

**11.2010**

**Manual de uso para el intercambio telemático de archivos con el  
Banco de España**

I.E. 2005.24

Departamento de Sistemas de Información

---

## Hoja de Control

<b>Título</b>	Manual de uso para el intercambio telemático de archivos con el Banco de España
<b>Autor</b>	Departamento de Sistemas de Información
<b>Versión</b>	04.1
<b>Fecha</b>	30-11-2010

## Registro de Cambios

<b>Versión</b>	<b>Fecha</b>	<b>Motivo del cambio</b>
01	18-09-2006	Se autoriza la utilización de la red privada IP del SNCE sustituyendo a la antigua red x-25. Se autoriza la utilización del servicio FileAct de SWIFTNet. Se incluye una nota para las entidades con PGP 9.0 o posterior.
02	14-03-2008	Se autoriza la utilización de la red privada del Banco de España. Se autoriza la utilización de la red interadministrativa del Mº de Administraciones Públicas. Se elimina la posibilidad del alta en el servicio con correo X.400 o Editran a través de la red X-25 aunque siga autorizado para los que ya lo están usando. Se modifican los procedimientos relacionados con certificados electrónicos para adaptarlos a la aplicación de obtención de certificados por Internet. Se reestructura el documento para su mejor comprensión.
03	18-08-2009	Especificaciones para envío/recepción de ficheros FileAct en el servicio bde.eca.sf Reestructuración y actualización contenidos.
04	01-06-2010	Especificaciones para envío de ficheros al Banco de España utilizando la interface Web vía RedBdE, Intranet Administrativa o Internet.
04.1	30-1-2010	Modificaciones relativas a la dirección destinataria de las cartas de alta e inclusión de datos de contacto funcional y eliminación especificaciones datos de red en Editran.

## ÍNDICE

1	Introducción	1
2	Responsabilidades del Banco de España sobre la información transmitida entre el Banco de España y la entidad	2
3	Canales de comunicación	3
3.1	Introducción	3
3.1.1	Canales de comunicación aceptados por el Banco de España	3
3.1.2	Mecanismos de control de acceso aceptados	3
3.1.3	Condiciones generales para el envío y recepción de archivos entre la entidad y el Banco de España	3
3.2	ITW - Interface Web para envío de ficheros.	4
3.2.1	Introducción	4
3.2.2	Equipamiento	4
3.2.3	Condiciones para el envío y recepción de archivos	4
3.2.4	Envío de archivos de la entidad al Banco de España	4
3.2.5	Recepción de archivos del Banco de España en la entidad	4
3.2.6	Mecanismos de control de acceso: autorización mediante certificados digitales	4
3.2.7	Manual de uso ITW	5
3.3	Editran	5
3.3.1	Equipamiento	5
3.3.2	Condiciones para el envío y recepción de archivos	5
3.3.3	Envío de archivos de la entidad al Banco de España	5
3.3.4	Recepción de archivos del Banco de España en la entidad	5
3.3.5	Mecanismos de control de acceso aceptados	5
3.4	Servicio FileAct de SWIFTNet	6
3.4.1	Equipamiento	6
3.4.2	Condiciones para el envío y recepción de archivos	6
3.4.3	Condiciones particulares para el envío de archivos de la entidad al Banco de España	6

3.4.4	Condiciones particulares para la recepción de archivos del Banco de España en la entidad	6
3.5	Correo electrónico Internet	7
3.5.1	Introducción	7
3.5.2	Equipamiento	7
3.5.3	Condiciones para el envío y recepción de archivos	7
3.5.4	Condiciones particulares para el envío de archivos de la entidad al Banco de España	7
3.5.5	Condiciones particulares para la recepción de archivos del Banco de España en la entidad	7
3.5.6	Mecanismos de control de acceso aceptados: Cifrado y firmado mediante certificados digitales	8
4	Mecanismos de seguridad	9
4.1	Cuestiones generales	9
4.2	Cifrados específicos sobre Editran	9
4.3	Cifrado y firmado mediante certificados digitales	9
4.3.1	Condiciones generales	9
4.3.2	Aspectos generales a tener en cuenta cuando se utilicen certificados electrónicos en el mecanismo de correo electrónico Internet	10
4.3.3	Respaldo de claves	10
4.3.4	Autorización de entidades a procesos	11
4.3.5	Autorización de nuevos certificados a un proceso informático que la entidad ya esté utilizando	11
4.3.6	Desautorización de certificados a un proceso informático	11
5	Procedimiento de alta de una entidad en un proceso	12
5.1	Cuestiones generales	12
5.2	Datos fijos que se deberán incluir en la carta de solicitud de alta	12
5.3	Datos variables	12
6	Anejo 1. Modelo de carta para solicitar el alta de comunicaciones al Banco de España	13
6.1	Datos fijos	14
6.2	Datos variables:	15
6.2.1	Para envíos al Banco de España mediante ITW	15

6.2.2	Para comunicaciones mediante correo electrónico Internet firmado y cifrado mediante certificados electrónicos:	16
6.2.3	Para comunicaciones mediante Editran utilizando la criptografía del SNCE o el cifrado de clave pública de Indra	17
6.2.4	Para comunicaciones mediante FileAct	17
7	Anejo 2. Formato de los archivos de datos	18
7.1	Correo electrónico internet e ITW	18
7.2	Editran (Cifrado SNCE y cifrado de clave pública de Indra)	18
7.3	Juego normal de caracteres	18
8	Anejo 3. Procedimientos de gestión de certificados	21
8.1	Solicitud de certificados al Banco de España	21
8.2	Renovación de certificados emitidos por el Banco de España	23
8.3	Revocación de certificados emitidos por el Banco de España	23
8.4	Renovación del certificado de cifrado del Banco de España	24
8.5	Revocación de certificados emitidos por un PSC	24
8.6	Glosario de términos para certificados digitales	25
8.6.1	Definiciones	25
8.6.2	Acrónimos	25
9	Anejo 4: Características técnicas para la transmisión de ficheros vía FileAct	26
9.1	Consideraciones previas	26
9.1.1	Especificaciones para realizar el e-ordering	26
9.1.2	Parametrización para envío	26
9.1.3	Parametrización recepción	27
9.1.4	Pruebas de conectividad	27
10	Datos de contacto	29



## 1 Introducción

Con este documento se pretende facilitar el envío y la recepción de archivos hacia/desde el Banco de España, para lo que se deberá usar alguno de los canales de comunicación, detallados más adelante.

A los efectos de esta instrucción, se define como “canal” a un protocolo específico implementado en una red concreta, y como “proceso” al procedimiento de intercambio de ficheros definido por el departamento destinatario de la información a intercambiar entre las entidades y el Banco de España.

Cada departamento elaborará las instrucciones y directrices específicas para cada proceso de intercambio de ficheros, indicando también los canales de comunicación permitidos para dicho proceso. Estas instrucciones se denominarán en este documento “Manual de Uso”, aunque podrían tener un título diferente.

Será responsabilidad de la entidad realizar las operaciones correspondientes de instalación y configuración del equipo y del software, siguiendo las instrucciones que el Banco de España y el proveedor del servicio/producto suministran.

La transmisión de datos se podrá realizar de forma general a través de cualquiera de los canales de transmisión que a continuación se detallan:

- ITW - Interface Web para envío de ficheros (a través de RedBdE, Intranet Administrativa o Internet)
- Producto de transmisión de archivos Editran (a través de RedBdE, Intranet Administrativa o SNCE)
- Servicio FileAct de SWIFTNet
- Correo electrónico Internet

En el apartado 3 se detallan los distintos los canales de comunicación existentes en el Banco de España y sus condiciones de uso; en el apartado 4 se describen los mecanismos de seguridad admitidos, y en el apartado 5 se establece el procedimiento de solicitud de alta de una entidad en un proceso.

