NRC de la certificación**: Cada certificación de asociación tercero-número de cuenta incluirá un número de referencia completo como "firma" de la Entidad Financiera de la validez de los datos **NOK** • El tercero no tiene relación con el número de cuenta • El número de cuenta no existe **`protocolData`** Datos de protocolo.
Respuesta	El resultado de la certificación de la asociación tercero-número de cuenta se recibe desde la Entidad Financiera de forma asíncrona en la URL de callback indicada en la solicitud de certificación previa a la Entidad Financiera.

3.2.3.3 Función: Lote de asociaciones tercero-números de Cuenta Certificados

Características	Función de Callback en la Pasarela de Pagos que recibe desde la Entidad Financiera la certificación de **múltiples asociaciones tercero-número de cuenta** En el caso en que la aplicación Departamental solicitase la certificación de un lote de asociaciones tercero-número de cuenta, la Pasarela de Pagos se encargó previamente de "trocear" el lote en "paquetes" para cada una de las Entidades Financieras de forma que a cada una de ellas únicamente le llegan solicitudes de certificación relacionados con sus números de cuenta. En este caso, la Pasarela de Pagos se encargará de recibir las múltiples respuestas de las diferentes Entidades Financieras y componer un lote de respuesta único a la Aplicación Departamental. **IMPORTANTE:** • La URL de esta función de callback se envía en los datos de protocolo (*protocolData*) de las solicitudes a las Entidades Financieras • Se expondrá una única función de callback para recibir el resultado de la certificación de un lote de asociaciones tercer-número de cuenta.
Origen	**Servicio** de la Pasarela de la Entidad Financiera
Destino	**Pasarela de Pagos**
Método HTTP	POST
Función	**module=***certGateway* **function=***multipleHolderCertified* ***Parámetros***: **holderCertCertifiedDataList**: Lista de estructuras **holderCertCertifiedData** con los datos enviados previamente desde la Pasarela de Pagos (asociación tercero-número de cuenta) certificados por la Entidad Financiera o DNI del tercero o Número de cuenta encriptado con las claves simétricas intercambiadas entre la Pasarela de Pagos y la Entidad Financiera o Resultado de la certificación: **OK** • El tercero está asociado al número de cuenta de alguna forma (titular, autorizado, co-titular, etc) En este caso, la Entidad Financiera incluirá un **NRC de la certificación**: Cada certificación de asociación tercero-número de cuenta incluirá un número de referencia completo como "firma" de la Entidad Financiera de la validez de los datos **NOK** • El tercero no tiene relación con el número de cuenta • El número de cuenta no existe NOTA: Dado que el número de registros a certificar puede ser muy grande, este parámetro con la lista de registros a certificar se enviará comprimido en formato ZIP **protocolData** Datos de protocolo.
Respuesta	El resultado de la certificación múltiple de asociación tercero-número de cuenta se recibe desde la Entidad Financiera de forma asíncrona en la URL de callback indicada en la solicitud de certificación previa a la Entidad Finaciera

3.2.4 Funciones expuestas por la Pasarela de Pagos para Aplicaciones Departamentales

3.2.4.1 Resumen



Funciones expuestas por la Pasarela de Pagos para Aplicaciones Departamentales

Función	Descripción	Parámetros de Entrada	Parámetros de Vuelta (se envían a la URL callback indicada por la Aplicación Departamental)
Certificar una asociación tercero-número de cuenta	Certifica si un número de cuenta individual está asociada con un tercero dado	• DNI del tercero • Número de cuenta (encriptado) • Timestamp • URL callback de la aplicación departamental	• DNI del tercero • Número de cuenta (encriptado) • Resultado (OK/NOK/Error) • NRC • Timestamp
Certificar un lote de asociaciones tercero-número de cuenta	Certifica de forma on-line un lote de múltiples asociaciones tercero-número de cuenta La pasarela de Pagos se encargará de "trocear" el lote con los paquetes de validación para cada Entidad Financiera y de volver a componer el lote de respuesta "juntando" las respuestas de cada Entidad Financiera.	• Una lista de registros con: ▪ DNI del tercero ▪ Número de cuenta (encriptado) • Timestamp • URL callback de la aplicación departamental	• Una lista de registros con: ▪ DNI del tercero ▪ Número de cuenta (encriptado) ▪ Resultado (OK/NOK/Error) ▪ NRC • Timestamp

