
Guía de configuración del cliente para el envío del reporte FATCA

V2.0

Tabla de contenido

1.	Introducción.....	3
1.	Definición del Servicio para Producción.....	3
1.1	Consideraciones Generales.....	3
1.2	Configuración del Servicio.....	3
2.2.1.	Binding.....	4
2.2.2.	EndpointBehaviors.....	4
2.2.3.	Client.....	4
1.3	Instalación de la Jerarquía del Certificado.....	5
1.4	Instalación de certificados para la autenticación y envío del reporte FATCA.....	9
2.	Clases.....	21
3.	Tipo de archivo.....	22
3.1	Tipo FATCA 1.....	22
4	Mensajes de validación.....	24
5	Versiones.....	25

1. Introducción

El contenido de esta guía tiene como objetivo explicar la forma en que las Instituciones Financieras pueden realizar tanto la **configuración de un cliente como el envío oficial del archivo XML** a través del servicio FATCA expuesto por el BCCR.

1. Definición del Servicio para Producción

1.1 Consideraciones Generales

- El objetivo principal de esta sección es lograr establecer una comunicación entre el BCCR y el/los cliente(s) configurado(s) por una Institución Financiera usuaria del servicio.
- El servicio expuesto es un Windows Communication Foundation (WCF).
- **NO** es necesario indicar las direcciones IP públicas de los equipos que se utilizarán para hacer los envíos oficiales.
- La función del servicio consiste en mostrar al usuario el estado de la comunicación entre el BCCR y la Institución Financiera.
- La respuesta del servicio se retorna en formato XML.
- Esta configuración aplica para el archivo **web.config** del cliente que consume el WCF FACTA.
- El servicio está publicado en la ruta:

<https://servicioleyfatca.go.cr/servicesftc/fatcaxml.svc>

1.2 Configuración del Servicio

Se debe establecer una referencia del servicio publicado por el BCCR utilizando la ruta <https://servicioleyfatca.go.cr/servicesftc/fatcaxml.svc>

Se recomienda que el archivo de configuración (**web.config**) del cliente contenga las siguientes secciones:

2.2.1. Binding

```
<bindings>
  <wsHttpBinding>
    <binding name="WSFatcaHttpsBinding" closeTimeout="10:30:00"
      openTimeout="10:30:00" receiveTimeout="10:30:00" sendTimeout="00:30:00"
      maxBufferSize="2147483646" maxReceivedMessageSize="2147483646">
      <readerQuotas maxDepth="64" maxStringContentLength="2147483647"
        maxArrayLength="2147483647" maxBytesPerRead="2147483647"
        maxNameTableCharCount="2147483647" />
      <security mode="TransportWithMessageCredential">
      <transport clientCredentialType="Certificate" proxyCredentialType="None" realm="" />
      <message clientCredentialType="Certificate" negotiateServiceCredential="true"
        algorithmSuite="Default" />
      </security>
    </binding>
  </wsHttpBinding>
</bindings>
```

2.2.2. EndpointBehaviors

```
<endpointBehaviors>
  <behavior name="BCCR_Servidor_Behavior">
    <clientCredentials>
      <clientCertificate findValue="CN=BCCR-FC-XXXXXX.XXXXX.XX.XXX-###, OU=FATCA, O=BCCR, L=SJ, C=CR"
        storeLocation="LocalMachine" storeName="My"
        x509FindType="FindBySubjectDistinguishedName"/>
      <serviceCertificate>
        <authentication certificateValidationMode="PeerOrChainTrust"
          revocationMode="NoCheck" trustedStoreLocation="LocalMachine" />
      </serviceCertificate>
    </clientCredentials>
  </behavior>
</endpointBehaviors>
```

2.2.3. Client

```
<client>
  <endpoint address="https://servicioleyfatca.go.cr/servicesftc/FatcaXml.svc"
    behaviorConfiguration="BCCR_Servidor_Behavior" binding="wsHttpBinding"
    bindingConfiguration="WSFatcaHttpsBinding" contract="BS.Fatca.IFatcaXml"
    name="WSHttpBinding_IFatcaXml">
    <identity>
      <dns value="spe.bccr.fi.cr"/>
    </identity>
  </endpoint>
</client>
```

Nota:

En el recuadro 2.2.2. EndpointBehaviors, es necesario que cada Institución Financiera ingrese el GIIN de la entidad responsable de realizar el envío del reporte FATCA y el número de nodo ingresado durante la solicitud del certificado, ejemplo:

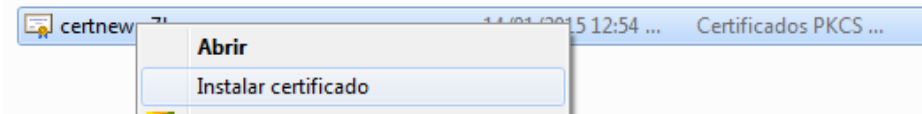
`findValue="CN=BCCR-FC-ABC123.00000.LE.188-100, OU=FATCA, O=BCCR, L=SJ, C=CR"`

Lo anterior se debe porque a partir del 2017 cuando una Institución Financiera realice el proceso de envío del reporte FATCA, se validará el identificador único otorgado por el IRS a cada entidad.

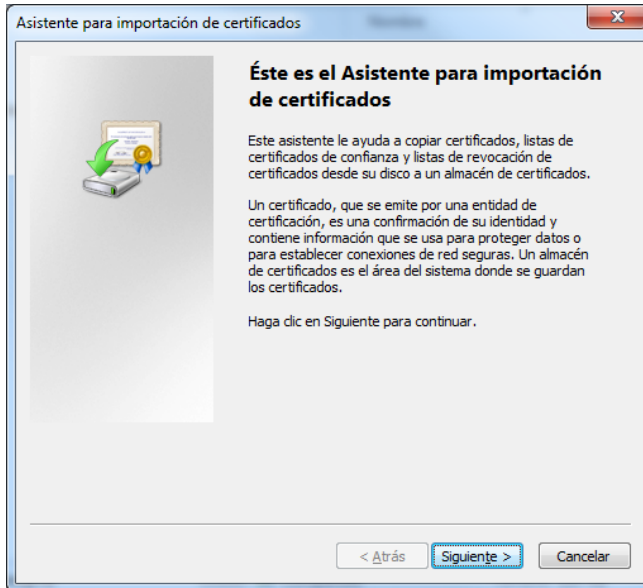
1.3 Instalación de la Jerarquía del Certificado

Se debe instalar la siguiente jerarquía de certificados para que el cliente pueda crear el canal de seguridad y establecer la relación de confianza con el servidor.