Finalmente se añaden unos anejos para mayor aclaración de lo establecido en los puntos anteriores. Se recomienda revisar estas instrucciones en su totalidad antes de proceder a realizar intercambios telemáticos con el Banco de España.

## **2 Responsabilidades del Banco de España sobre la información transmitida entre el Banco de España y la entidad**

El Banco de España establecerá los procedimientos y herramientas informáticas, dentro de las posibilidades tecnológicas de cada momento, para que la transmisión de la información entre la entidad y éste se efectúe de una manera segura y eficiente.

El Banco de España sólo se responsabilizará de la información transmitida por vía telemática en los términos en que ésta haya sido recibida y desde el momento de su recepción en sus dependencias, en la forma que se determine. De igual modo se responsabilizará del adecuado tratamiento de la información recibida de las entidades, velando asimismo por que la información que se envíe desde el Banco de España se produzca según los procedimientos establecidos en cada momento.

No serán responsabilidad del Banco de España los posibles errores o manipulaciones de ninguna clase, intencionada o no, que pudieran afectar a la información transmitida por vía telemática por las entidades, ya fueran aquellos causados bien por la propia entidad transmisora o bien por terceras personas, siempre que se hubieran producido antes de la recepción de la información en el Banco de España.

### 3 Canales de comunicación

#### 3.1 Introducción

##### 3.1.1 Canales de comunicación aceptados por el Banco de España

Los canales actuales aceptados de forma genérica por el Banco de España para la transmisión telemática de archivos son:

- ITW - Interface Web (a través de RedBdE, Intranet Administrativa o Internet)
- Producto de transmisión de archivos Editran. (a través de RedBdE, Intranet Administrativa o SNCE)
- Servicio FileAct de SWIFTNet.
- Correo electrónico Internet.

##### 3.1.2 Mecanismos de control de acceso aceptados

En general, los archivos (confidenciales o no), que se intercambian entre las entidades y el Banco de España irán cifrados. Dependiendo de la vía de transmisión que se utilice se han habilitado los siguientes medios:

VÍA DE TRANSMISIÓN	MODALIDAD DE CIFRADO
ITW	Certificados digitales
Editran	Cifrado SNCE: Servicios de criptografía especificados en las Instrucciones Operativas de la Norma SNCE002
	Cifrado INDRA: Software de clave pública de Indra
Servicio FileAct de SWIFTNet	El proporcionado por SWIFT
Correo electrónico Internet	Certificados digitales

Una descripción más detallada de los mismos se encuentra en el apartado 4.

##### 3.1.3 Condiciones generales para el envío y recepción de archivos entre la entidad y el Banco de España

Según se indicó anteriormente, el departamento propietario de la información a intercambiar elaborará las instrucciones y directrices específicas para cada proceso de intercambio (denominadas en este documento "Manual de Uso", aunque podrían tener un título diferente), indicando también los canales de comunicación permitidos para el proceso. Estos manuales podrán establecer horarios distintos de los generales establecidos para cada vía de comunicación. El envío de archivos fuera de los períodos previstos puede dar lugar a errores o al no procesamiento de los archivos enviados.

Los archivos de datos que se envíen al Banco de España, una vez preparados para ser procesados, podrán sufrir cambios de juego de caracteres (de ASCII a EBCDIC y viceversa), por lo que es obligatorio usar exclusivamente el conjunto de caracteres detallados en el anejo 2 (o el más limitado que pueda exigir el correspondiente sistema de información del Banco de España), ya que el uso de caracteres distintos puede dar lugar a errores en el procesamiento de los archivos.

A medida que el Banco de España vaya adaptando sus diferentes sistemas de información, irá comunicando a las entidades las condiciones para el envío y la recepción de archivos con la antelación suficiente.

## **3.2 ITW - Interface Web para envío de ficheros.**

### **3.2.1 Introducción**

El sistema ITW permite el intercambio de ficheros con el Banco de España desde el portal de acceso del Banco de España accesible desde RedBdE y la Intranet Administrativa o desde el portal del Banco de España en internet.

### **3.2.2 Equipamiento**

- Navegador Web Internet Explorer 6.0 o superior
- Certificados digitales
- Acceso a la red desde la que se realizará el envío de ficheros

### **3.2.3 Condiciones para el envío y recepción de archivos**

Salvo indicación en contrario o por necesidades específicas, el sistema estará disponible de 8.00 a 22.00 de lunes a viernes salvo festivos a nivel nacional y europeo.

### **3.2.4 Envío de archivos de la entidad al Banco de España**

Por cada transmisión, sólo se enviará un archivo con las características detalladas en el anejo 2.

Cada sistema de información del Banco de España notificará en el correspondiente Manual de Uso los posibles valores distintos de los generales para el envío de los distintos archivos.

### **3.2.5 Recepción de archivos del Banco de España en la entidad**

El Banco de España pondrá a disposición de la entidad los archivos destinados a la misma que los usuarios autorizados podrán recoger del Banco de España a través del canal ITW.

Los archivos permanecerán a disposición de la entidad durante un periodo de tiempo determinado pasado el cual dejarán de estar disponibles para las entidades.

### **3.2.6 Mecanismos de control de acceso: autorización mediante certificados digitales**

Para realizar el proceso de autenticación, autorización al envío y creación del entorno de seguridad para su transmisión, se utilizarán certificados electrónicos que podrán ser emitidos, bien por un Prestador de Servicios de Certificación (en adelante PSC) de entre los reconocidos por el Banco de España según lo publicado en la dirección <http://pki.bde.es>, bien por el propio Banco de España.

En el Manual de Uso asociado a cada proceso se podrán limitar, en caso de que esta vía de comunicación esté admitida, las Autoridades de Certificación admitidas para dicho servicio.

Para más información, consultar el apartado 4.3.

### **3.2.7 Manual de uso ITW**

Las instrucciones para el envío de ficheros por el sistema ITW se describen en el documento: "ITW - Manual de uso" disponible en la dirección:

<http://www.bde.es/webbde/es/secciones/servicio/intercambio/intercambio.html>

## **3.3 Editran**

### **3.3.1 Equipamiento**

Para poder intercambiar archivos con el Banco de España usando esta vía, la entidad debe tener una licencia de uso del producto Editran en cualquiera de las plataformas soportadas por este producto. Si no se posee licencia y se pretende adquirir para poder intercambiar archivos con el Banco de España usando esta vía, la entidad debe ponerse en contacto con el suministrador de Editran con objeto de conocer las ofertas para las distintas plataformas hardware y conocer cuál se adapta mejor a su infraestructura informática.

Esta vía se utilizará mediante protocolo TCP/IP y las opciones de cifrado vendrán establecidas por los enlaces de la red a través de la cual se esté accediendo. Las redes admitidas para ello son las siguientes

- Red privada virtual SNCE;
- Red privada virtual de Banco de España (RedBdE);
- Red privada virtual del Ministerio de Administraciones Públicas (Intranet Administrativa).

### **3.3.2 Condiciones para el envío y recepción de archivos**

Salvo indicación en contrario o por necesidades específicas, el sistema estará disponible de 8.00 a 22.00 de lunes a viernes salvo festivos a nivel nacional y europeo.

### **3.3.3 Envío de archivos de la entidad al Banco de España**

Por cada transmisión, sólo se enviará un archivo con las características detalladas en el anejo 2.

Cada sistema de información del Banco de España notificará en el correspondiente Manual de Uso los posibles valores distintos de los generales para el envío de los distintos archivos.

### **3.3.4 Recepción de archivos del Banco de España en la entidad**

El Banco de España enviará en cada mensaje un único fichero de datos.

De acuerdo con los requerimientos de cada proceso específico los ficheros se intentan enviar durante un periodo de tiempo determinado pasado el cual los archivos pendientes de envío dejan de estar disponibles para dicho envío.