3.2.4.2 Función: Certificar Asociación Tercero-Número de Cuenta

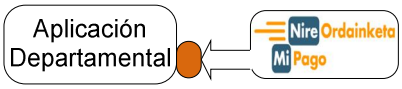
Características	Certifica **una única asociación tercero-número de cuenta** La certificación on-line implica que la respuesta a la solicitud de certificación es inmediata o prácticamente inmediata (unos minutos max)
Origen	**Aplicación Departamental**
Destino	**Pasarela de Pagos**
Método HTTP	GET (preferiblemente) / POST
Función	**module=***certGateway* **function=***holderCert* ***Parámetros**:* **`holderCertData`**: Datos a certificar (asociación tercero-número de cuenta) • DNI del tercero • Número de cuenta encriptado con las claves simétricas intercambiadas entre la Pasarela de Pagos y la Entidad Financiera **`protocolData`** Datos de protocolo. El dato más relevante es la ***URL de callback* en la Aplicación Departamental donde la Pasarela de Pagos "notificará" de forma asíncrona el resultado de la operación devuelto por la Entidad Financiera**
Respuesta	El resultado de la certificación de la asociación tercero-número de cuenta se devuelve de forma asíncrona a la URL de callback en la Aplicación Departamental incluida en el parámetro *protocolData* Como respuesta a la invocación HTTP a la función *holderCert* se devuelve una estructura **`operationResult`** que indica si el mensaje con la solicitud de certificación de asociación tercero-número de cuenta ha sido recibido y va a ser procesado (enviado a una Entidad Financiera)

3.2.4.3 Función: Certificar un lote de números de cuenta

Características	Certifica un lote (múltiples) asociaciones tercero-número de cuenta. La Pasarela de Pagos decidirá cuál de las formas es la más adecuada para tratar la petición en función del número de solicitudes de certificación En cualquier caso, la Pasarela de Pagos se encargará de "trocear" el lote en "paquetes" para cada una de las Entidades Financieras de forma que a cada una de ellas únicamente le llegan solicitudes de certificación relacionados con sus números de cuenta. Una vez recibidas las respuestas individuales de cada una de las Entidades Financieras, la Pasarela de Pagos compondrá un lote de respuesta único a la Aplicación Departamental de forma que para esta última la existencia de múltiples Entidades Financieras es transparente.
Origen	**Aplicación Departamental**
Destino	**Pasarela de Pagos**
Método HTTP	POST
Función	**module=***certGateway* **function=***multipleHolderCert* ***Parámetros***: **`holderCertDataList`**: Lista de estructuras holderCertData cada una de las cuales contiene un registro de datos a certificar (asociación tercero-número de cuenta) • DNI del tercero • Número de cuenta encriptado con las claves simétricas intercambiadas entre la Pasarela de Pagos y la Entidad Financiera NOTA: Dado que el número de registros a certificar puede ser muy grande, este parámetro con la lista de registros a certificar se enviará comprimido en formato ZIP **`protocolData`** Datos de protocolo. El dato más relevante es la ***URL de callback*** **en la Aplicación Departamental donde la Pasarela de Pagos "notificará" de forma asíncrona el resultado de la operación devuelto por la Entidad Financiera**
Respuesta	El resultado de la certificación de múltiples asociaciones tercero-número de cuenta se devuelve de forma asíncrona a la URL de callback en la Aplicación Departamental incluida en el parámetro *protocolData* Como respuesta a la invocación HTTP a la función *holderCert* se devuelve una estructura **`operationResult`** que indica si el mensaje con la solicitud de certificación de múltiples asociaciones tercero-número de cuenta ha sido recibido y va a ser procesado.

