SUSTITUCIÓN DE CERTIFICADOS EN SOPORTE PAPEL 3.0 (SCSPv3)

Palabras clave
Ley 11/2007, administración electrónica, eliminación de certificados en soporte papel, intercambio de datos entre administraciones públicas.

1. Introducción

El derecho del ciudadano a no presentar documentos que obren en poder de las administraciones públicas está reconocido en la Ley 30/1992, del Régimen Jurídico y del Procedimiento Administrativo Común, y en la Ley 11/2007, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.

Para facilitar el ejercicio de este derecho el Ministerio de la Presidencia (antiguo Ministerio de Administraciones Públicas) definió, mediante la especificación SCSP (Sustitución de Certificados en Soporte Papel), los aspectos técnicos referentes a la arquitectura y estándares de intercambio necesarios para posibilitar el uso generalizado de transmisiones de datos entre organismos, necesarias para el ejercicio de sus competencias en el marco de un procedimiento administrativo. De esta forma SCSP aporta a las administraciones públicas un nuevo método de intercambio seguro de información entre ellas.

Los trámites que deberán hacer los ciudadanos se verán muy simplificados si el organismo tramitador es autorizado por el ciudadano a recabar los certificados directamente de los organismos emisores que los expidan. De este modo, aquellos organismos que para el ejercicio de sus competencias en el marco de un procedimiento administrativo, pidan certificados a los ciudadanos que deben ser expedidos por la Administración verán sus procedimientos agilizados y podrán realizar la tramitación totalmente de forma electrónica.

Para las administraciones supondrá un ahorro de costes al disminuir el número de certificados a realizar para el ciudadano. En el caso del ciudadano supone un ahorro de tiempo y coste, y la agilización en la resolución de sus trámites.

2. SCSPv2

SCSPv2 define las siguientes características para las transmisiones de datos que se realicen entre administraciones:

- El formato de las transmisiones de datos es XML.
  Se han definido dos documentos (petición y respuesta) con dos partes; la primera, Datos Genéricos, donde se transmite información común a todos los certificados en papel que se sustituyen, como la relativa al organismo solicitante, al organismo emisor, al interesado al que se refieren los datos, y la relativa a la propia transmisión. En la segunda parte de Datos Específicos, cada organismo define los campos que transmite en función del tipo de certificado en papel que se está sustituyendo. Estos datos específicos también deberán estar en formato XML, pero es obligación de cada organismo emisor publicar el esquema XSD que indica la estructura del mismo. También se han definido otros dos documentos XML "Confirmación petición" y "Solicitud respuesta" que se emplean cuando la petición es realizada en modo asíncrono, para indicar que la petición se recibió correctamente y para solicitar la respuesta transcurrido el Tiempo Estimado de Respuesta indicado por el emisor respectivamente.
- El envío de peticiones y respuestas se realiza mediante servicios Web.
- El protocolo utilizado para la comunicación es SOAP sobre https.
- La infraestructura de comunicaciones sobre la que se apoya todo el servicio de sustitución de certificados en soporte papel es la Red SARA.

- Para asegurar la autenticación, confidencialidad e integridad de la información transmitida se emplea el protocolo SSL, exigiendo identificación a ambos extremos mediante certificado electrónico reconocido.
- La integridad de los datos y el no repudio se garantiza firmando tanto las peticiones como las respuestas emitidas en el sistema. La firma se transmite en la cabecera SOAP del mensaje, utilizando la codificación XMLdSig.
- Para la conservación de la información, cada organismo emisor deberá almacenar las transmisiones emitidas durante el tiempo establecido en la normativa aplicable. Se propone un sistema y esquema de almacenamiento común a todos los organismos emisores y otro común para todos los organismos requirentes, (incluidos en las librerías).
- El sistema permite que la petición-respuesta sea síncrona o asíncrona.

En el marco de un grupo de trabajo formado por varios organismos entre ellos la AEAT y la TGSS, se han definido y construido unas librerías que implementan SCSPv2 y, que se integran con las aplicaciones. Las librerías son distribuidas gratuitamente por el Ministerio de la Presidencia a los organismos, facilitando la implantación del sistema. Estas librerías están desarrolladas en Java y en .Net. Por otro lado, cualquier organismo puede desarrollar el sistema basándose en las especificaciones funcionales y técnicas de SCSP.