### **3.3.5 Mecanismos de control de acceso aceptados**

Criptografía propia del SNCE o clave pública de Indra. (Ver [apartado 4](#))

### **3.4 Servicio FileAct de SWIFTNet**

#### **3.4.1 Equipamiento**

Para poder intercambiar archivos con el Banco de España usando esta vía, la entidad deberá disponer de los medios técnicos que SWIFT tiene fijados para la misma, así como haber solicitado previamente su inscripción en los grupos cerrados de usuarios (CUG) bde.eca.sfl (pilot) y bde.eca.sf (live) por el procedimiento de suscripción al servicio (e-ordering) establecido en la página [www.swift.com](http://www.swift.com).

Todos los costes inherentes a la transmisión de ficheros, incluido el tráfico, serán por cuenta de la entidad.

#### **3.4.2 Condiciones para el envío y recepción de archivos**

Salvo indicación en contrario o por condicionantes particulares, el sistema estará disponible de 8.00 a 22.00 de lunes a viernes salvo festivos a nivel nacional y europeo.

Al ser un servicio de almacenamiento y reenvío (store&forward), la entidad podrá enviar/recibir ficheros siempre que el servicio FileAct de SWIFTNet esté disponible.

Una vez solicitada el alta del proceso según se describe en el [Anejo1](#) (puntos 6.1 y 6.2) y tras haber sido aprobados los e-ordering correspondientes a los servicios especificados en el apartado anterior, es necesario realizar unas pruebas de conectividad básicas para garantizar la configuración adecuada en los entornos Pilot y Live, según se describe en el [anejo 4](#) (punto 9).

Dichas pruebas son prerequisite para habilitar la transmisión de ficheros vía FileAct en el entorno de producción para el proceso solicitado y para su realización el Banco de España coordinará y planificará la ejecución de las mismas con la entidad.

Si la entidad hubiera realizado las pruebas de homologación básicas anteriormente no sería necesaria la realización de las mismas.

#### **3.4.3 Condiciones particulares para el envío de archivos de la entidad al Banco de España**

Los ficheros pueden enviarse comprimidos según se contempla en el apartado 6.2.3. En este caso el archivo comprimido solo contendrá un único fichero.

El horario de transmisión es el general detallado anteriormente, salvo que el sistema de información correspondiente del Banco de España establezca períodos determinados. El envío de archivos fuera de los períodos previstos puede dar lugar a errores o al no procesamiento de los archivos enviados.

#### **3.4.4 Condiciones particulares para la recepción de archivos del Banco de España en la entidad**

El horario de transmisión es el general detallado anteriormente, salvo que el sistema de información correspondiente del Banco de España establezca períodos determinados. El archivo

será transmitido durante los períodos previstos a petición de la entidad, siempre que ésta tenga actualizado correctamente el fichero de configuración del sistema.

### **3.5 Correo electrónico Internet**

#### **3.5.1 Introducción**

El correo electrónico Internet está muy difundido, sin embargo, no es fiable (un pequeño porcentaje de mensajes no llegan a su destino; se puede suplantar al remitente, etc.), por ello, esta vía de intercambio no está autorizada para todos los servicios electrónicos ofrecidos por el Banco de España. Solo se podrá usar si el correspondiente manual de uso de sistema de información donde se indican los formatos y condiciones particulares del intercambio así lo detalla.

#### **3.5.2 Equipamiento**

- Una dirección de correo;
- Una aplicación cliente de correo electrónico;
- Un certificado digital admitido por el BdE y que contenga la dirección de correo desde la que se va a realizar el envío.

#### **3.5.3 Condiciones para el envío y recepción de archivos**

El horario general de transmisión es de 24 horas al día, 7 días a la semana. Sin previo aviso, a partir de las 22:00 hasta las 8:00 del día siguiente pueden producirse interrupciones del servicio, así como en los días no laborables a nivel nacional.

#### **3.5.4 Condiciones particulares para el envío de archivos de la entidad al Banco de España**

Por cada transmisión, sólo se enviará un archivo cifrado con las características detalladas en el anejo 2. El archivo deberá ir como un anejo del mensaje y este anejo deberá ser del tipo indefinido (Binary Body Part 14).

La dirección de correo a la que deben enviarse los mensajes con los archivos es la siguiente: [correo@procesos.bde.es](mailto:correo@procesos.bde.es)

#### **3.5.5 Condiciones particulares para la recepción de archivos del Banco de España en la entidad**

El Banco de España enviará en cada mensaje un archivo de texto y opcionalmente un archivo de datos cifrado. El archivo de datos irá como un anejo del mensaje y será del tipo indefinido (Binary Body Part 14).

La dirección del buzón remitente del mensaje se adaptará al previsto por el sistema de información del Banco de España

Para su identificación por la entidad receptora, los primeros caracteres del Asunto del mensaje se adaptarán a los previstos en el Manual de Uso asociado al proceso para cada entidad.

### **3.5.6 Mecanismos de control de acceso aceptados: Cifrado y firmado mediante certificados digitales**

En general, cuando se admita el uso de certificados electrónicos, éstos podrán ser emitidos, bien por un Prestador de Servicios de Certificación (en adelante PSC) de entre los reconocidos por el Banco de España según lo publicado en la dirección <http://pki.bde.es>, bien por el propio Banco de España.

En el Manual de Uso asociado a cada proceso se indicará, en caso de que esta vía de comunicación esté admitida, las autoridades de certificación o restricciones reconocidas para su emisión (Banco de España y/o PSCs).

Para más información, consultar el apartado 4.

## 4 Mecanismos de seguridad

### 4.1 Cuestiones generales

En general, los archivos (confidenciales o no), que se intercambian entre las entidades y el Banco de España irán cifrados. Dependiendo de la vía de transmisión que se utilice se han habilitado los siguientes medios:

VÍA DE TRANSMISIÓN	MODALIDAD DE CIFRADO
Interfaz web para el envío de ficheros	Certificados digitales
Editran	Cifrado SNCE: Servicios de criptografía especificados en las Instrucciones Operativas de la Norma SNCE002 Cifrado INDRA: Software de clave pública de Indra
Servicio FileAct de SWIFTNet	El proporcionado por SWIFT
Correo electrónico Internet	Certificados digitales

### 4.2 Cifrados específicos sobre Editran

Las entidades participantes como asociadas en el SNCE que se conecten vía Editran podrán utilizar los servicios de criptografía especificados en la Norma SNCE002.

El resto de entidades utilizarán el software de clave pública de Indra.

#### **Servicios de criptografía de la Norma SNCE002.**

A las entidades que participan como asociadas en el SNCE, Indra les suministrará las interfaces desarrolladas para poder utilizar desde Editran estos servicios, informándoles sobre cómo se deben parametrizar las sesiones, tanto en Editran/P como en Editran/G.

#### **Criptografía de clave pública de Indra.**

Esta modalidad de criptografía debe ser contratada con Indra informándoles de que se va a utilizar para efectuar transmisiones con el Banco de España. El suministrador proporcionará la documentación adecuada para efectuar la parametrización.

En caso de que la entidad intercambie información con el Banco de España a través de la VPN o de la red de la Intranet Administrativa, el intercambio de la clave pública entre los dos puntos se hará automáticamente con el producto de Editran, usando para ello la sesión TELEGC.

### 4.3 Cifrado y firmado mediante certificados digitales

#### 4.3.1 Condiciones generales

El uso de certificados electrónicos como mecanismo de seguridad en el intercambio de información con el Banco de España está admitido para el correo electrónico Internet y para la interfaz web de envío de ficheros.

En general, cuando se admita el uso de certificados electrónicos en un servicio electrónico del Banco de España, éstos podrán haber sido emitidos por un Prestador de Servicios de Certificación (en adelante PSC) de entre los reconocidos por el Banco de España según lo

publicado en la dirección <http://pki.bde.es> o por la Autoridad de Certificación del propio Banco de España.

El anejo 3 describe el procedimiento de solicitud de un certificado a la Autoridad de Certificación del Banco de España, para aquellos casos en los que esté admitida esta posibilidad.