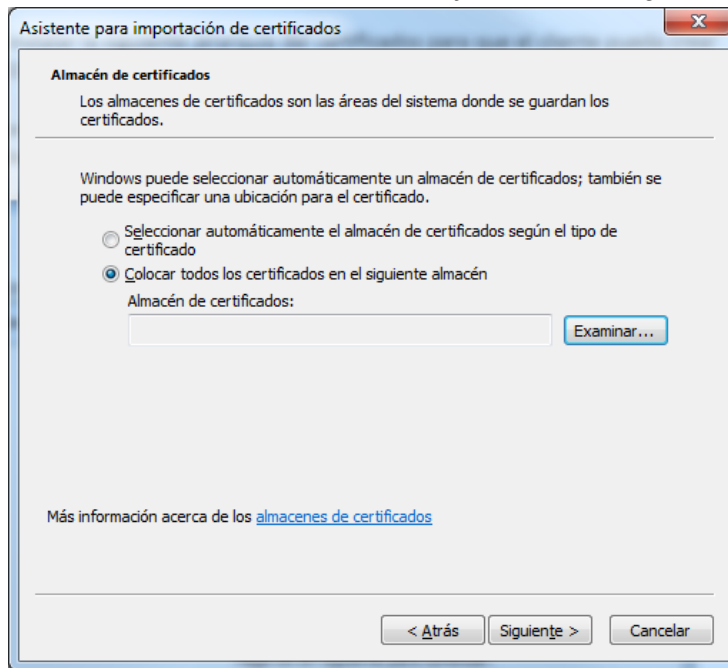
- a. Descargar el archivo *"Cadena_Confianza_CAExternaBCCR.zip"* del sitio www.bccr.fi.cr/fatca
- b. Clic derecho sobre el archivo y seleccionar *"Instalar certificado"*.



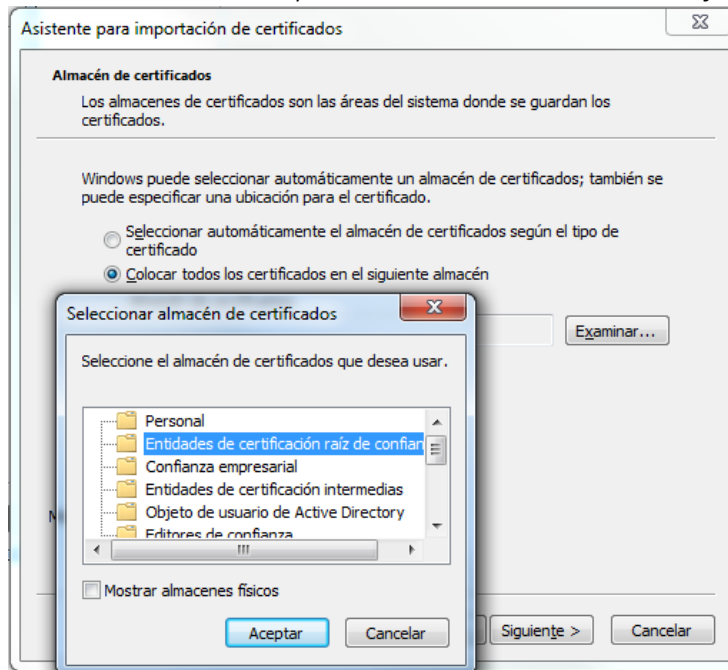
- c. Presionar *"siguiente"*.



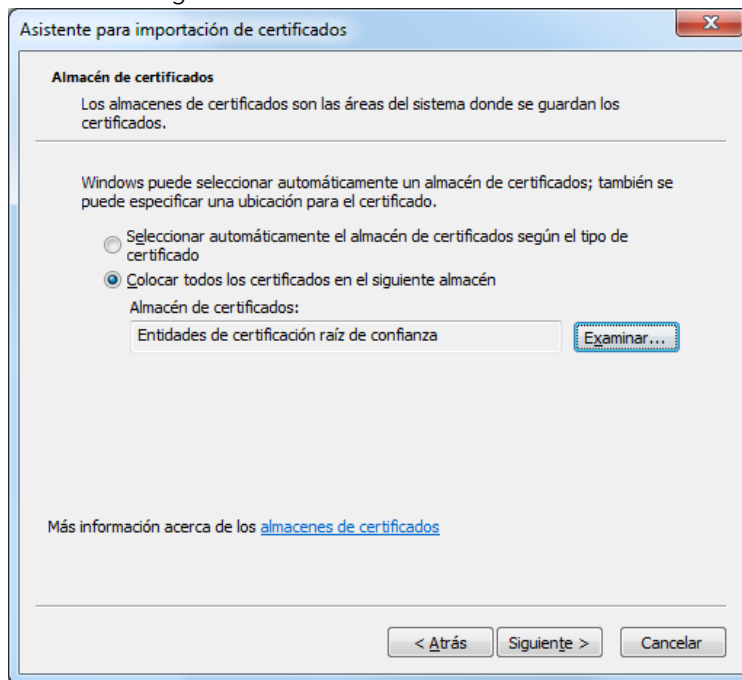
d. Seleccionar “Colocar todos los certificados en el siguiente almacén”.



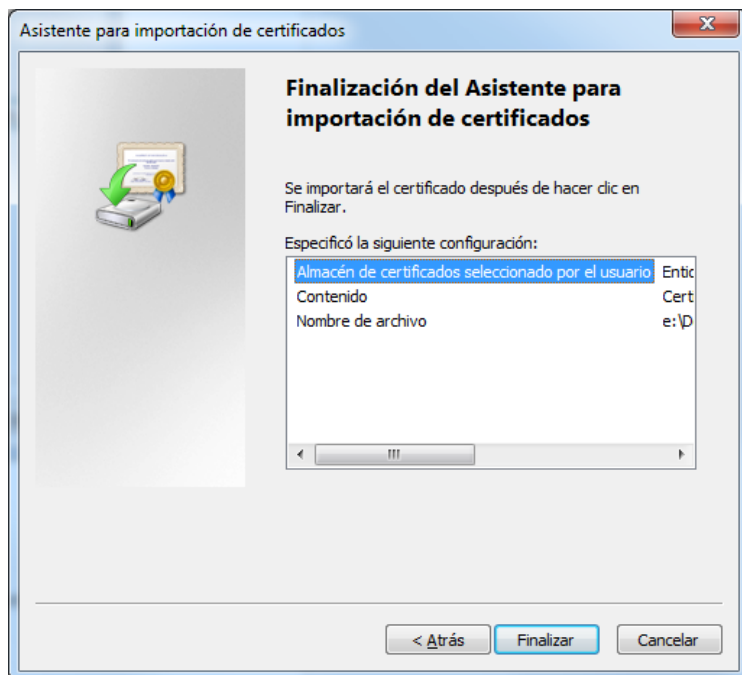
e. Presionar “Examinar” y seleccionar “Entidades de certificación raíz de confianza”.