El funcionamiento del servicio es el siguiente:
- El organismo requeriente transmite una petición identificada de datos al organismo emisor.
- El organismo emisor valida el certificado y la firma del requirente y si está autorizado a pedir estos datos.
- Envía la solicitud al back-office para tramitarla.
- Transmite la respuesta firmada al requirente.

En el modelo síncrono, sólo se admiten peticiones de consultas unitarias, esto es, solo se puede recabar información de un único tipo de certificado, relativa a un único titular. La respuesta del servicio Web debe ser en línea, sobre la misma conexión https establecida entre el requirente y el emisor.
En el modelo asíncrono, se admiten peticiones múltiples. En este caso, la petición contendrá muchas solicitudes, aunque en el sistema se ha determinado que todas ellas deben referirse a un único tipo de certificado. Tras recibir la petición el emisor confirmará la recepción al requirente y le indicará el Tiempo Estimado de Respuesta, transcurrido el cual podrá solicitarle la respuesta. Una vez transcurrido ese tiempo, para recoger la respuesta el requirente realizará un sondeo a un servicio web de recogida de respuestas.
Las peticiones múltiples están pensadas para procedimientos que se realizan en momentos puntuales, como por ejemplo un periodo abierto para solicitar subvenciones, en que el organismo tramitador se encuentra con que necesita en un breve periodo de tiempo, información relativa a muchos interesados.

Se permite a cada organismo personalizar tanto aquellos servicios/certificados que publica (en los que actúa como emisor) como aquellos servicios/certificados que va a usar o consultar (en los que actúa como requirente).

En la siguiente tabla se recogen los servicios en v2 que actualmente se encuentran en producción:

Organismo Emisor	Servicio
TGSS	Estar al corriente de pago con la Seguridad Social
	Alta en la Seguridad Social
AEAT	Certificado de la Renta de las Personas Físicas
	Domicilio fiscal
	Certificados de estar al corriente de las obligaciones tributarias
	Contratación con las administraciones públicas
	Obtención de licencias de transporte
	Solicitud de subvenciones y ayudas
	Tramitación de permisos de residencia y trabajo para extranjeros
SPEE Servicio Público de Empleo Estatal	**Servicios de prestaciones por desempleo**
	Situación actual
	Importes actuales
	Importes percibidos por periodo
DGP	Consulta de datos de identidad
	Datos de Identidad-Verificación
INE	Datos de residencia
	Datos de residencia extendidos
Educación	Títulos universitarios
	Títulos no universitarios
Catastro	Datos catastrales
	Certificación de titularidad
	Descriptiva y gráfica
Ministerio de la Presidencia	Cambio de domicilio

Tabla 1: Servicios SCSPv2 en producción

3. SCSPv3

Después de casi 4 años de uso de la primera versión estable de SCSP, SCSPv2, en distintos proyectos indicados en la Tabla 1 se ha puesto en evidencia una serie de carencias o mejoras necesarias que han desembocado en la versión 3 de SCSP.

La versión SCSPv3 incorpora las siguientes novedades:

- Debido a la desaparición del Ministerio de Administraciones Públicas, y con el objetivo de obtener un lugar de referencia para poder ubicar los esquemas de SCSP, se ha sustituido el espacio de nombres map.es por intermediacion.redsara.es para hacerlos independientes de la nomenclatura de los organismos que los usan, e indicar que la versión soportada es adecuada para la intermediación.