Para el canal de intercambio basado en correo electrónico Internet se requiere además disponer de una copia del certificado asociado a la dirección de correo a la que se han de enviar los mensajes. El titular de dicho certificado es el propio Banco de España, y ha de ser utilizado por la entidad para el cifrado de los mensajes de correo electrónico salientes. El Banco de España dispone de la clave privada necesaria para descifrar dichos mensajes. En la dirección de Internet <http://pki.bde.es/certs> se pueden obtener los certificados necesarios:

- Jerarquía de certificación de la PKI del Banco de España, es decir, certificados de la Autoridad de Certificación Raíz y de la Autoridad de Certificación Corporativa. Estos certificados son necesarios para que la aplicación de correo electrónico pueda confiar en el certificado mencionado a continuación
- Certificado asociado a la dirección de correo a la que se realizan los envíos. Habitualmente<sup>1</sup> se habrá de incorporar este certificado en una entrada de la libreta de direcciones de la aplicación cliente de correo electrónico asociada a la dirección correo@procesos.bde.es.

#### **4.3.2 Aspectos generales a tener en cuenta cuando se utilicen certificados electrónicos en el mecanismo de correo electrónico Internet**

- Para poder firmar un mensaje suele ser necesario que el certificado a utilizar contenga la dirección de correo desde el que se envía ya que, de lo contrario, la aplicación cliente de correo electrónico podría no permitir efectuar la firma. El Banco de España no está en disposición de ofrecer soporte técnico en este sentido a las entidades usuarias, por lo que se deberá consultar la documentación de la aplicación de correo electrónico en cuestión para conocer las peculiaridades de la misma al respecto del uso de certificados.

- Se admitirá que los mismos certificados puedan ser utilizados en procesos de sistemas de información distintos dentro de la misma entidad. No obstante, debe tenerse en cuenta que la reutilización de un certificado podría implicar la necesidad de utilizar en la entidad el mismo buzón de correo para todos los sistemas de información que usen dicho certificado. De lo contrario, la aplicación cliente de correo electrónico podría no permitir la firma de los mensajes salientes. En cualquier caso, será necesario que las claves privadas sean accesibles por todos los sistemas de información que compartan certificados.

#### **4.3.3 Respaldo de claves**

Se recomienda hacer copias de seguridad de las parejas de claves y de los certificados, independientemente de quien lo haya emitido (un PSC o el BdE).

Por otra parte, en el caso de utilizar certificados de persona física o de persona jurídica emitidos por un PSC, con objeto de asegurar la disponibilidad del servicio, se recomienda autorizar a dos o más certificados a cada proceso.

---

<sup>1</sup> Confirmar esta necesidad en la documentación de la aplicación cliente de correo electrónico.

#### **4.3.4 Autorización de entidades a procesos**

La solicitud de autorización de certificados a un proceso se tramitará mediante la carta de solicitud de alta en procesos ([ver Anejo 1](#)).

Existen varias posibilidades:

- Si se desea que el Banco de España emita un nuevo certificado (en el caso de que el proceso admita esta opción), se habrá de tramitar previamente la solicitud del certificado<sup>1</sup> e incluir el número de petición en la carta.
- Si se desea utilizar un certificado ya existente emitido por el Banco de España en el pasado, se habrá de incluir su nombre distintivo (conocido como DN, ver apartado 6) en la carta.
- Si se desea utilizar un certificado ya existente emitido por un Prestador de Servicios de Certificación, habrá que adjuntar además:
  - Cuando la vía de comunicación elegida sea correo electrónico Internet, la copia del certificado en formato .cer o .crt<sup>2</sup>
  - Cuando la vía de comunicación elegida sea ITW, el nombre distintivo del certificado (DN).

#### **4.3.5 Autorización de nuevos certificados a un proceso informático que la entidad ya esté utilizando**

Consistirá en el envío de una carta firmada por el solicitante en su día de alta en el proceso (o persona que lo sustituya) que contenga los datos de los nuevos certificados a autorizar al intercambio de información con el Banco de España. La información a incluir sobre los certificados es la misma que se describe en el apartado 4.3.4.

En el caso de correo electrónico, la autorización a un proceso informático de un nuevo certificado de componente emitido por el Banco de España implicará la desautorización automática del certificado o certificados hasta entonces vigentes. Sin embargo la autorización de un certificado emitido por un PSC, no implicará la desautorización de los certificados vigentes<sup>3</sup>.

En el caso de ITW, la autorización de un certificado emitido por un PSC, no implicará la desautorización de los certificados vigentes<sup>4</sup>.

#### **4.3.6 Desautorización de certificados a un proceso informático**

Consistirá en el envío de una carta firmada por el solicitante en su día de alta en el proceso (o persona que lo sustituya) que contenga los datos del certificado a desautorizar para el intercambio de información con el Banco de España.

La desautorización de todos los certificados autorizados a un proceso de información (uno en el caso de que se utilicen certificados de componente emitidos por Banco de España) implicará el cese de intercambio de información entre el Banco de España y la entidad a través de dicho proceso.

---

<sup>1</sup> Ver el anejo 3 sobre gestión de certificados emitidos por el Banco de España.

<sup>2</sup> Es muy importante no enviar el certificado en formato .pfx o .p12 ya que, en este caso, se estaría también facilitando una copia de la clave privada asociada, con el correspondiente riesgo para su seguridad

<sup>3</sup> Si se desea autorizar certificados emitidos por un PSC a un sistema de información cuyo certificado anterior hubiera sido emitido por el Banco de España, será necesario enviar una desautorización explícita de este último certificado.

<sup>4</sup> Si se desea autorizar certificados emitidos por un PSC a un sistema de información cuyo certificado anterior hubiera sido emitido por el Banco de España, será necesario enviar una desautorización explícita de este último certificado.

## 5 Procedimiento de alta de una entidad en un proceso

### 5.1 Cuestiones generales

La adscripción de una entidad a un proceso que implique el intercambio telemático de archivos con el Banco de España se realizará **enviando una carta firmada al Banco de España según el Anejo 1 (incluyendo los datos que se especifican en los apartados 6.1 y 6.2)**, en la que se especificará necesariamente los datos generales de la entidad y el proceso al que la entidad desea adherirse; así como la vía de comunicación elegida y el mecanismo de seguridad que se va a utilizar.

La carta deberá ser firmada de forma autógrafa por una persona reconocida por el departamento destinatario de la información que se desea transmitir.

Esta carta podrá ser sustituida por el envío de un correo electrónico firmado utilizando un certificado de persona jurídica emitido para la entidad por un Prestador de Servicios de Certificación admitido por el Banco de España<sup>1</sup>.

Una vez recibida la carta en el Banco de España y aprobada la adhesión por el Departamento competente, el Departamento de Sistemas de Información realizará las configuraciones necesarias para recibir/enviar los ficheros de la entidad según los mecanismos elegidos por ella (siempre de acuerdo con los procedimientos admitidos en cada proceso).

Por su parte, la entidad deberá también realizar las configuraciones requeridas para poder habilitar la recepción y envío de información por los medios telemáticos especificados en la carta.

Una vez terminadas las configuraciones necesarias en el Banco de España el remitente de la carta (o la persona especificada como contacto técnico) recibirá un correo electrónico informándole de la disponibilidad de la vía para el intercambio de los archivos para el proceso solicitado.

### 5.2 Datos fijos que se deberán incluir en la carta de solicitud de alta

Constituyen los datos de la entidad, la persona responsable de la información en la entidad y el proceso al que se quieren adherir. Como contacto técnico conviene indicar el nombre, teléfono y dirección de correo de algún miembro de la entidad que pueda resolver las posibles incidencias de comunicación que surjan durante las transmisiones.

### 5.3 Datos variables

Se especificará necesariamente la vía de comunicación elegida de entre las disponibles para el proceso, y los procedimientos de seguridad que se van a aplicar para dicha vía. Ver el apartado 6.2 para saber qué es necesario aportar en cada caso.