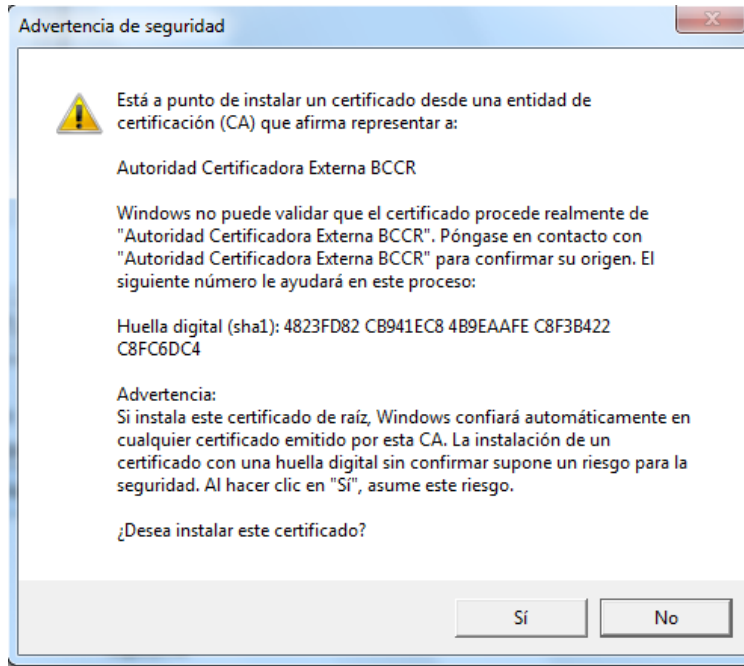
f. Presionar “*Siguiente*”.



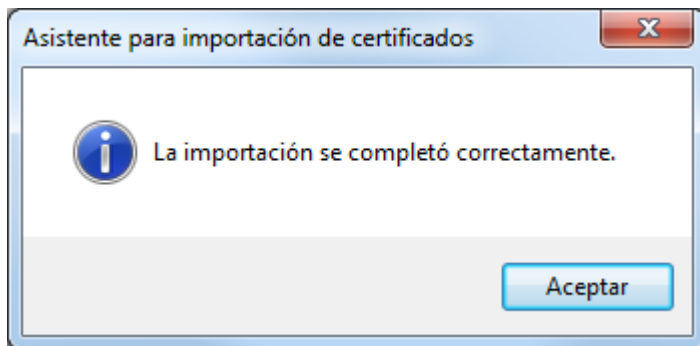
g. Presionar “*Finalizar*”.



- h. En la advertencia de seguridad indicar que **Sí** desea instalar el certificado “*Autoridad Certificadora Externa BCCR*”.



- i. Aplicar los mismos pasos anteriores para el certificado “*CARaizBCCR*”.
- j. Cuando finaliza la importación de un certificado, el asistente indica que la operación se realizó correctamente.



1.4 Instalación de certificados para la autenticación y envío del reporte FATCA

Para gestionar un certificado con el estándar del subject GIIN FATCA, el usuario designado por cada entidad debe ingresar al sitio web FATCA y realizar el proceso de solicitud mediante los siguientes pasos:

Ingresar al sitio FATCA, opciones de “Seguridad, Certificados”.



- a. Presionar la acción “agregar”.

Seguridad

Solicitudes de Certificados para WebServices

refrescar agregar eliminar generar enviar configurar descargar exportar

^- Número de Nodo x

	<input type="checkbox"/>	Solicitud	Número de	Fecha Solicitud	Estado Solicitud	Expiración Certificado
No hay registros para mostrar.						

- b. Completar los datos de la solicitud:

Número de Nodo: consecutivo para identificar el equipo en el que se instalará el certificado.

Descripción: texto libre para indicar la razón de la solicitud del certificado.

Crear Solicitud

Datos de la solicitud:

Número de Nodo

Descripción

c. Presionar el botón finalizar para completar la solicitud.

Crear Solicitud

Luego de agregar la solicitud, se debe marcar de la lista y presionar el botón Generar para obtener el script que se debe ejecutar en el nodo para el cual desea solicitar el certificado digital. Seguidamente, debe completar la solicitud con el request obtenido luego de ejecutar el script en el nodo.

d. Seleccionar la solicitud del certificado y presionar la acción “generar”.

Seguridad

Solicitudes de Certificados para WebServices

^- Número de Nodo x

<input type="checkbox"/>	Solicitud	Número de	Fecha Solicitud	Estado Solicitud	Expiración Certificado
<input checked="" type="checkbox"/>		68	100	30/03/2017 03:26:38 p.m.	Creada

Detalle Certificado WebServices Asociados Seguimiento

Detalle

Número Request:

Descripción: Certificado de prueba

Generar script para ejecutar en el nodo

Script para crear una solicitud de certificado

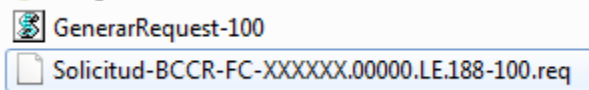
A continuación se generará el script para crear una solicitud de certificado.

Debe realizar los siguientes pasos:

- Renombrar la extensión del archivo obtenido a ".vbs" (eliminar el "_")
- Copie el archivo en un dispositivo de almacenamiento removible
- Ejecute el archivo (doble click) **en el servidor que requiere el certificado digital**
- Luego de la ejecución del script verifique que se generó la solicitud (archivo "req")
- Utilizando la acción Enviar asocie el archivo "req" a la solicitud correspondiente

¿Quieres abrir o guardar **GenerarRequest-100.vbs_** (6,26 KB) desde **leyfatca-pru.dnz-p.local**?

- e. Renombrar el archivo *.vbs_ y eliminar el caracter '_'. Este archivo se debe ejecutar en la máquina sobre la cual se está solicitando el certificado. Al ejecutar el archivo se creará en la misma ubicación un archivo con extensión ".req".



- f. Enviar el archivo .req obtenido mediante la acción "enviar".

Seguridad

Solicitudes de Certificados para WebServices

^- Número de Nodo x

<input type="checkbox"/>	Solicitud	Número de	Fecha Solicitud	Estado Solicitud	Expiración Certificado
<input checked="" type="checkbox"/>		68	100	30/03/2017 03:26:38 p.m.	Creada

Detalle Certificado WebServices Asociados Seguimiento

Detalle

Número Request:

Descripción: Certificado de prueba

Enviar Solicitud

Elegir archivo request

Seleccione un archivo con extensión "req" para enviar:

d-BCCR-FC-XXXXXX.000

Después de realizar el envío, el sistema notifica al usuario que el certificado fue aprobado.

refrescar agregar eliminar generar enviar configurar descargar exportar

~ Número de Nodo x

	<input type="checkbox"/>	Solicitud	Número de	Fecha Solicitud	Estado Solicitud	Expiración Certificado
v Número de Nodo: 100						
	<input type="checkbox"/>	68	100	30/03/2017 03:26:38 p.m.	Aprobada	30/03/2018 03:38:22 p.m.

Resultado del envío del request.

El certificado fue aprobado

- g. Seleccionar la solicitud y descargar el certificado mediante la acción "descargar".