3.2.5 Funciones expuestas por la Aplicación Departamental para la Pasarela de Pagos

3.2.5.1 Resumen



Funciones expuestas por la Aplicación Departamental para la Pasarela de Pagos (en la URL de callback)

Función	Descripción	Parámetros de Entrada	Parámetros de Vuelta (se envían de forma síncrona como respuesta a la llamada)
Asociación tercero-número de cuenta certificado	Recibe el resultado de la certificación de la asociación de un tercero con un número de cuenta	• DNI del tercero • Número de cuenta (encriptado) • Resultado (OK/NOK) • Timestamp	• Resultado (OK/NOK/Error) • Timestamp
Lote de asociaciones tercero-número de cuenta certificados	Recibe el resultado de la certificación de un lote de asociaciones tercero-número de cuenta	• Una lista de registros con: ▪ DNI del tercero ▪ Número de cuenta (encriptado) • Timestamp	• Resultado (OK/NOK/Error) • Timestamp

3.2.5.2 Función: Asociación tercero-número de Cuenta Certificado

Características	Función de Callback en la Aplicación Departamental que recibe desde la Pasarela de Pagos (que a su vez lo ha recibido de la Entidad Financiera) la certificación de **una única asociación tercero-número de cuenta**
Origen	**Pasarela de Pagos**
Destino	**Aplicación Departamental**
Método HTTP	GET (preferiblemente) / POST
Función	**module=***certGateway* **function=***holderCertified* ***Parámetros**:* **`holderCertCertifiedData`**: Datos enviados (asociación tercero-número de cuenta) previamente desde la Aplicación Departamental a la Pasarela de Pagos y de ahí a la Entidad Financiera para se certificados. o DNI del tercero o Número de cuenta encriptado con las claves simétricas intercambiadas entre la Pasarela de Pagos y la Entidad Financiera o Resultado de la certificación: **OK** • El tercero está asociado al número de cuenta de alguna forma (titular, autorizado, co-titular, etc) En este caso, la Entidad Financiera incluirá un **NRC de la certificación**: Cada certificación de asociación tercero-número de cuenta incluirá un número de referencia completo como "firma" de la Entidad Financiera de la validez de los datos **NOK** • El tercero no tiene relación con el número de cuenta • El número de cuenta no existe **`protocolData`** Datos de protocolo.
Respuesta	El resultado de la certificación de la asociación tercero-número de cuenta se recibe desde la Pasarela de Pagos de forma asíncrona en la URL de callback indicada en la solicitud de certificación previa a la Pasarela de Pagos.

3.2.5.3 Función: Lote de asociaciones tercero-número de Cuenta Certificados

Características	Función de Callback en la Aplicación Departamental que recibe desde Pasarela de Pagos (que a su vez recibe de la Entidad Financiera) la certificación de **múltiples asociaciones tercero-número de cuenta** En el caso en que la aplicación Departamental solicitase la certificación de un lote de asociaciones tercero-número de cuenta, la Pasarela de Pagos se encargó previamente de "trocear" el lote en "paquetes" para cada una de las Entidades Financieras de forma que a cada una de ellas únicamente le llegan solicitudes de certificación relacionados con sus números de cuenta. En este caso, la Pasarela de Pagos se encargará de recibir las múltiples respuestas de las diferentes Entidades Financieras y componer un lote de respuesta único a la Aplicación Departamental. **IMPORTANTE:** • La URL de esta función de callback se envía en los datos de protocolo (*protocolData*) de las solicitudes a la Pasarela de Pagos • Se expondrá una única función de callback para recibir el resultado de la certificación de un lote de asociaciones tercer-número de cuenta.
Origen	**Pasarela de Pagos**
Destino	**Aplicación Departamental**
Método HTTP	POST
Función	**module=***certGateway* **function=***multipleHolderCertified* ***Parámetros***: **holderCertCertifiedDataList**: Lista de estructuras **holderCertCertifiedData** con los datos (asociación tercero-número de cuenta) enviados previamente desde la Aplicación Departamental a la Pasarela de Pagos para ser certificados por la Entidad Financiera o DNI del tercero o Número de cuenta encriptado con las claves simétricas intercambiadas entre la Pasarela de Pagos y la Entidad Financiera o Resultado de la certificación: **OK** • El tercero está asociado al número de cuenta de alguna forma (titular, autorizado, co-titular, etc) En este caso, la Entidad Financiera incluirá un **NRC de la certificación**: Cada certificación de asociación tercero-número de cuenta incluirá un número de referencia completo como "firma" de la Entidad Financiera de la validez de los datos **NOK** • El tercero no tiene relación con el número de cuenta • El número de cuenta no existe NOTA: Dado que el número de registros a certificar puede ser muy grande, este parámetro con la lista de registros a certificar se enviará comprimido en formato ZIP **EOF:** End Of File Se puede dar la situación de que desde una Aplicación Departamental se solicite la validación de la asociación tercero-número de cuenta en una Entidades Financieras no integradas en la Pasarela de Pagos (interoperabilidad telemática), por lo que la certificación se hará manualmente (ver punto 4-Alternativa de Funcionamiento Manual). En este caso, la respuesta puede demorarse y por esta razón, es posible que la Pasarela de Pagos devuelva la respuesta en varios envíos: • Uno para las respuestas recibidas on-line • Otro para las respuestas recibidas más tarde (resueltas manualmente en la Entidad Financiera). El parámetro EOF indica si se han enviado todas las certificaciones solicitas originalmente o alguna está pendiente de certificación manual.

