Instructions on how to request, download and install a digital certificate via OCI

This document describes the procedure to obtain the digital certificate required to use the DMO software in accordance with Instruction 1/2006, in order to fulfill the obligation of systematic communication referred in articles 20 of Law 10/2010 of 28 April on the prevention of money laundering and terrorist financing and 27 of its Regulations, approved by Royal Decree 304/2014 of 5 May.

All applications must be processed through the OCI application in accordance with the following instructions:

1. **Access the OCI application:** The OCI application is accessible through the link "Infraestructura de Clave Pública del Banco de España", available at the Sepblac website at www.sepblac.es > Sujetos Obligados > Trámites > Comunicación sistemática. Access is alternatively available through the following url http://pki.bde.es/pkibde/es/menu/solicitudes/ o by clicking here.

   Once on the Banco de España PKI website, click on "*Acceder a la aplicación sin autenticación*".

2. **Request a new certificate:** The OCI application shows on its homepage all the steps that must be followed in order to obtain and install a new certificate. Go directly to step 2 "*Solicitud electrónica del certificado*". Complete the electronic application form according with the following instructions and click on "*Solicitar certificado*":

   - *Datos de la empresa solicitante*: Business name ("*Nombre*") and CIF or BIC code ("*Número de identificación fiscal (CIF/BIC)*") must be mandatorily filled out in this section.

   - *Uso para el que se solicita el certificado*: "Sepblac" must be mandatorily selected from the list.

   - *Datos del responsable del certificado*: Details on the obliged entity representative to Sepblac must be introduced in this section: Name ("*Nombre*"), first surname ("*Primer apellido*"), second surname if so ("*Segundo apellido*"), position ("*Cargo*"), phone ("*Teléfono*"), e-mail, type of id ("*Tipo de documento identificativo*") and id number ("*Nº de documento identificativo*").

- *Datos del contacto técnico*: Phone ("*Teléfono*") and e-mail address of the obliged entity technical contact must be mandatorily filled out in this section.

  Please note that any details included in this section might be used in any future communication in relation to technical aspects related to the certificate (including notifications on the expiration and the necessary renewal of the certificate), thus it is highly recommended to include the details of the obliged entity representative to Sepblac.

All fields will be validated by clicking the submit button ("*Solicitar certificado*"). Should validation be successful, the request will be saved by the OCI application and a single identification request reference will be shown on screen. A PDF document with the application details including the single identification request reference will be generated. Both the PDF document and the single identification request reference must be saved for the next steps. Request status will change to Pending of approval ("*Pendiente de aprobación*")

3. **Print, sign and submit the application to Sepblac via post mail:** The PDF document generated in the previous step must be both side printed and signed by the obliged entity representative to Sepblac under "*Firma del solicitante*", in section "*Aceptación de condiciones*".

   The document consists of two copies: one for the requester and one for Sepblac. The "*Ejemplar para enviar al Banco de España*" issue must be submitted by post mail to the following address:

   Sepblac
   Calle Alcalá, 48
   28014 Madrid Spain

4. **Application approval:** Sepblac will receive both the hand signed application via post mail and the electronic request. Sepblac will check the details and approve or reject the request.

   - In case of approval, the status of the request will change to Approved ("*Aprobada*") and a notification will be sent via e-mail. The process might be continued.

   - In case of rejection, the status of the request will change to Rejected ("*Rechazada*") and a notification detailing the reasons for rejection will be sent via e-mail.

5. **Keys generation:** The requester must access the OCI application by following the indications detailed on step 1 and go directly to step 4 "*Generación de las claves asociadas a la solicitud*". Log in with the CIF or BIC code and the single

identification request reference ("*Código de la solicitud*"). Only if the status of the request is Approved ("*Aprobada*"), click on Key generation ("*Generar claves*")

The OCI application will generate a public and a private key that will be automatically stored in the internet browser of the computer used for accessing the OCI application. In case the process be successful, the status of the request will change to Public key sent ("*Clave pública enviada*"). The PKI authority will generate the private key within the next 24 hours. Once the certificate have been generated the status of the request will change to Generated ("*Certificado generado*") and a notification will be sent to the obliged entity representative to Sepblac via e-mail.

6. **Download and install the Certificate:** The requester must access the OCI application by following the indications detailed in step 1 and go directly to step 5 "*Descarga del certificado*". Log in with the CIF/BIC code and the single identification request reference ("*Código de la solicitud*"). Only if the status of the request is Generated ("*Certificado generado*"), click on Certificate installation ("*Instalar certificado*")

   Warning! The PC used to download and install the certificate must be the same used in the previous step.

   The certificate will be automatically installed. A message will indicate that the installation has completely been done and the status of the request will change to Downloaded ("*Certificado descargado*").

7. **Certificate and keys backup:** The aim of this step is the generation of a certificate file PKCS#12 (.pfx) for its later installation in the DMO software in order to start reporting declarations.

   The requester must access the OCI application by following the indications detailed in step 1 and go directly to step 6 "*Copia de seguridad del certificado y claves a un fichero*". Follow the link "*Pulse aquí para conocer los pasos a seguir para realizar una copia de seguridad*" in order to check the procedure to be followed.

   The process basically consists on exporting the certificate into a file, including the private key, and protecting it with a password. A folder in the PC and a name for the file must be provided by the user. The downloaded file will have to be loaded to the DMO software in order to start reporting declarations.