Seguridad

Solicitudes de Certificados para WebServices

refrescar agregar eliminar generar enviar configurar **descargar** exportar

~ Número de Nodo x

	<input type="checkbox"/>	Solicitud	Número de	Fecha Solicitud	Estado Solicitud	Expiración Certificado
v Número de Nodo: 100						
	<input checked="" type="checkbox"/>	68	100	30/03/2017 03:26:38 p.m.	Aprobada	30/03/2018 03:38:22 p.m.

Tipos de archivo disponibles para bajar

Eliga el tipo de archivo que desea bajar para el certificado
CN=BCCR-FC -XXXXXX.00000.LE.188-100, OU=FATCA, O=BCCR, L=SJ, C=CR

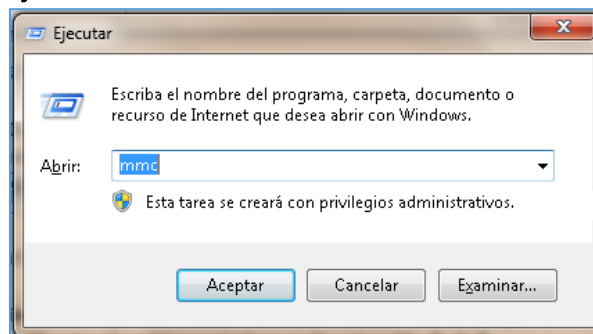
Certificado digital para colocar en el store del servidor de la entidad Dado que no existen webservices aprobados, solamente se puede generar el certificado digital

1. Instalación del certificado digital.

IMPORTANTE: la instalación del certificado se debe realizar en la máquina o equipo donde se ejecutó el archivo anterior con la extensión “.vbs”. Adicionalmente para los pasos de instalación de certificados con llave privada, es necesario hacerlo bajo un usuario administrador.

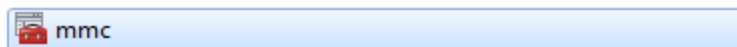
- 1.1 En la ventana “Ejecutar” de Windows (aparece presionando las teclas **Windows + r**) escribir la instrucción “**mmc**”, o en el “buscador” de Windows escribir la instrucción “**mmc**” y abrir el ejecutable **mmc.exe**.

Ejecutar de Windows

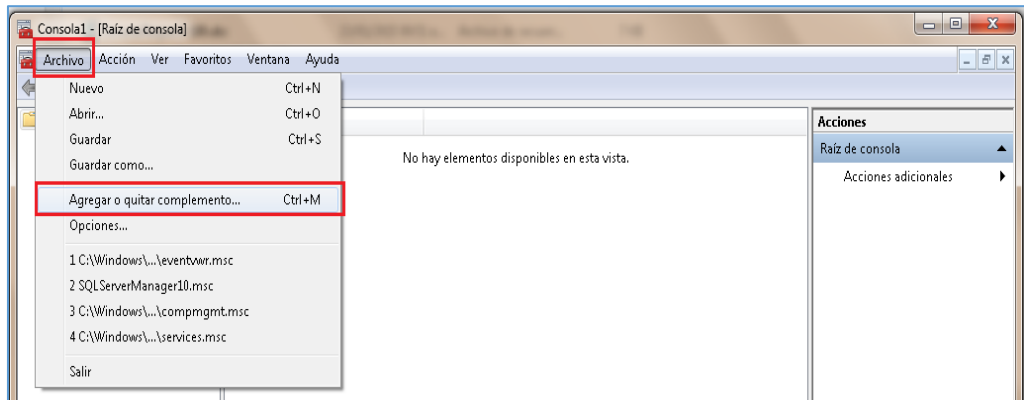


Buscador de Windows

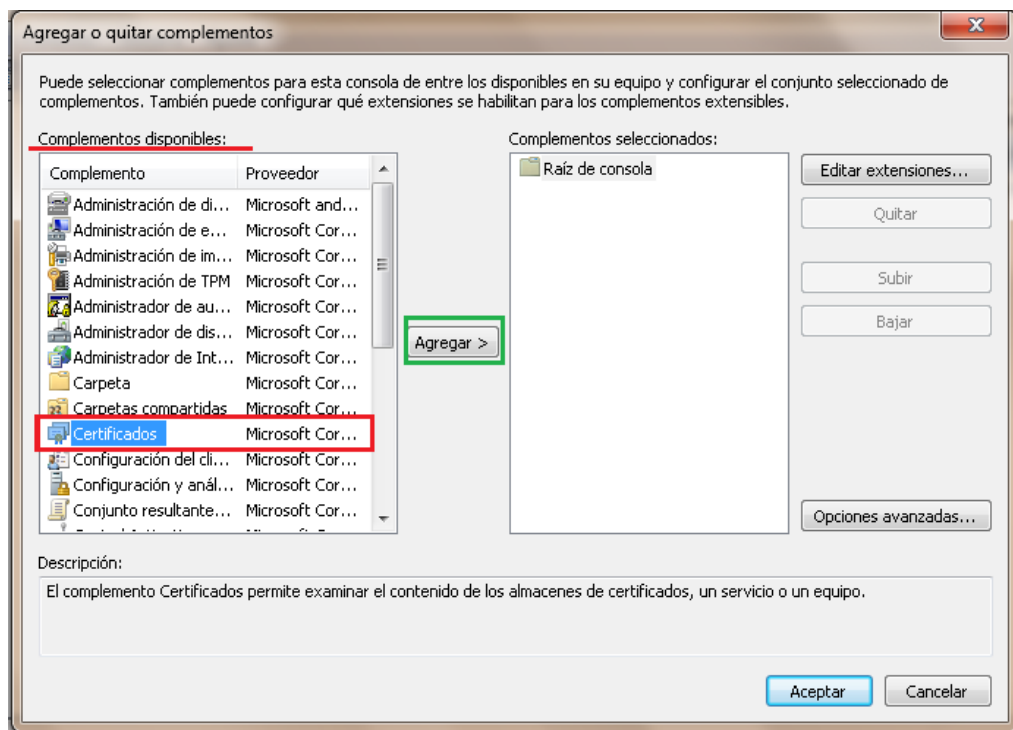
Programas (1)



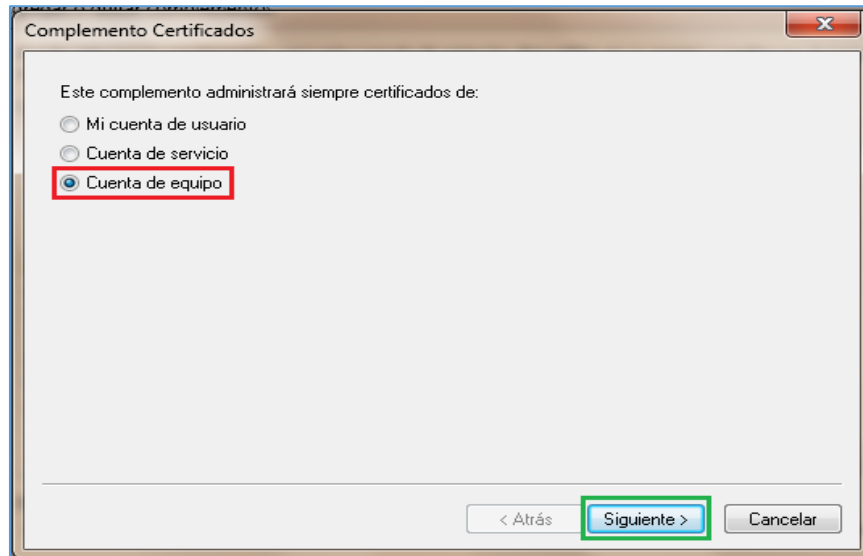
- 1.2 Dentro del **mmc**, ir a la pestaña de “**Archivo**” y dar clic sobre la opción de “**Agregar o quitar complemento**”.