	`protocolData` Datos de protocolo.
Respuesta	El resultado de la certificación múltiple de asociación tercero-número de cuenta se recibe desde la Entidad Financiera de forma asíncrona en la URL de callback indicada en la solicitud de certificación previa a la Entidad Finaciera

3.2.6 Estructuras de Datos intercambiadas

En este punto se resumen cada una de las estructuras de datos intercambiadas en las funciones detalladas anteriormente:

3.2.6.1 Solicitudes de Certificación

holderCertData

Descripción	Datos a certificar: pareja tercero-número de cuenta.
Estructura	holderCertData — Estructura que encapsula los datos sobre el tercero y el número de cuenta type — tipo de certificación (normalmente *accountNumber*) encType — Encriptación del número de cuenta accountNumberFormat — Formato del número de cuenta (normalmente IBAN) itemToCertNumber (CDATA) — Número de cuenta encriptado con la clave simétrica intercambiada entre la Pasarela de Pagos y la Entidad Financiera citizenId — Identificador del tercero (normalmente el DNI)

Ejemplo XML	`<holderCertData type='accountNumber' encType='hex' accountNumberFormat='iban'>`
	`<itemToCertNumber><![CDATA[`
	`6BC5E5582726500BB248EE788B63650608C7E2CCC8E9F760`
	`]]></itemToCertNumber>`
	`<citizenId>78882525</citizenId>`
	`</holderCertData>`

holderCertDataList

Descripción	Estructura que encapsula múltiples estructura de datos a certificar: pareja tercero-número de cuenta. (utilizado en las solicitudes de certificación múltiple)
Estructura	holderCertDataList — Encapsula varias estructuras *holderCertData* itemCount — Número de elementos *holderCertData* holderCertData — Estructura que encapsula los datos sobre el tercero y el número de cuenta

Ejemplo XML	`<holderCertDataList itemCount='3'>`
	`<holderCertData>…</holderCertData>`
	`<holderCertData>…</holderCertData>`
	`<holderCertData>…</holderCertData>`
	`</holderCertDataList>`

3.2.6.2 Respuestas de Certificación

holderCertCertifiedData

Descripción	Estructura que encapsula la respuesta a una solicitud de certificación de la asociación entre un tercero y un número de cuenta
Estructura	holderCertCertifiedData: Encapsula • Datos de la asociación tercero-cuenta que se han certificado • Resultado de la certificación holderCertData: Estructura que encapsula los datos sobre el tercero y el número de cuenta (ver punto anterior) holderCertResponse: Respuesta a la certificación timeStamp: Sello de tiempo finantialOrgCode: Código de la Entidad Financiera NRC: NRC generado para la operación certCode: Código de certificación (la respuesta de la certificación de la asociación tercero-número de cuenta). Códigos Generales: -1: el tercero no está asociado al número de cuenta o el número de cuenta no existe 1: el tercero es titular/cotitular de la cuenta. 2: el tercero es autorizado de la cuenta - 2: el tercero es titular de la cuenta pero ésta ha sido modificada. [En este caso se envía la nueva cuenta en el mismo formato usado en el envió de la consulta de la cuenta original] Códigos de Error -999: Error debido a la infraestructura de la Entidad Financiers (*p.e. las máquinas de HOST que realizan la validación caídas*). **Implica** que tras un tiempo, con la infraestructura recuperada, la **Pasarela realizará la misma consulta** esperando obtener un código general de resultado [*-1,1,2,-2*] updatedHolderCertData: En el caso de que se devuelva el código [-2], esta estructura contendrá el nuevo número de cuenta. [Ver ejemplo[2] de xml de cuenya modificada. accountConstraintList / accountContraint id: En el caso de que la cuenta tenga restricciones se podrá enviar . • Ejemplo : [Restricción para cargo en cuenta] accountConstrat ID= DISALLOW_WITHDRAW