---

<sup>1</sup> Consultar la dirección <http://pki.bde.es/pscs>

## 6 **Anejo 1. Modelo de carta para solicitar el alta de comunicaciones al Banco de España**

Se debe enviar una carta siguiendo el siguiente modelo, y añadiendo los datos variables que proceda, a la siguiente dirección postal:

Banco de España  
Sistemas de Información  
Servicio de Gestión de Clientes BdE  
Apartado de Correos 15  
28080 Madrid

La carta también puede ser presentada directamente en el Registro General del Banco de España, sito en el edificio de Alcalá 48.

Esta carta podrá asimismo ser sustituida por un mensaje de correo electrónico firmado electrónicamente, utilizando un certificado de persona jurídica emitido para la entidad por un Prestador de Servicios de Certificación reconocido por el Banco de España<sup>1</sup>. La dirección a la que se ha de enviar es la siguiente:

[gestionclientesbde@bde.es](mailto:gestionclientesbde@bde.es)

---

<sup>1</sup> Consultar la dirección <http://pki.bde.es/pscs>

## 6.1 Datos fijos

*“Muy Sres. nuestros:*

*Por la presente les comunicamos nuestros datos para el intercambio de archivos con Vds., respecto al siguiente proceso informático del Banco de España:*

- **Identificación proceso:** P P P P P P (este dato figurará en el Manual de Uso específico de cada proceso, según los datos que se deseen intercambiar)
- **Nombre de la entidad:** Nombre de mi organización S.A.
- **Código de la entidad:** n n n n (p. ej. 0135)
- **CIF de nuestra entidad:** Gxx/nnnnnnnnnnn

- **Persona de contacto técnico de nuestra entidad:** (persona con la que se contactará en caso de problemas durante la transmisión de información)

Nombre y apellidos:

Teléfono:

email:

- **Persona de contacto funcional de nuestra entidad:** (persona con la que se contactará en caso de incidencias de tipo funcional)

Nombre y apellidos:

Teléfono:

email:

**Mecanismo de comunicación y cifrado elegido:** En este apartado, se debe especificar claramente los mecanismos de comunicación y seguridad que se van a emplear. (Los datos que necesariamente se han de incluir según la vía elegida figuran en el **apartado 6.2 – datos variables**)

Atentamente,

Nombre, Cargo y Firma del solicitante<sup>1</sup>”

---

<sup>1</sup> Esta firma podrá ser manuscrita, en caso de comunicación a través de correo postal o, electrónica, en caso de comunicación a través de correo electrónico.

## 6.2 Datos variables:

A continuación se especifican las distintas posibilidades según la vía de comunicación elegida.

### 6.2.1 Para envíos al Banco de España mediante ITW

#### Red de acceso:

Especificar la opción elegida de entre las tres siguientes y ver además siguientes apartados

RedBdE/Intranet Administrativa/Internet

**Certificados:** especificar según el caso los que se van a utilizar para ITW:<sup>1</sup>

#### 6.2.1.1 Para la solicitud de alta de entidad o autorización de certificados a un proceso:

Dependiendo del emisor del certificado que se desee utilizar, deberá especificarse:

- *Certificados emitidos por un PSC*<sup>2</sup>

**DN\_:** \_\_\_\_\_

**DN\_:** \_\_\_\_\_

**DN\_:** \_\_\_\_\_

(Ej.: CN=ENTIDAD MI ENTIDAD – CIF Q00000000 – NOMBRE ESPAÑOL ESPAÑOL JUAN – NIF 00000000T,  
OU = 1234567890, OU = FNMT Clase 2 CA, O = FNMT, C = ES)

- *Certificados de componente emitidos por el BdE*<sup>3</sup>

**DN\_:** \_\_\_\_\_

(Ej.: CN=[EG] Q00000000 RI-C36 0001,OU=COMPONENTES,OU=MI ENTIDAD, C=ES)

- *Caso de solicitar la generación de un nuevo certificado de componente del BdE4*  
“Se adjunta solicitud de emisión de certificado”.

**Número de petición:** \_\_\_\_\_” (Ej.: 1234567890)

#### 6.2.1.2 Para la desautorización de certificados a un proceso ya existente

Certificados a desautorizar

DN (1): \_\_\_\_\_

DN (2): \_\_\_\_\_

DN (3): \_\_\_\_\_

<sup>1</sup> Seleccionar la opción que proceda.

<sup>2</sup> Dado que los certificados emitidos por un PSC están asignados a una persona física concreta, se admitirán varios certificados de este tipo para cada proceso.

<sup>3</sup> En el caso de utilizar certificados de componente emitidos por el Banco de España sólo se admitirá un certificado por proceso.

<sup>4</sup> Adjuntar el formulario de solicitud obtenido en la aplicación de obtención de certificados, cuyo acceso se puede encontrar en la dirección <http://pki.bde.es/oci>. El número de petición se obtendrá automáticamente al rellenar la solicitud en la aplicación de obtención de certificados.

## 6.2.2 Para comunicaciones mediante correo electrónico Internet firmado y cifrado mediante certificados electrónicos:

### 6.2.2.1 Solicitud de alta de entidad o autorización de certificados a un proceso:

Indicar siempre la dirección de correo electrónico Internet a utilizar y los certificados a emplear:

- Caso de certificados emitidos por un PSC <sup>1</sup>

Nombre del fichero\_: \_\_\_\_\_

Nombre del fichero\_: \_\_\_\_\_

Nombre del fichero\_: \_\_\_\_\_

En este caso se deberá incluir en la carta el fichero en soporte magnético, y el nombre de dicho fichero debe coincidir con el especificado en la carta.

- Caso de certificados de componente emitidos por el BdE <sup>2</sup>

DN\_: \_\_\_\_\_

(Ej.: CN=[EG] Q00000000 RI-C36 0001, OU=COMPONENTES, OU=MI ENTIDAD, C=ES)

- Caso de solicitar la generación de un nuevo certificado de componente del BdE<sup>3</sup>

Se adjunta solicitud de emisión de certificado. Número de petición: \_\_\_\_\_

(Ej.: 1234567890)

### 6.2.2.2 Desautorización de certificados a un proceso ya existente:

Certificados a desautorizar

DN (1): \_\_\_\_\_

DN (2): \_\_\_\_\_

DN (3): \_\_\_\_\_

NOTA: Es habitual que la aplicación cliente de correo electrónico requiera que el certificado a utilizar para la firma contenga la dirección de correo del buzón desde el que se envían los mensajes. De lo contrario, dicha aplicación podría no permitir efectuar la firma. El Banco de España no puede ofrecer soporte técnico en este sentido a las entidades usuarias, por lo que se deberá consultar la documentación de la aplicación de correo electrónico en cuestión para conocer las peculiaridades de la misma al respecto del uso de certificados;

---

<sup>1</sup> Los archivos se adjuntarán en formato ".cer" o ".crt". Dado que los certificados emitidos por un PSC están asignados a una persona física concreta, se admitirán varios certificados de este tipo para cada proceso.

<sup>2</sup> En el caso de utilizar certificados de componente emitidos por el Banco de España sólo se admitirá un certificado por proceso.

<sup>3</sup> Adjuntar el formulario de solicitud obtenido en la aplicación de obtención de certificados, cuyo acceso se puede encontrar en la dirección <http://pki.bde.es/oci>. El número de petición se obtendrá automáticamente al rellenar la solicitud en la aplicación de obtención de certificados.

### **6.2.3 Para comunicaciones mediante Editran utilizando la criptografía del SNCE o el cifrado de clave pública de Indra**

**- Parámetros de Editran:**

ASCII-EBCDIC (A/E):	X
versión Editran/P:	X.X
versión Editran/G:	X.X
versión de cifrado:	X.X

**- Red de acceso:**

RedBdE/ Intranet Administrativa/ SNCE (Especificar la opción elegida)

### **6.2.4 Para comunicaciones mediante FileAct**

**Datos a adjuntar en el alta del proceso**

- **DN** utilizado para el envío o recepción de ficheros vía FileAct:

Ej.: cn=eca,o=yourbic8,o=swift

Donde “yourbic8” es el BIC de la entidad.