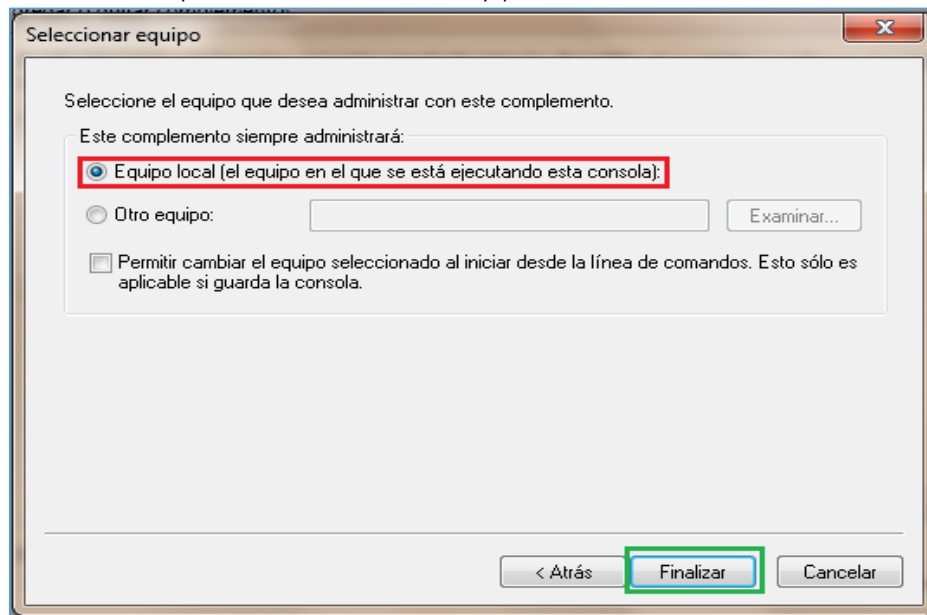
1.3 En la ventana de **“Agregar o quitar complementos”**, elegir de los complementos disponibles la opción de **“certificados”**, y presionar **“Agregar”**.



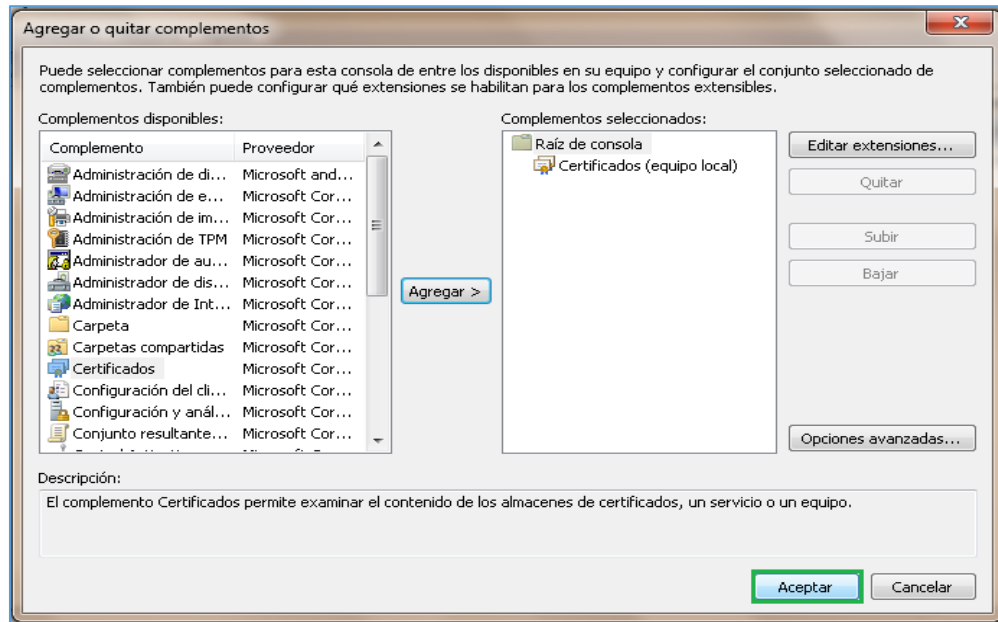
1.4 A continuación en la ventana de **“Complemento Certificados”** elegir la opción **“Cuenta de equipo”** y presionar **“Siguiente”**.



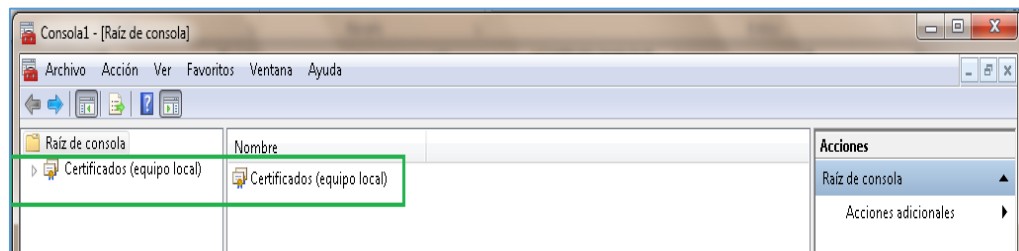
1.5 En la ventana de “*Seleccionar equipo*”, elegir la opción “*Equipo local*” seleccionada predeterminadamente y presionar “*Finalizar*”.