Ejemplo [1]: XML de Cuenta en la que el Tercero es Titular	`<holderCertCertifiedData>`
	`<holderCertData type='accountNumber' encType='hex' accountNumberFormat='iban'>`
	`<itemToCertNumber><![CDATA[`
	`6BC5E5582726500BB248EE788B63650608C7E2CCC8E9F760`
	`]]></itemToCertNumber>`
	`<citizenId>78882525</citizenId>`
	`</holderCertData>`
	`<holderCertResponse>`
	`<timeStamp>1282839644970</timeStamp>`
	`<finantialOrgCode>9999</finantialOrgCode>`
	`<certCode>1</certCode>`
	`<nrc enctype='hex'>xxxxxxxx</nrc>`
	`</holderCertResponse>`

```
</holderCertCertifiedData>
```

Ejemplo [2] XML de Cuenta en la que el Tercero es Titular pero el número de cuenta ha cambiado.

```
<holderCertCertifiedData>
        <holderCertData type='accountNumber' encType='hex'
                        accountNumberFormat='iban'>
                <itemToCertNumber><![CDATA[
                6BC5E5582726500BB248EE788B63650608C7E2CCC8E9F760
                ]]></itemToCertNumber>
                <citizenId>78882525</citizenId>
        </holderCertData>
        <holderCertResponse>
                <timeStamp>1282839644970</timeStamp>
                <finantialOrgCode>9999</finantialOrgCode>
                <certCode>-2</certCode>
                <nrc enctype='hex'>xxxxxxxx</nrc>
                <!—Nuevo Número de Cuenta -→
                <updatedHolderCertData
                          enctype='hex'
                          accountNumberFormat='cc'
                          type='accountNumber' >
                    <itemToCertNumber><![CDATA[
                6BC5E5582726500BB248EE788B63650608C7E2CCC8E9F760
                ]]></itemToCertNumber>
                </updatedHolderCertData>
        </holderCertResponse>
</holderCertCertifiedData>
```

Ejemplo [3] XML de Cuenta en la que el Tercero es Titular pero tiene restricciones para cargo en cuenta

```
<holderCertCertifiedData>
        <holderCertData type='accountNumber' encType='hex'
                        accountNumberFormat='iban'>
                <itemToCertNumber><![CDATA[
                8BC5E5582726500BB248EE788B63650608C7E2CCC8E9F760
                ]]></itemToCertNumber>
                <citizenId>78882525</citizenId>
        </holderCertData>
        <holderCertResponse>
                <timeStamp>1282839644970</timeStamp>
                <finantialOrgCode>9999</finantialOrgCode>
                <certCode>1</certCode>
                <nrc enctype='hex'>xxxxxxxx</nrc>
                 <accountConstraintList>
                   <accountConstraint id='DISALLOW_WITHDRAW'>
                 <accountConstraintList>
        </holderCertResponse>

</holderCertCertifiedData>
```

holderCertCertifiedDataList

Descripción	Estructura que encapsula las respuestas individuales a una solicitud de múltiples certificaciones de la asociación entre un tercero y un número de cuenta
Estructura	holderCertCertifiedDataList — Encapsula la respuesta a solicitudes de certificación múltiples en elementos *holderCertCertifiedData* itemCount — Número de elementos holderCertCertifiedData — Encapsula la respuesta de una certificación sencilla (individual) de asociación tercero-número de cuenta: • Datos de la asociación tercero-cuenta que se han certificado • Resultado de la certificación

