Instrucciones para la solicitud, descarga e instalación de un certificado digital vía OCI

El presente documento describe el procedimiento de solicitud del certificado digital requerido para la utilización del software DMO, tal como se establece en la Instrucción 1/2006, para el cumplimiento de la obligación de comunicación sistemática a que se refieren los artículos 20 de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo y 27 de su Reglamento, aprobado por Real Decreto 304/2014, de 5 de mayo.

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

1. **Acceso a la aplicación OCI:** La aplicación OCI es accesible a través del sitio web del Sepblac en www.sepblac.es > Sujetos Obligados > Trámites > Comunicación sistemática, haciendo clic en el enlace "Infraestructura de Clave Pública del Banco de España". Alternativamente se podrá acceder a través de la url http://pki.bde.es/pkibde/es/menu/solicitudes/ o haciendo clic aquí.

   Una vez en el sitio web de la PKI del Banco de España haga clic en "Acceder a la aplicación sin autenticación".

2. **Solicitud de un nuevo certificado:** La aplicación OCI detalla en su página web todos los pasos que se deben seguir a fin de obtener e instalar un nuevo certificado. Vaya directamente al paso 2 "Solicitud electrónica del certificado". Cumplimente el formulario electrónico de acuerdo con las siguientes instrucciones y haga clic en "Solicitar certificado":

   - Datos de la empresa solicitante: Se deben consignar obligatoriamente el nombre y el CIF o el código BIC del sujeto obligado.

   - Uso para el que se solicita el certificado: Se debe seleccionar obligatoriamente la opción "Sepblac".

   - Datos del responsable del certificado: Se deben consignar obligatoriamente los datos del representante del sujeto obligado ante el Sepblac.

   - Datos del contacto técnico: Se deben consignar obligatoriamente el teléfono y la dirección de correo electrónico del contacto técnico.

Tenga en consideración que los datos de contacto técnico consignados en este apartado serán empleados en cualquier futura comunicación en relación con aspectos técnicos relativos al certificado (incluidas las notificaciones sobre la caducidad y necesidad de renovación del certificado), por lo que se recomienda incluir los datos del representante del sujeto obligado ante el Sepblac o de alguno de sus autorizados.

Al hacer clic en el botón "Solicitar Certificado" se procederá al validado de todos los datos del formulario. En caso de que la validación sea correcta, la solicitud quedará almacenada en la aplicación OCI y se mostrará un identificador único de la solicitud en pantalla. Asimismo, se generará un documento PDF con los detalles de la solicitud, incluido el identificador único de la solicitud. Tanto el PDF como el identificador deben conservarse para su uso en los siguientes pasos. El estatus de la solicitud cambiará al estado "Pendiente de aprobación".

3. **Impresión, firma y envío de la solicitud por correo postal al Sepblac:** El documento PDF generado en el paso anterior deberá ser impreso a doble cara y firmado por el representante del sujeto obligado ante el Sepblac en el apartado "Firma del solicitante", dentro de la sección "Aceptación de condiciones".

   El documento consta de dos copias: una para el solicitante y otras para el Sepblac. El "Ejemplar para enviar al Banco de España" deberá ser remitido por correo postal a la siguiente dirección:

   Sepblac
   Calle Alcalá, 48
   28014 Madrid

4. **Aprobación de la solicitud:** el Sepblac recibirá ambas, la solicitud firmada vía postal y por la solicitud electrónica El Sepblac comprobará los datos y aprobará o rechazará la solicitud.

   - En caso de aprobación, el estatus de la solicitud cambiará al estado "Aprobada" y se enviará un correo electrónico al representante. Se podrá continuar con el paso siguiente.

   - En caso de rechazo, la solicitud cambiará al estado "Rechazada" y se enviará una notificación indicando las causas del rechazo por correo electrónico.

5. **Generación de claves:** El solicitante debe acceder a la aplicación OCI siguiendo las indicaciones detalladas en el paso 1 y accediendo directamente al paso 4 "Generación de las claves". Identifíquese con el CIF o el código BIC y el identificador único de la solicitud. Sólo si el estatus de la solicitud es "Aprobada", haga clic en "Generar claves".

La aplicación OCI generará una clave pública y otra privada que serán almacenadas automáticamente en el navegador del ordenador desde donde se está accediendo a la aplicación OCI. En el caso de que el proceso finalice con éxito, el estatus de la solicitud cambiará al estado "Clave pública enviada". La autoridad PKI generará el certificado en el plazo de 24 horas. Una vez que el certificado haya sido generado el estatus de la solicitud cambiará al estado "Certificado Generado" y se enviará una notificación al representante del sujeto obligado ante el Sepblac por correo electrónico.

6. **Descarga e instalación del certificado:** El solicitante debe acceder a la aplicación OCI siguiendo las indicaciones detalladas en el paso 1 y hacer clic directamente en el paso 5 "Descarga del certificado". Identifíquese con el CIF o código BIC y el identificador único de la solicitud. Sólo si el estatus de la solicitud es "Certificado generado", haga clic en "Instalar certificado".

   ¡Atención! El ordenador empleado para la descarga e instalación del certificado debe ser el mismo que el empleado en el paso anterior.

   El certificado se instalará automáticamente. Un mensaje indicará que la instalación se ha completado correctamente y el estatus de la solicitud cambiará al estado "Certificado descargado".

7. **Copia de seguridad del certificado y las claves:** El objeto de este paso es la generación de un fichero de certificado en formato PKCS#12 (.pfx) para su instalación posterior en la aplicación DMO a fin de comenzar a enviar las declaraciones.

   El solicitante debe acceder a la aplicación OCI siguiendo las indicaciones detalladas en el paso 1 y hacer clic directamente en el paso 6 "Copia de seguridad del certificado y claves a un fichero". Siga el enlace "Pulse aquí para conocer los pasos a seguir para realizar una copia de seguridad" para consultar el proceso a seguir.

   Básicamente, el proceso consiste en exportar el certificado a un fichero, incluyendo la clave privada, y protegiendo dicho fichero con una contraseña. Durante el proceso se solicitará especificar la carpeta en la que se guardará el fichero y el nombre del mismo. El fichero descargado deberá cargarse en la aplicación DMO a fin de comenzar a enviar las declaraciones.