1.6 En la ventana de “*Agregar o quitar complementos*”, presionar “*Aceptar*”.

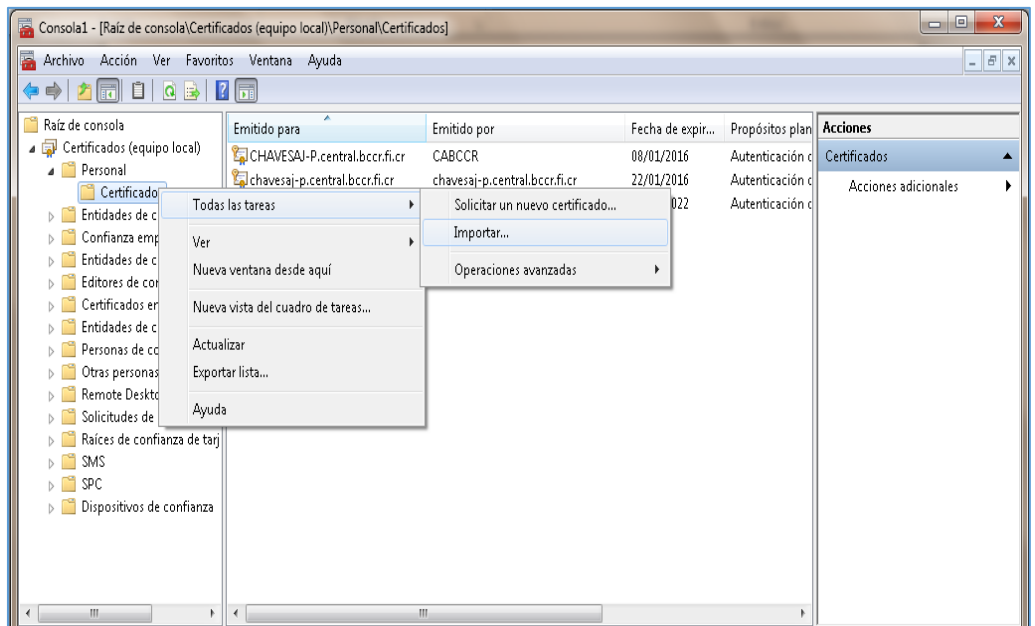
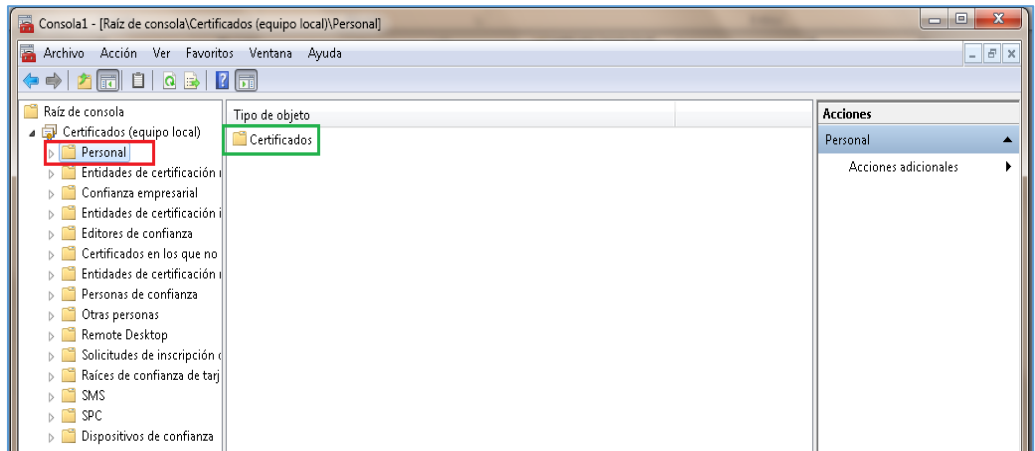


1.7 En la vista principal del **mmc** (Raíz de consola), se generó un registro de certificado.

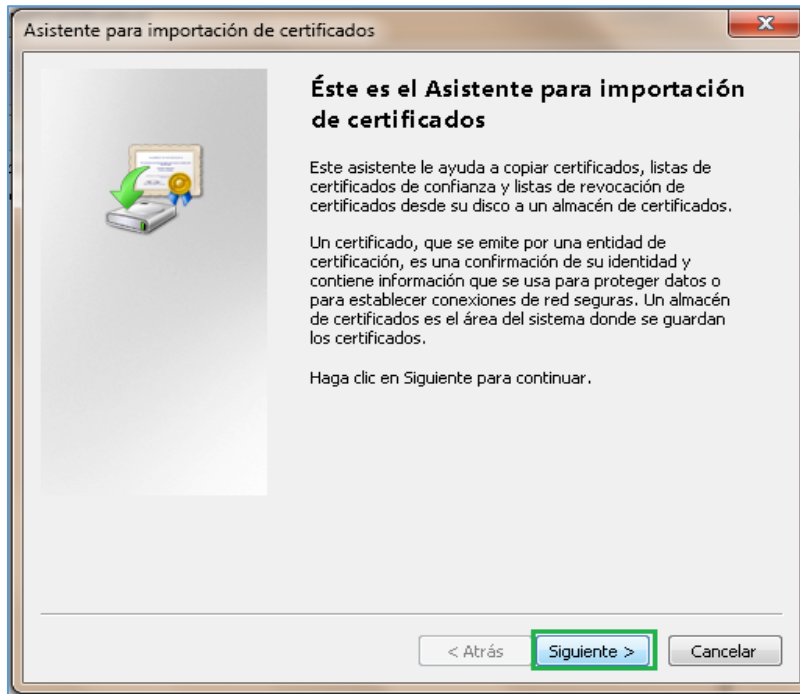


1.8 Expandir la lista de *“Certificados (equipo local)”* en la *“Raíz de consola”* y elegir la opción *“Personal”*. Luego dar doble clic sobre el tipo de objeto *“Certificados”*.

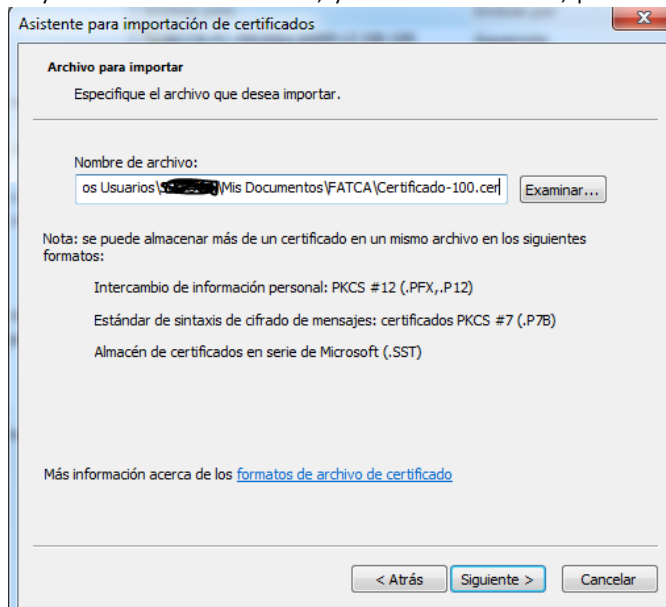
1.9 En la opción de *“Certificados”* dar clic derecho y elegir las opciones *“Todas las tareas - Importar”*.