- **Compresión:** SI/NO (especificar)

Ver además apartado 9 – ([Anejo 4](#) – especificaciones técnicas para el uso de FileAct)

## 7 **Anejo 2. Formato de los archivos de datos**

Salvo que en el correspondiente Manual de Uso del Banco de España se indique otra cosa, los archivos de datos en el Banco de España, antes de ser enviados, o una vez recibidos y descifrados (en su caso), tendrán las siguientes características generales:

### 7.1 **Correo electrónico internet e ITW**

- Archivo de texto;
- Código ASCII extendido, (página de códigos 850, MS-DOS Multilingual) o ISO 8859-1 (página de códigos 1200, Unicode Latin-1). A elección de la entidad por cada proceso del Banco de España, aunque, en determinados casos, puede que el correspondiente Manual de Uso del sistema de información del Banco de España lo determine unívocamente;
- Cada registro finalizará con el valor "LF" (código hexadecimal "0A");
- En cada registro se puede omitir el conjunto de caracteres a espacios (en código hexadecimal "20") inmediatamente antes del valor "LF" de fin de registro;
- El último registro, además del carácter "LF", podrá llevar de forma opcional, marca de fin de archivo físico "EOF" (código hexadecimal "1A");
- Caracteres admitidos: únicamente el juego normal de caracteres.

### 7.2 **Editran (Cifrado SNCE y cifrado de clave pública de Indra)**

- Archivo de texto;
- Código EBCDIC;
- Caracteres admitidos: únicamente el juego normal de caracteres.

### 7.3 **Juego normal de caracteres**

A continuación se detalla el conjunto de caracteres que componen el juego normal de caracteres, de uso general y que pueden encontrarse en los archivos de datos (texto) en el Banco de España después de ser recibidos y descifrados (en su caso) o antes de ser enviados en su intercambio con las entidades.

Carácter	Código EBCDIC	Código ASCII (pag. 850)	Código ISO 8859-1 (pag.1200)
A	C1	41	41
B	C2	42	42
C	C3	43	43
D	C4	44	44
E	C5	45	45
F	C6	46	46
G	C7	47	47
H	C8	48	48
I	C9	49	49
J	D1	4A	4A
K	D2	4B	4B
L	D3	4C	4C

M	D4	4D	4D
N	D5	4E	4E
Ñ(EÑE mayúscula)	7B	A5	D1
O	D6	4F	4F
P	D7	50	50
Q	D8	51	51
R	D9	52	52
S	E2	53	53
T	E3	54	54
U	E4	55	55
V	E5	56	56
W	E6	57	57
X	E7	58	58
Y	E8	59	59
Z	E9	5A	5A
a	81	61	61
b	82	62	62
c	83	63	63
d	84	64	64
e	85	65	65
f	86	66	66
g	87	67	67
h	88	68	68
i	89	69	69
j	91	6A	6A
k	92	6B	6B
l	93	6C	6C
m	94	6D	6D
n	95	6E	6E
ñ(eñe minúscula)	6A	A4	F1
o	96	6F	6F
p	97	70	70
q	98	71	71
r	99	72	72
s	A2	73	73
t	A3	74	74
u	A4	75	75
v	A5	76	76
w	A6	77	77
x	A7	78	78
y	A8	79	79
z	A9	7A	7A
espacio	40	20	20
0	F0	30	30
1	F1	31	31
2	F2	32	32
3	F3	33	33
4	F4	34	34

5		F5	35	35
6		F6	36	36
7		F7	37	37
8		F8	38	38
9		F9	39	39
*	(asterisco)	5C	2A	2A
\$	(dólar)	5B	24	24
&	(ampersand)	50	26	26
%	(tanto por ciento)	6C	25	25
@	(arroba)	7C	40	40
<	(menor)	4C	3C	3C
>	(mayor)	6E	3E	3E
"	(doble comilla)	7F	22	22
-	(guión)	60	2D	2D
?	(interrogación)	6F	3F	3F
:	(dos puntos)	7A	3A	3A
(	(paréntesis izdo.)		4D	28
)	(paréntesis dcho.)	5D	29	29
.	(punto)	4B	2E	2E
,	(coma)	6B	2C	2C
=	(igual)	7E	3D	3D
/	(barra)	61	2F	2F
+	(más)	4E	2B	2B
'	(comilla)	7D	27	27
FF	(salto de página)		0C	0C
CR	(retorno de carro)		0D	0D
LF	(nueva línea)		0A	0A
EOF	(fin de fichero)		1A	1A

El Banco de España observará este conjunto de caracteres en el envío de archivos de datos a las entidades. En sentido contrario, la existencia de caracteres distintos de los anteriormente detallados puede dar lugar a errores en el procesamiento de los archivos recibidos en el Banco de España, y por lo tanto a su rechazo.

## 8 **Anejo 3. Procedimientos de gestión de certificados**

### 8.1 **Solicitud de certificados al Banco de España**

Dado que, en determinados casos, puede no resultar conveniente para una entidad utilizar certificados de persona física o de persona jurídica emitidos por un Prestador de Servicios de Certificación en los procesos de envío/recepción telemática de archivos, el Banco de España ofrece la posibilidad de que la PKI del Banco de España emita certificados de componente informático para entidades externas<sup>1</sup>. Estos certificados podrán ser utilizados por las entidades en sus relaciones con Banco de España para la autenticación y el cifrado de comunicaciones.

Dadas sus características (estos certificados no contienen datos personales, sino que incluyen únicamente información de identificación de la entidad y la dirección de correo electrónico desde la que se van a realizar los envíos), son susceptibles de ser reutilizados por diferentes personas y/o sistemas de información dentro de la entidad.

La solicitud de la emisión de un certificado digital al Banco de España se realizará utilizando la aplicación de obtención de certificados por Internet, accesible a través de la página <http://pki.bde.es/oci>. En dicha página se ofrecen dos alternativas:

#### **Opción 1.** *Solicitud de certificado accediendo de forma anónima*

El formulario de solicitud del certificado será firmado de forma manuscrita por la misma persona que va a solicitar el alta de la entidad en el proceso informático o la autorización del certificado a un proceso ya existente (ver el apartado 4.3.5). Por tanto, sólo se admitirán solicitudes firmadas por una persona que ya figure en el Banco de España como representante de la entidad para la que se solicita el certificado. La solicitud de un certificado utilizando esta opción sólo será posible si el proceso para el que se va a utilizar el certificado lo admite.

Los pasos a seguir, guiados por la aplicación informática, son los siguientes:

- Acceder a la aplicación pulsando el enlace disponible;
- Descargar e instalar los certificados de la jerarquía de certificación del Banco de España, es decir, la Autoridad de Certificación raíz y la Autoridad de Certificación Corporativa (este paso sólo ha de realizarse la primera vez por cada ordenador en el que se vaya a utilizar el certificado);
- Rellenar un formulario electrónico con la información necesaria para la emisión del certificado. Al enviar dicha información, se obtendrá un número de petición y un documento electrónico en formato PDF que se habrá de imprimir y firmar de forma manuscrita por la misma persona que vaya a firmar la solicitud de alta de la entidad en el proceso informático;
- Incluir el número de petición obtenido en la carta de solicitud de alta de la entidad en el proceso informático (o de autorización del certificado a un proceso ya existente), y enviar por correo postal ambos formularios en papel (el de solicitud de alta y el de solicitud de certificado) a la dirección indicada en el anejo 2;
- Una vez recibido el formulario de solicitud del certificado, el Banco de España procederá a su aprobación (o rechazo, en caso de que la solicitud contenga alguna información incorrecta);

