

BANCO DE ESPAÑA

Dirección General de Supervisión.
Planificación de Supervisión
Grupo de Innovación Tecnológica

Mayo 2008

Instrucciones para la solicitud, descarga e instalación de un certificado de componente informático para el intercambio de correo electrónico seguro con los distintos grupos de inspección del Banco de España

1 Introducción

El Banco de España, como Prestador de Servicios de Certificación, puede emitir certificados electrónicos para las entidades con las que intercambia información de forma telemática.

Además de los certificados de firma y cifrado asociados a personas físicas o jurídicas y sujetos a la ley de firma, el Banco ha desarrollado otra modalidad de certificados que se denominan **certificados de componente informático para entidades externas**.

Estos certificados, que permiten tanto la firma como el cifrado, están pensados para ser utilizados no por una sola persona, sino por un grupo de trabajo y son, por ello un medio muy adecuado para facilitar una comunicación más segura entre las distintas entidades supervisadas y la Dirección General de Supervisión, a través del correo electrónico.

El presente documento describe el procedimiento de solicitud, descarga e instalación del certificado digital requerido para el intercambio de correo electrónico seguro con los distintos grupos de inspección del Banco de España, a través de la aplicación OCI .

2 Solicitud y descarga

Las solicitudes de certificados se tramitarán mediante la aplicación OCI, tal y como se detalla a continuación:

2.1 Solicitud y descarga de certificados PKIBDE para las entidades

La solicitud y descarga de los certificados se realiza mediante una aplicación informática accesible desde el sitio web del Banco de España (www.bde.es) seleccionando, en ese sitio web, la opción >Servicios al público>Certificados y firma electrónica>Solicitud de certificados a PKIBDE.

Existen dos modalidades de acceso a la aplicación y ambas producen resultados totalmente equivalentes. La primera, denominada acceso anónimo o sin autenticación, no requiere que el usuario disponga de un certificado de persona jurídica emitido por un Prestador de Servicios de Certificación (PSC) aceptado por el Banco de España mientras que la segunda si lo precisa.

2.1.1 Acceso sin autenticación

Se accederá a la aplicación informática, denominada OCI, en modo anónimo, entrando en la web del Banco de España www.bde.es, y seleccionando >Servicios al público>Certificados y firma electrónica>Solicitud de certificados a PKIBDE y, a continuación, el enlace **Acceder a la aplicación sin autenticación**.

La aplicación muestra los seis pasos a seguir para la obtención de un certificado de entidad externa del Banco de España:

2.1.1.1 Paso 1 de 6: Instalación de los certificados de las Autoridades de Certificación de la PKI del Banco de España.

Se instalan el certificado de la autoridad de certificación raíz (ACraiz.crt) y el de la autoridad de certificación corporativa (ACcorporativa.crt).

2.1.1.2 Paso 2 de 6: Solicitud electrónica del certificado.

Deberán cumplimentarse los datos siguientes

- Datos de la empresa solicitante:

Número de identificación fiscal (CIF) de la entidad (*).

Nombre de la entidad (*).

E-mail(*). Dirección desde la que se utilizará el certificado para el envío y recepción de mensajes de correo electrónico firmado y cifrado.

- Datos del responsable del certificado (firmará manuscritamente el formulario generado):

Nombre y apellidos (*).

Cargo.

Teléfono (*).

E-mail.

Tipo y Nº de documento identificativo.

- Datos del contacto técnico (por si es necesario contactar durante el proceso de generación del certificado):

Teléfono.

E-mail.

Los mensajes de correo electrónico relacionados con el ciclo de vida del certificado serán enviados a las direcciones de correo electrónico del responsable y del contacto técnico.

Una vez cumplimentada, pulsar la opción "Solicitar Certificado". Se validará automáticamente el formato de los datos y la cumplimentación de los campos obligatorios (los marcados con *).