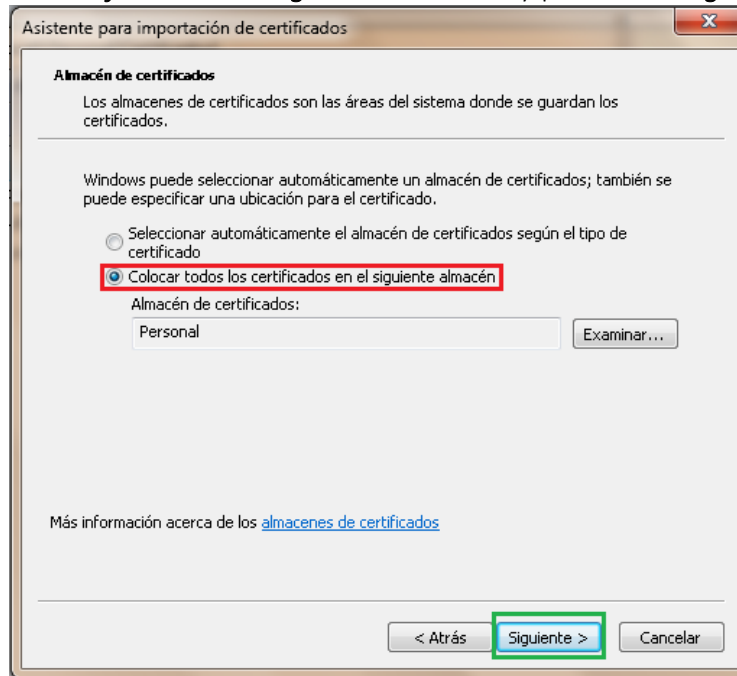
1.10 A continuación, se muestra el asistente para la importación de certificados. Presionar ***"Siguiente"***.



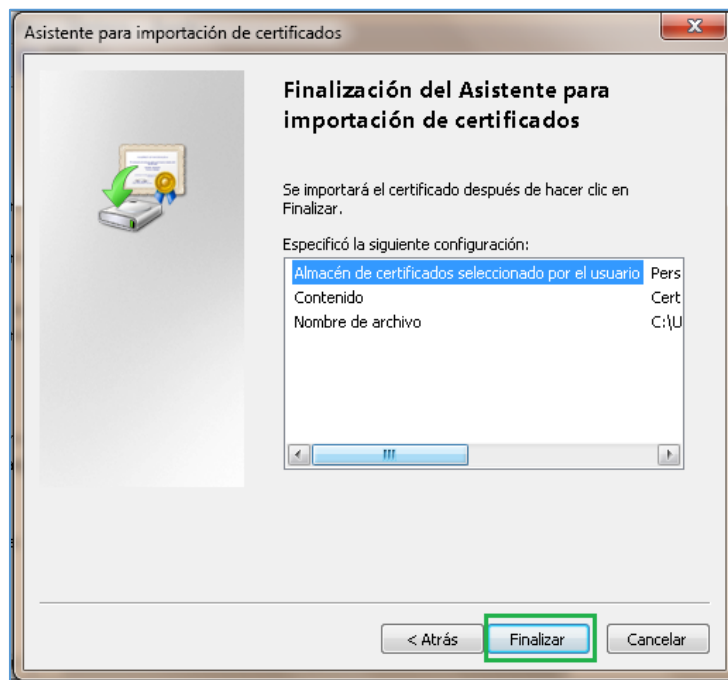
1.11 A continuación, seleccionar la ruta del certificado descargado previamente cuya extensión es “.cer”, y una vez ubicado, presionar “*Siguiete*”.



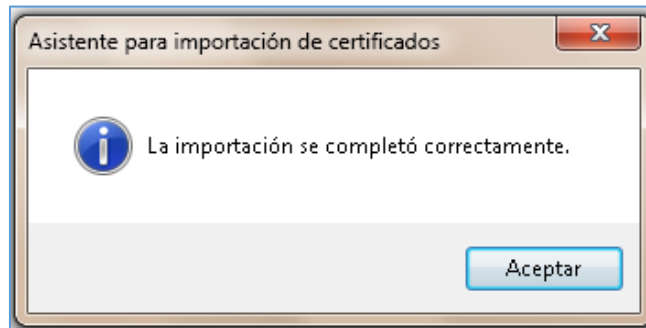
1.12 En la ventana “*Almacén de certificados*”, seleccionar la opción “*Colocar todos los certificados en el siguiente almacén*” y presionar “*Siguiente*”.



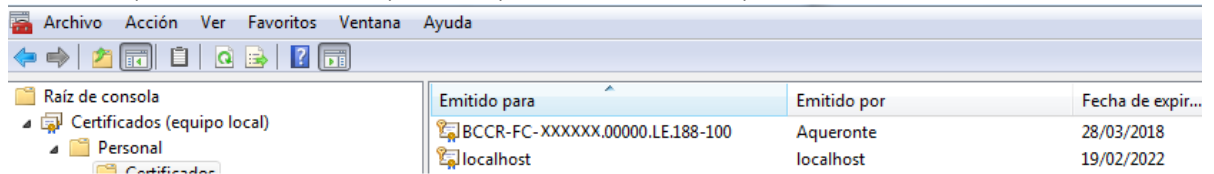
1.13 Finalizar el asistente.



Mensaje de confirmación exitosa.

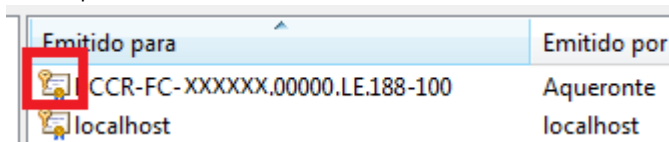


2. Verificar que el certificado importado presente una llave privada.



Emitido para	Emitido por	Fecha de expir...
BCCR-FC-XXXXXX.00000.LE.188-100	Aqueronte	28/03/2018
localhost	localhost	19/02/2022

Llave privada.



Emitido para	Emitido por
BCCR-FC-XXXXXX.00000.LE.188-100	Aqueronte
localhost	localhost

2. Clases

Nota: Para consumir el servicio, se recomienda que el usuario tenga permisos de administrador sobre el equipo en el que ejecuta la aplicación. Además, la aplicación para realizar el envío del reporte FATCA debe consumir el servicio utilizando el Framework de Microsoft .Net 4.5.2 o superior.

El Servicio WCF expone la función **Enviar**¹ la cual permite la transferencia de archivos (reportes FATCA) solicitados por el Ministerio de Hacienda para su posterior envío al IRS.

Método

```
Public Function Enviar(ByVal archivo() As Byte, _  
                      ByVal periodo As Integer, _  
                      ByVal anyo As Integer) As String
```

Archivo

Arreglo de Bytes con el contenido del archivo.

Periodo

Período al que pertenece la información. En este caso archivo XML se envía de forma anual y el valor esperado en este parámetro es siempre 1.

Año

Año al que pertenece la información. Este dato debe ser consistente con el elemento **ReportingPeriod**² contenido en el encabezado del reporte FATCA.

Respuesta

Retorna el estado y la descripción del procesamiento del reporte FATCA.

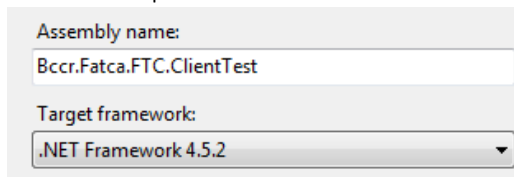
```
<Fatca>  
  <Codigo/>          --Resultado del procesamiento  
  <Detalle/>         --Resultado de las validaciones  
</Fatca>
```

¹ Asegurarse de actualizar la referencia al servicio para obtener la última versión publicada.