---

<sup>1</sup> Para más información, consultar la Política de Certificación de este tipo de certificados en la página <http://pki.bde.es/politicas>

- El solicitante recibirá un mensaje de correo electrónico en el que se indicará que se ha aprobado o rechazado la solicitud. Si en el plazo de unos 30 días desde el envío el formulario por correo postal no se ha recibido dicho mensaje, se habrá de acceder a la aplicación (según se describe en el apartado siguiente) para comprobar si la solicitud ya ha sido aprobada o rechazada y simplemente el mensaje no ha llegado, o bien si aún está pendiente de gestionar, en cuyo caso se podrá contactar con el Banco de España, a través de los datos de contacto indicados en el apartado 10, para confirmar su estado;
- Acceder a la aplicación e identificarse utilizando el número de identificación fiscal de la entidad (CIF) y el número de petición. Se podrá visualizar el estado de la solicitud y, en el caso de que haya sido aprobada, se podrá proceder a generar una pareja de claves RSA (pública y privada) y se enviará la pública automáticamente al Banco de España;
- En el Banco de España se recibirá la clave pública y, transcurrido un tiempo breve (unos minutos o, a lo sumo, unas horas) se emitirá el certificado. En ese momento se enviará un mensaje de correo electrónico a la entidad informando de que ya puede descargarlo. Si transcurridas unas 24 horas desde la generación de las claves no se hubiera recibido el mensaje, se podrá entrar de nuevo en la aplicación para comprobar el estado de la solicitud, por si el mensaje se hubiera perdido;
- Descargar e instalar el certificado en el navegador;
- Realizar una copia de seguridad del certificado y claves.

**Opción 2.** *Solicitud de certificado utilizando un certificado de persona jurídica emitido por un Prestador de Servicios de Certificación aceptado por el Banco de España*

Se ofrece esta posibilidad para solventar aquellas situaciones en las que la entidad ya dispone de un certificado emitido por un PSC pero que su utilización no es conveniente en la comunicación con el Banco de España. Algunos ejemplos de esta situación podrían ser: la persona física responsable del certificado es distinta de la que va a comunicarse con el Banco de España y no se desea solicitar un nuevo certificado al PSC para dicha persona; el certificado no contiene la dirección de correo electrónico desde la que se va a realizar el envío de la información y no se desea acudir al PSC a obtener uno nuevo; el proceso informático al que se va a enviar la información no tiene contemplados los certificados de ese PSC, etc.

También se puede utilizar esta alternativa para proceder a la renovación de un certificado de componente para entidades externas emitido por el Banco de España y que está a punto de caducar.

Los pasos a seguir, guiados por la aplicación informática, son los siguientes:

- Identificarse en la aplicación utilizando el certificado del PSC;
- Descargar e instalar los certificados de la jerarquía de certificación del Banco de España, es decir, la Autoridad de Certificación raíz y la Autoridad de Certificación Corporativa (este paso sólo ha de realizarse la primera vez por cada ordenador en el que se vaya a utilizar el certificado);
- Realizar la solicitud del certificado, la cual comprende de los siguientes puntos:
  - Rellenar un formulario electrónico con la información necesaria para la emisión del certificado del Banco de España;
  - Generar en el navegador de Internet una pareja de claves RSA (una pública y una privada) y enviar la pública al Banco;

- Firmar electrónicamente la solicitud utilizando el certificado de persona jurídica del PSC.
- En el BdE se procesará automáticamente la solicitud y, transcurrido un tiempo breve (unos minutos o, a lo sumo, unas horas) se emitirá el certificado. En ese momento se enviará un mensaje de correo electrónico a la entidad informando de que ya puede descargarlo. Si transcurridas unas 24 horas desde la generación de las claves y firma de la solicitud no se hubiera recibido el mensaje, se podrá acceder de nuevo a la aplicación para comprobar el estado de la solicitud, por si el mensaje se hubiera perdido;
- Descargar e instalar el certificado en el navegador;
- Realizar una copia de seguridad del certificado y claves.

Nota: si se utiliza esta segunda alternativa, la solicitud de alta de la entidad en un proceso informático o de autorización de certificado a un proceso (ver apartados 4.3.4 y 4.3.5), se habrá de realizar posteriormente a la obtención del certificado y habrá que incluir en ella el nombre distintivo del certificado obtenido.

## 8.2 Renovación de certificados emitidos por el Banco de España

Cuando un certificado se encuentre próximo a su fecha de expiración, la entidad deberá proceder a su renovación.

Para renovar un certificado emitido por el Banco de España, el solicitante deberá tener instalado en el navegador el certificado que está a punto de caducar<sup>1</sup>. A continuación, deberá acceder a la página <http://pki.bde.es/oci>, pulsar en el enlace de “acceso autenticado en base a un certificado” y elegir el certificado a renovar para identificarse. La aplicación mostrará la lista de certificados de componente informático emitidos por el Banco de España para la entidad. Se deberá elegir el certificado a punto de caducar y pulsar el botón de renovación. Los pasos siguientes son semejantes a los descritos en el apartado anterior para el caso de acceso con certificado.

Para mayor información, consultar el manual de la aplicación de obtención de certificados por Internet que se puede encontrar en la página indicada anteriormente.

**Importante:** tal como se indica en el apartado 4.3.5, si la vía de comunicación para el envío de ficheros al BdE es correo electrónico Internet, una vez realizada la renovación del certificado se habrá de comunicar al Banco de España que se desea que el nuevo certificado sea autorizado al proceso informático al que se accedía con el antiguo.

## 8.3 Revocación de certificados emitidos por el Banco de España

Si la entidad entiende que un certificado emitido para ella por el Banco de España y que está utilizando en algún proceso informático ha dejado de ser confiable, deberá proceder a su revocación. Para ello, se presentan dos alternativas:

### 1 Caso en que aún se disponga del certificado a revocar

En este caso, se podrá acceder a la aplicación de obtención de certificados utilizando el certificado a revocar como mecanismo de autenticación. El enlace a dicha aplicación se encuentra en la página <http://pki.bde.es/oci>. La aplicación mostrará la lista de certificados de componente

<sup>1</sup> Si el certificado ya estuviera caducado, la entidad deberá solicitar un nuevo certificado como si se tratara de la primera vez.

informáticos emitidos por el Banco de España para la entidad. Se deberá seleccionar el certificado a revocar y pulsar el botón de revocación.

Para mayor información, consultar el manual de la aplicación de obtención de certificados por Internet que se puede encontrar en la página indicada anteriormente.

## **2 Caso en que no se disponga del certificado a revocar**

En estas situaciones, deberá obtenerse el formulario de solicitud de revocación de certificado ubicado en la página <http://pki.bde.es/oci>. Para hacerlo llegar al Banco de España, existen dos posibilidades:

- Si acompaña a la solicitud de un nuevo certificado descrita en el apartado 8.1 opción 1, imprimir el formulario de revocación, firmarlo de forma manual por la misma persona que solicita el nuevo certificado, y enviarlo por correo postal a la dirección indicada en el anejo 1;
- Si no acompaña a la solicitud de un nuevo certificado, enviar el formulario de revocación por correo electrónico firmado a la dirección de correo electrónico indicada al final de este documento. El certificado utilizado para firmar podrá ser cualquier certificado de persona jurídica emitido para la entidad por un PSC admitido por el Banco de España.

## **8.4 Renovación del certificado de cifrado del Banco de España**

Este procedimiento sólo se aplica a la vía de comunicación basada en correo electrónico Internet.

Cuando el certificado cuyo titular es el del Banco de España (asociado a la dirección [correo@procesos.bde.es](mailto:correo@procesos.bde.es)) esté a punto de caducar, será renovado y publicado en la dirección de Internet <http://pki.bde.es>. A partir de ese momento se recomienda a las entidades que actualicen dicho certificado en la libreta de direcciones de su aplicación cliente de correo electrónico y lo utilicen para el intercambio de información con el Banco de España, aunque podrán seguir utilizando el anterior hasta que caduque.