Si la validación es satisfactoria, la solicitud quedará almacenada en el sistema OCI y se mostrará un identificador único de solicitud. También se presentará la opción de generar un documento PDF con todos los datos de la solicitud, incluido el identificador. Tanto el PDF como el identificador se deberán guardar para utilizarlos en los pasos siguientes del proceso. La solicitud cambiará al estado "Pendiente de Aprobación".

2.1.1.3 Paso 3 de 6: Generación y envío del formulario de solicitud al Banco de España por correo postal.

El documento PDF generado en el paso anterior se imprimirá en una impresora de doble cara y se firmará, en el apartado “Firma del solicitante” dentro de la sección Aceptación de condiciones, por el responsable del certificado ante el BdE. En el caso de no disponer de una impresora de doble cara, se imprimirá en otra impresora y se firmarán todas las hojas.

El documento consta de dos copias, pero sólo se enviará el “Ejemplar para enviar al Banco de España” por correo postal a la dirección:

BANCO DE ESPAÑA
Planificación de Supervisión
Grupo de Innovación Tecnológica
c/ Alcalá, 522
28027 Madrid

El BdE recibirá, por un lado, la solicitud firmada vía correo postal y, por otro, el formulario electrónico de la solicitud vía sistema OCI. Se cotejarán los datos recibidos por ambos sistemas y se procederá a su aprobación o rechazo vía OCI.

En caso de aprobación, la solicitud cambiará al estado “Aprobada” y se enviará una notificación por correo electrónico al responsable del certificado. Se podrá continuar con el paso siguiente.

En caso de rechazo, la solicitud cambiará al estado “Rechazada” y se enviará una notificación por correo electrónico al responsable del certificado, indicando la causa del rechazo y los pasos a seguir.

2.1.1.4 Paso 4 de 6: Generación de las claves asociadas a la solicitud.

Se entrará en la aplicación OCI en modo anónimo para introducir el CIF y el identificador de la solicitud. Se verificará que la solicitud se encuentra en estado “Aprobada” y se pulsará la opción “Generar Claves”.

La aplicación generará un par de claves - una pública y otra privada - que serán almacenadas automáticamente - sin intervención del usuario - en el navegador del PC desde donde se está accediendo a OCI.

En el caso de que el paso finalice sin errores, la solicitud cambiará al estado “Clave pública Enviada”. La PKI generará el certificado en un plazo de 24 horas y lo dejará disponible en la aplicación OCI para que el responsable de la entidad lo pueda descargar. Una vez generado el certificado, la solicitud cambiará al estado “Certificado Generado” y se enviará una notificación por correo electrónico al responsable del certificado. Se podrá continuar con el paso siguiente.

2.1.1.5 Paso 5 de 6: Descarga del certificado.

Se entrará en la aplicación OCI en modo anónimo para introducir el CIF y el identificador de la solicitud. Se verificará que la solicitud se encuentra en estado “Certificado Generado” y se pulsará la opción “Instalar Certificado”.

¡¡Importante!!: es necesario que el PC desde donde se generaron las claves sea el mismo que el que se va a utilizar para descargar e instalar el certificado.

El certificado se descargará e instalará automáticamente sin intervención del usuario. Tras finalizar un mensaje indicará que la instalación ha sido correcta y la solicitud cambiará al estado “Certificado Descargado”. Se podrá continuar con el paso siguiente.

2.1.1.6 Paso 6 de 6: Copia de seguridad del certificado y claves a un fichero.

Se entrará en la aplicación OCI en modo anónimo y al pulsar el enlace **Pulse aquí para conocer los pasos a seguir para realizar una copia de seguridad**, podrá consultar los detalles del procedimiento a seguir.

Básicamente, el proceso consiste en exportar el certificado a un fichero, incluyendo la clave privada y protegiendo dicho fichero con una contraseña o PIN. Su finalidad es la de almacenar una copia de respaldo del certificado y claves.