² <https://www.irs.gov/pub/fatca/pub5124userguidev20draft.pdf>

Configuración del cliente con TLS:

- Verificar que el cliente utiliza el Framework de .Net 4.5.2 (o superior), ejemplo:



The image shows a configuration window with two fields. The first field is labeled 'Assembly name:' and contains the text 'Bccr.Fatca.FTC.ClientTest'. The second field is labeled 'Target framework:' and is a dropdown menu currently showing '.NET Framework 4.5.2'.

- Antes de consumir el servicio para realizar el envío, se debe agregar la siguiente línea que especifica el protocolo de seguridad TLS:

```
System.Net.ServicePointManager.SecurityProtocol = SecurityProtocolType.Tls11 Or SecurityProtocolType.Tls12  
respuesta = servicio.Enviar(archivo, periodo, anyo)
```

3. Tipo de archivo

3.1 Tipo FATCA 1

3.1.1 Cargar un nuevo reporte FATCA: para cargar un reporte de tipo FATCA1, es necesario que cada entidad compruebe mediante el esquema XSD otorgado por el IRS en su sitio web FATCA que el reporte XML cumple con el estándar de validaciones FATCA.

3.1.2 Cargar nuevos nodos FATCA a un archivo base: para cargar nuevos nodos FATCA1 a un archivo base (reporte FATCA1 almacenado en el repositorio previamente y con estado finalizado), el elemento “<sfa:MessageRefId>” ubicado dentro del nodo “<ftc:MessageSpec>” del archivo actual (reporte FATCA1 reciente) debe ser igual al “<sfa:MessageRefId>” del archivo base. Los elementos “<ftc:DocRefId>”, al utilizar el formato recomendado por el IRS “**GIIN + GUID**”, asegura que ninguno de estos elementos ubicados dentro del nodo “<ftc:ReportingFI>” sean iguales, ya que esta validación es contemplada por el IRS durante la revisión del reporte FATCA.

Nota: los archivos tipo FATCA1 no deben contener nodos de corrección, ejemplo, “<sfa:CorrMessageRefId>” o “<ftc:CorrDocRefId>”.

Importante: cuando una entidad ha enviado un reporte FATCA de manera exitosa, si desea adjuntar nuevos datos a un reporte enviado previamente, el elemento “<sfa:MessageRefId>” debe referenciar al archivo base enviado. De igual manera, si se realizan varias recargas, el elemento “<sfa:MessageRefId>” del archivo reciente deberá referenciar siempre al último archivo finalizado exitosamente.

Nota: para conocer más a fondo las validaciones, estructura, ejemplos, caracteres no permitidos en los reportes y formatos de cada archivo, es necesario que cada entidad ingrese al sitio oficial FATCA perteneciente al Internal Revenue Service (IRS) de Estados Unidos:

- Esquemas y recomendaciones del IRS:
<https://www.irs.gov/businesses/corporations/fatca-xml-schemas-and-business-rules-for-form-8966>
- Caracteres no permitidos por el IRS:
<https://www.irs.gov/businesses/corporations/fatca-xml-schema-best-practices-for-form-8966>
- Estándar electrónico del IRS:
<https://www.irs.gov/pub/fatca/pub5124userguidev20draft.pdf>

4 Mensajes de validación

La siguiente tabla muestra los mensajes retornamos al usuario por parte del servicio WCF.

Código	Descripción	Datos Adicionales
0	El archivo ha sido recibido exitosamente.	No
1	Ocurrió un error interno.	No
2	La entidad con Id fatca [{0}] no se encuentra registrada.	Sí
3	La entidad [{0}] con el Id Fatca [{1}] no ha firmado el acuerdo de uso.	Sí
4	El archivo suministrado se encuentra vacío.	No
5	El archivo no corresponde a un archivo xml.	No
6	El archivo suministrado no corresponde a un archivo esperado [{0}].	Sí
7	El archivo suministrado no es válido según el esquema. Contiene los siguientes errores: {0}.	Sí
8	El Id Fatca suministrado en el archivo no coincide con el Id Fatca de la entidad.	No
9	Ya existe una carga para ese mismo archivo. Código de verificación: [{0}].	Sí
10	La fecha del período del archivo no coincide con la suministrada.	No
11	La fecha plazo para hacer envíos correspondientes al año [{0}] es [{1}] y su carga se intentó tramitar el [{2}]. Posterior a la fecha de cierre sólo se aceptan archivos de tipo "FATCA2".	Sí
12	El archivo con código de verificación [{0}] corresponde a un archivo Fatca 2, y esté sólo será permitido después de la fecha de cierre.	Sí
13	El archivo con código de verificación [{0}] corresponde a un archivo FATCA2, pero no se han suministrado datos previos.	Sí
14	Error en el procesamiento del consolidado parcial o recarga de un archivo FATCA con errores. <ul style="list-style-type: none">• Por ejemplo: Error, el elemento <sfa:MessageRefId> del archivo base debe coincidir con el elemento <sfa:CorrMessageRefId> del archivo actual.	Sí
15	El año proporcionado [{0}] no es el esperado. No se puede verificar contra la fecha de cierre.	Sí

5 Versiones

Versión	Descripción
2.0	Se actualiza la información referente a certificados y tipos de archivos FATCA. Se adjuntan enlaces oficiales del IRS.
1.8.0	Se agrega explicación de re carga de archivos.
1.7.0	Se actualiza la sección 5(Mensajes de validación).
1.6.0	Se agrega la sección de la configuración del servicio para producción.
1.5.2	Se actualiza la sección 3 (Clases) se definen los parámetros que recibe la función Enviar . Se agregan nuevos mensajes de validación (4, 5, 6, 7, 8, 9, 10,11) a la sección 4.
1.4.1	Se actualiza la sección 2.4 (Instalación de certificados para la autenticación) Se agrega una especificación al paso 3.
1.3.4	Se actualiza la sección 2.2 (Configuración del servicio) para la comunicación con el uso de certificados digitales. Se agrega el punto 2.4 (Instalación de certificados para la autenticación). Esta sección describe la configuración del cliente, para la autenticación mediante el uso de un certificado digital. Se actualiza la sección 3 (Clases). Se agrega una nota importante sobre la ejecución de la aplicación. Se actualiza la sección 4 (Mensajes de validación). Se agrega nuevos mensajes de validación.
1.2.2	Se elimina el punto 2.2.4 y se reemplaza por la sección 2.3 <u>Instalación de la Jerarquía del Certificado</u> . Con esta actualización se resuelven los problemas de la relación de confianza entre el cliente y el servidor.

1.1.1	Se actualiza la sección 2.2 (Configuración del servicio). Se agrega especificación del elemento <system.net> para el archivo de configuración del cliente para la fase de pruebas con el servicio.
1.0	Guía de configuración para validar la prueba inicial de comunicación entre el BCCR y las Instituciones Financieras que utilizan el servicio FATCA.