## **8.5 Revocación de certificados emitidos por un PSC**

La solicitud de revocación de este tipo de certificados deberá realizarse acorde al procedimiento que establezca el PSC elegido, por lo que el Banco de España quedará al margen de esta gestión.

En cualquier caso, aunque el certificado una vez revocado sería rechazado por el Banco de España, se deberá notificar la desautorización de dicho certificado a todos los sistemas de información a los que tuviera acceso, tal como se describe en el apartado 4.3.6.

## 8.6 Glosario de términos para certificados digitales

### 8.6.1 Definiciones

**Certificado digital:** un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad.

**Clave pública y clave privada:** la criptografía asimétrica en la que se basa la PKI emplea un par de claves en la que lo que se cifra con una de ellas sólo se puede descifrar con la otra y viceversa. A una de esas claves se la denomina pública y se la incluye en el certificado digital, mientras que a la otra se la denomina privada y únicamente es conocida por el titular del certificado y, si procede, por el Archivo de Claves.

**Jerarquía de confianza:** Conjunto de autoridades de certificación que mantienen relaciones de confianza por las cuales una AC de nivel superior garantiza la confiabilidad de una o varias de nivel inferior. En el caso de la PKI del Banco de España, la jerarquía tiene dos niveles, la AC Raíz en el nivel superior garantiza la confianza de sus AC subordinadas.

**Prestador de Servicios de Certificación:** persona física o jurídica que expide certificados digitales o presta otros servicios en relación con la firma electrónica.

**Titular:** persona o componente informático para el que se expide un certificado digital y es aceptado por éste o por su solicitante en el caso de los certificados de componente o por el representante en el supuesto de persona jurídica.

### 8.6.2 Acrónimos

**AC:** Autoridad de Certificación.

**DN:** Distinguished Name (Nombre Distintivo). Identificación unívoca de una entrada dentro de la estructura de directorio X.500. El DN de un certificado contiene información sobre la identidad del titular del certificado.

**DPC:** Declaración de Prácticas de Certificación.

**PC:** Política de Certificación.

**PKI:** Public Key Infrastructure (Infraestructura de Clave Pública).

**PSC:** Prestador de servicios de certificación.

## 9 Anejo 4: Características técnicas para la transmisión de ficheros vía FileAct

### 9.1 Consideraciones previas

Para transmitir ficheros vía FileAct deberán pedir la adhesión a los servicios siguientes:

#### NOMBRES DE SERVICIO FILEACT SEGÚN ENTORNOS DEL BANCO DE ESPAÑA

Entorno	Nombre del servicio ( <i>Service Name</i> )
Preproducción	bde. eca. sf!p
Producción	bde. eca. sf

Nota: El DN que adquiera las colas tiene que tener el rol RBAC de SnF Requestor para poder recoger los ficheros de las colas SWIFT.

#### 9.1.1 Especificaciones para realizar el e-ordering

##### SWIFTNet Closed User Group Information

- CUG category: member1

##### Traffic Routing for Store and Forward Service

- Es necesario añadir una regla el Responder DN = “\*,o=bic8,o=swift”

#### 9.1.2 Parametrización para envío

Parámetro	Contenido	Observaciones
<i>Requestor DN</i>	Deberá ser el DN definido en los datos a adjuntar en el alta del proceso: Ej.: cn=eca,o=yourbic8,o=swift.	Donde “yourbic8” será el BIC de la entidad que envía el fichero .
<i>Responder DN</i>	Deberá ser obligatoriamente: cn=eca,o=espbesmm,o=swift	
<i>Service Name</i>	bde.eca.sf!p o bde.eca.sf	En función del entorno al que se acceda.
<i>Request Type</i>	pacs.xxx.genfasf01	Literalmente
<i>User Reference</i>	Referencia del fichero para el remitente	
<i>File Location</i>	Ruta del fichero en el sistema del remitente	
<i>File Name</i>	Nombre del fichero que va a enviar el remitente (el solicitante), que no debe contener ni blancos ni caracteres especiales (#,_,*,& ...).	
<i>File Description</i>	Obligatoriamente PPPPPP.	Donde PPPPP es el nombre del proceso según identificación del banco de España.

<i>File Info</i>	Información adicional sobre el fichero a enviar.	Se considera válidos los siguientes valores: SwCompression = ZIP SwCompression = Gzip, o SwCompression = None.
<i>Signed</i>	Deberá obligatoriamente estar marcado	
<i>Store-And-Forward</i>	Deberá obligatoriamente estar marcado	
<i>Delivery Notification Queue</i>	La que se defina en el e-ordering	

### 9.1.3 Parametrización recepción

<b>Parámetro</b>	<b>Contenido</b>	<b>Observaciones</b>
<i>Requestor DN</i>	cn=eca,o=espbesmm,o=swift	
<i>Responder DN</i>	Deberá ser la definida en los datos a adjuntar en el alta del proceso: Ej.: cn=eca,o=yourbic8,o=swift.	Donde "yourbic8" es el BIC de la entidad receptora del fichero.
<i>Service Name</i>	bde.eca.sf!p o bde.eca.sf	En función del entorno al que se acceda.
<i>Request Type</i>	pacs.xxx.genfasf01	Literalmente
<i>User Reference</i>	Referencia del fichero en Banco de España	
<i>File Description</i>	PPPPPP.	Donde PPPPP es el nombre de la identificación del Banco de España.
<i>File Info</i>	Información adicional sobre el fichero a enviar.	SwCompression = Gzip o SwCompression = None dependiendo de si se ha solicitado compresión en los datos a adjuntar.

### 9.1.4 Pruebas de conectividad

Una vez autorizada la pertenencia a dichos grupos por parte de los administradores del Banco de España la entidad deberá realizar en los dos servicios citados las siguientes pruebas básicas de envío y recepción de ficheros:

#### Prueba de recepción de un fichero comprimido

En esta prueba se realizará el envío desde el Banco de España de un fichero comprimido de 5 Kb. El formato será típico de los envíos que realice el Banco de España.

File Description = ITAPR1  
SwCompression = Gzip.

Esta prueba garantizará que los siguientes elementos están en funcionamiento:

- La configuración para poder recibir ficheros mediante FileAct SnF enviados por el Banco de España.
- El solicitante tiene correctamente configurados los parámetros del CUG de SWIFT asociado al servicio FileAct SnF del Banco de España.
- El encaminamiento a través de los sistemas de SWIFT funciona sin problemas.
- Las colas de recepción están correctamente definidas en el solicitante.
- Los parámetros específicos definidos por el Banco de España para este tipo de envíos son tratados correctamente.
- La capacidad de recibir ficheros comprimidos

#### Prueba de envío de un fichero comprimido

En esta prueba se realizará el envío desde la entidad al Banco de España de un fichero comprimido de 5 Kb. El formato será típico de los envíos que realice el Banco de España.

File Description = ITAPR2  
SwCompression = Gzip o Zip o None

La prueba garantizará que los siguientes elementos están en funcionamiento:

- La configuración para poder enviar ficheros mediante FileAct SnF al Banco de España.
- El solicitante tiene correctamente configurados los parámetros del CUG de SWIFT asociado al servicio FileAct SnF de ECA.
- El encaminamiento a través de los sistemas de SWIFT funciona sin problemas.
- Los parámetros específicos definidos por el Banco de España para este tipo de envíos son tratados correctamente.
- Los ficheros deben ir firmados (casilla Signed marcada).
- La capacidad de enviar ficheros comprimidos.

## **10 Datos de contacto**

Para cualquier aclaración sobre el contenido de este documento pueden llamar al tfno. 91.338.67.34 o enviar un correo a la dirección [itaadmin@bde.es](mailto:itaadmin@bde.es).

Para resolver cualquier incidencia durante las transmisiones deberán contactar con el Centro de Ayuda al Usuario, en el teléfono 91.338.66.66.