2.1.2 Acceso con certificado aceptado por el Banco de España

Se accederá a la aplicación OCI entrando en la web del Banco de España www.bde.es, y seleccionando >Servicios al público>Certificados y firma electrónica>Solicitud de certificados a PKIBDE y, a continuación, el enlace **Acceder a la aplicación con autenticación mediante certificado**.

La aplicación muestra todos los cuatro pasos¹ a seguir para la obtención de un certificado de entidad externa del Banco de España:

2.1.2.1 Paso 1 de 4: Instalación de los certificados de las Autoridades de Certificación de la PKI del Banco de España.

Se instalan el certificado de la autoridad de certificación raíz (ACraiz.crt) y el de la autoridad de certificación corporativa (ACcorporativa.crt).

2.1.2.2 Paso 2 de 4: Solicitud de un nuevo certificado.

Cumplimentar la solicitud de certificados con los datos necesarios para ello, posteriormente realizar la firma electrónica de la información contenida en la solicitud, y finalmente la generación del par de claves asociadas al certificado.

- Datos de la empresa solicitante:

Se rellenan de forma automática con la información obtenida del certificado utilizado para la autenticación el CIF y el nombre de la entidad debiendo el usuario introducir

E-mail. Dirección desde la que se utilizará el certificado para el envío y recepción de mensajes de correo electrónico firmado y cifrado.

- Datos del responsable del certificado (firmará electrónicamente el formulario generado):

Nombre y apellidos.

Cargo.

Teléfono.

E-mail.

Tipo y Nº de documento identificativo.

- Datos del contacto técnico (por si es necesario contactar durante el proceso de generación del certificado):

¹ En este caso no es necesario el envío por correo físico de la solicitud ni la posterior generación de claves, procesos ambos que se obvian gracias a que el usuario se ha autenticado mediante un certificado admitido por el Banco de España.

Teléfono.

E-mail.

Los mensajes de correo electrónico relacionados con el ciclo de vida del certificado serán enviados a las direcciones de correo electrónico del responsable y del contacto técnico.

2.1.2.3 Paso 3 de 4: Descarga del certificado.

Se podrá acceder a la descarga/instalación del certificado de entidad externa emitido, así como a la de su solicitud firmada electrónicamente.

2.1.2.4 Paso 4 de 4: Copia de seguridad del certificado y claves a un fichero.

Se entrará en la aplicación OCI en modo anónimo y al pulsar el enlace [Pulse aquí para conocer los pasos a seguir para realizar una copia de seguridad](#), podrá consultar los detalles del procedimiento a seguir.

2.2 Intercambio de claves públicas entre el grupo de inspección y la entidad supervisada

Como último requisito previo al normal intercambio de información es preciso que ambas parte, grupo de inspección y entidad supervisada, dispongan cada una de ellas de la clave pública de la otra. Para conseguir ese objetivo se precisan dos pasos:

2.2.1 Envío de correo electrónico al buzón departamental del grupo

Una vez que la entidad haya descargado su certificado procederá a enviar un mensaje firmado al buzón departamental del grupo de inspección. De este modo el grupo de inspección obtendrá la clave pública de la entidad supervisada.

2.2.2 Instalación del certificado del grupo de inspección en la entidad supervisada.

El certificado del grupo de inspección podrá descargarse desde el sitio web de la PKIBDE (pki.bde.es), en concreto desde la página <http://pki.bde.es/certifdgsup.htm> donde se encuentran publicados los certificados PKIBDE de los diferentes grupos de inspección.

En aquellos casos en que no fuese posible la descarga por el procedimiento anterior¹, el grupo de inspección enviará desde el buzón departamental del grupo un mensaje firmado utilizando su certificado PKIBDE².

¹ En aquellos casos en los que el cliente de correo electrónico es Lotus Notes no es posible la descarga del certificado desde el sitio pki.bde.es

² Al firmar un mensaje queda automáticamente anexo el certificado del remitente.