Ejemplo XML	`<holderCertCertifiedDataList itemCount='3'>`
	`<holderCertCertifiedData>…</holderCertCertifiedData>`
	`<holderCertCertifiedData>…</holderCertCertifiedData>`
	`<holderCertCertifiedData>…</holderCertCertifiedData>`
	`</holderCertCertifiedDataList>`

3.2.6.3 Estructuras Comunes

protocolData

Descripción	Datos de protocolo de la llamada a función.
Estructura	protocolData — Estructura que encapsula los datos de protocolo token — Token de la llamada. Cada una de las llamadas entre sistemas tendrá un token único. Normalmente no se utiliza callBackURL — Dado que todas las llamadas son **asíncronas**, el sistema "destino" tiene que devolver la respuesta al sistema "origen" enviando un mensaje a la url de vuelta timeStamp — Sello de tiempo de la llamada
Ejemplo XML	<protocolData> <token>99asdfads1231</token> <callBackURL>URL</callBackURL> <timeStamp>dd:MM:yyyy-hh.mm.SS.MMMM</timeStamp> </protocolData>

OperationResult

Descripción	Resultado de una operación.
Estructura	operationResult — Encapsula el resultado de la llamada a una operación de un sistema resultado resultadoOK — **true** si la llamada al sistema ha sido exitosa. **NOTA**: No confundir con la respuesta de la función llamada. Simplemente indica que el sistema destino ha procesado correctamente la llamada, aunque es posible que la función devuelva un error. returnCode — Código de error devuelto por la función llamada returnValue — Valor devuelto por la función llamada **NOTA**: En el caso del presente proyecto en que la respuesta a todas las funciones es asíncrona (no se devuelve como respuesta directamente a la invocación de la función), tanto el campo *returnCode* como *returnValue* no tienen sentido
Ejemplo XML	<operationResult> <resultado> <resultadoOK>true</resultadoOK> <returnValue></returnValue> <returnCode>0</returnCode> </resultado> </operationResult>

4 Alternativa de Funcionamiento Manual

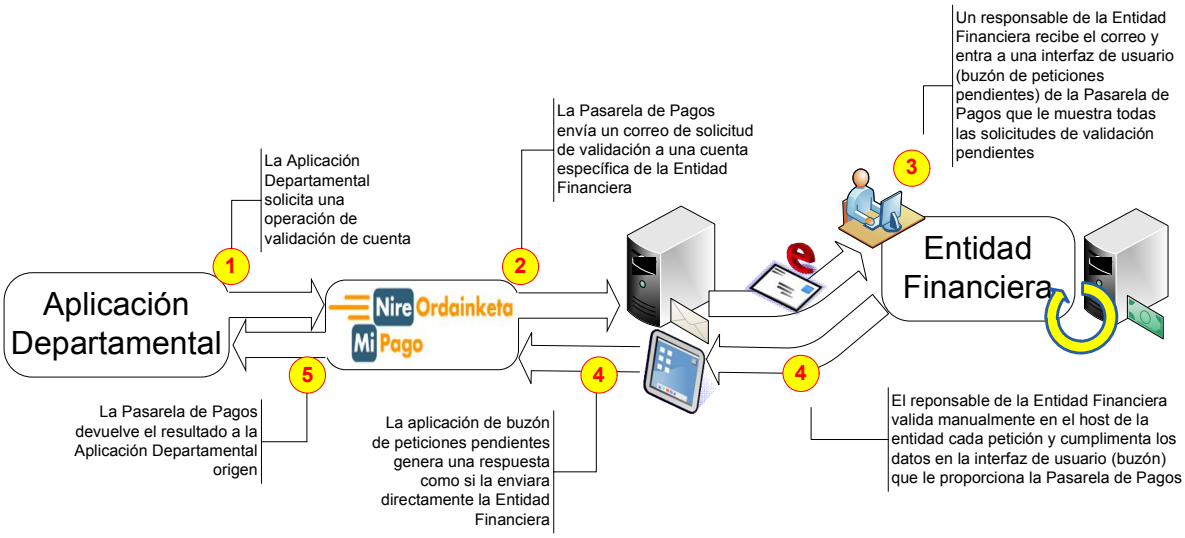
El funcionamiento anteriormente descrito propone una integración automática, sin intervención humana (o al menos no desde la parte de la Administración); este escenario es viable para el caso de todas las Entidades Financieras integradas en la Pasarela de Pagos, sin embargo aquellas otras que no están integradas tienen varias opciones:

1. Incorporarse de forma completa a la Pasarela de Pagos implementando todas las funcionalidades (pago en cuenta / con tarjeta, consulta del estado del pago, emisión de justificantes con NRC, etc)
2. Incorporarse en la Pasarela de forma parcial implementando únicamente la funcionalidad de validación de números de cuenta.
3. No incorporarse a la Pasarela de Pagos a nivel de integración de sistemas y resolver las peticiones de validación de número de cuenta corriente de forma manual.

Preferentemente las Entidades Financieras deberían abordar una integración de sistemas, bien con incorporándose plenamente a la Pasarela de Pagos o bien implementando únicamente la funcionalidad de validación del número de cuenta.

En casos muy concretos en los que el número de peticiones de validación no justifique la inversión de un desarrollo de integración de sistemas, se podría plantear la alternativa (3) que propone una integración manual.

Esta integración manual funcionará de la siguiente forma:



Básicamente se sustituye la interacción entre sistemas por una interfaz de usuario que simula un buzón de peticiones de validación pendientes proporcionado por la Pasarela de Pagos y donde un responsable de la Entidad Financiera tendrá que cumplimentar manualmente las peticiones.

5 ANEXO (I) : Algoritmos y Procesos de Encriptación

Proceso	Algoritmo	Claves
Generación del NRC	Algoritmo DES	Se proporcionarán dos semiclaves para la generación de HASH_MAC del Número de Referencia. Estas claves serán usados en la siguientes funcionalidades: 1) Pasarela de Pagos. 2) Pasarela de Validación de Cuentas *Nota: Para las Entidades Financieras que tengas implementadas la funcionalidades de la Pasarela de Pago no se requerirá intercambiar de nuevos la claves.*
Encriptación de Números de Cuenta y tarjetas	Algoritmo Triple DES	Se proporcionarán dos semiclaves para la encriptación de números de cuenta/tarjetas que Estas claves serán usados en la siguientes funcionalidades: 1) Pago Directo - Móvil , encriptación de nº de tarjeta. 2) Pasarela de Validación de Cuentas, encriptación de nº de cuenta. *Nota: Para las Entidades Financieras que tengan implementadas la funcionalidades de Pago Directo/Móvil no se requerirá intercambiar de nuevos la claves.*

6 ANEXO (II): GENERACIÓN DE NRC

El **NRC de Validación de Cuentas** se calcula en base a los siguientes campos:

Entidad Emisora	Identificador de la **Entidad Emisora** de la liquidación **11** caracteres (se rellena con ceros a la izquierda hasta la longitud del campo)	Código que **identifica a la Administración emisora** de la liquidación + sufijo de identificación de Órgano emisor de validación. Ejemplo : *04833001800* 11 Caracteres formados por : *04833001* ➔ *CIF sin letras GV* *800* ➔ *Juventud. Ayudas.*
	Identificador de la Petición de Validación **19** caracteres (se rellena con ceros a la izquierda hasta la longitud del campo)	Código **emitido por la Administración** y que permite identificar la petición de validación de cuenta.

Entidad Financiera	Identificador de la **Entidad Financiera** **4** caracteres	Código de 4 caracteres asignado por el Banco de España a la Entidad Financiera
	Identificador del Justificante de Petición de Validación para la Entidad Financiera **15** caracteres (se rellena con ceros a la izquierda hasta la longitud del campo)	Identificador interno del pago para la Entidad Financiera y que permite identificar la petición de validación 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.
Digito de Paridad	El digito será 0	Digito de paridad para la los datos de validación.

A partir de estos **50 caracteres** se genera una firma utilizando la **función MAC** (*Message Athentication 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 algorimo 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 (19 caracteres) y la firma (8 caracteres), en total 27 caracteres:

NRC (27) =	**Identificación del justificante (19)**		**+**	**firma (8)**
	Código de la Entidad Financiera	**Identificador del Justificante de Validación de Cuenta para la Entidad Financiera**	+	**firma**
27	**4**	**15**		**8**