- Introduce nuevos campos en el esquema (Datos Genéricos) asociados al "Solicitante" de la información, que se habían identificado como necesarios en el uso de la versión 2.
    - Unidad Tramitadora: Unidad dentro del Órgano Solicitante que realiza la solicitud.
    - Procedimiento
        - CodProcedimiento: Código del Procedimiento del Organismo tramitador
        - NombreProcedimiento: Nombre unívoco del procedimiento del Organismos tramitador.
    - IdExpediente: Identificador del expediente en el Organismo tramitador.
- Se ha cambiado el versionado de los esquemas, pasando de V2 a v3.
- Por motivos de interoperabilidad con los estándares actuales más modernos, se ha optado por sustituir el mecanismo de firma basado en XML-SIG puro, por el especificado dentro de la familia WS-Security. Modelo de firma más estandarizado e implementado por las distintas plataformas SOA.
- Incorpora la posibilidad de cifrado en las respuestas en aquellas situaciones que el emisor lo considere necesario por motivos de confidencialidad de la información a intercambiar. Por defecto, el cifrado irá siempre en la respuesta, aunque por necesidades del servicio se podría aplicar a cualquier mensaje intercambiado, y se cifrará exclusivamente aquella información especialmente sensible que se quiera proteger. Por regla general se cifrará el contenido del nodo <datos específicos>.

  El uso de cifrado se ha incorporado debido a que mientras que en SCSPv2 la comunicación entre organismos requirentes y emisores era punto a punto y con SSL la confidencialidad estaba garantizada, SCSPv3 está orientado a servicios intermediados, aunque no exclusivamente a ellos, en que un tercero podría ver la información en caso de que esta no estuviese cifrada.

Al igual que en SCSPv2 se han definido y construido unas librerías, que se integran con las aplicaciones y que el Ministerio de la Presidencia distribuye a los organismos gratuitamente facilitando la implantación del sistema. Estas librerías están desarrolladas en Java. Por otro lado, al igual que en SCSPv2 cualquier organismo puede desarrollar el sistema basándose en las especificaciones funcionales y técnicas de SCSPv3.

El funcionamiento es idéntico al de v2 en el caso en que el emisor no cifre sus respuestas. En el caso en que el emisor considere necesario por motivos de confidencialidad de la información a intercambiar cifrar su respuesta, el funcionamiento es el siguiente:

- El organismo requeriente transmite una petición identificada de datos al organismo emisor.
- El organismo emisor valida el certificado y la firma del requirente y si está autorizado a pedir estos datos.
- Envía la solicitud al back-office para tramitarla.
- Cifra la respuesta, la firma y se la transmite al requirente.
- El requirente valida la firma y descifra el mensaje.

Las librerías de SCSPv3 van a permitir que se puedan emplear los esquemas de la versión 2 y de la 3 en la misma aplicación. Esto permitirá que un requirente invoque emisores que empleen tanto esquemas de la v2 como de la v3, y que el emisor podrá procesar tanto peticiones con esquemas de v2 como con esquemas de v3.

En la siguiente tabla se recogen los servicios en v3 que actualmente se encuentran en producción:

Organismo Emisor	Servicio
TGSS	Estar al corriente de pago con la Seguridad Social (Deuda)
AEAT	Certificados de estar al corriente de las obligaciones tributarias para la solicitud de subvenciones y ayudas

Tabla 2: Servicios SCSPv3 en producción

4. ¿Qué es necesario para el uso de SCSP?

Los Requisitos para los organismos que deseen prestar el servicio son los siguientes:

- Estar conectado a la Extranet Administrativa SARA.
- Montar las librerías en un servidor o cumplir las especificaciones de "Sustitución de Certificados Soporte Papel".
- Conectar las librerías con la aplicación de tramitación del procedimiento o simplemente hacer una página que pida las transmisiones necesarias.
- Instalar un certificado X509V3 emitido por una autoridad de certificación reconocida por la Administración General del Estado en ese servidor.
- Para las CCAA y EELL, es necesario la firma de un convenio marco entre la administración requirente y el emisor.

5. Simplificación de la instalación de las librerías mediante un asistente de instalación y configuración

Con el objeto de facilitar la instalación y configuración de las librerías de Sustitución de Certificados en Soporte Papel se ha desarrollado un asistente para la instalación y configuración de las mismas (*Wizard*), el cual va guiando al usuario por diferentes pantallas de configuración permitiendo una instalación rápida y sencilla.

El *Wizard* mostrará en primer lugar la siguiente pantalla, donde se deberá seleccionar qué tipo de instalación se quiere realizar: Nuevo Requirente, Nuevo Emisor, Modificación de un requirente o Modificación de un Emisor.

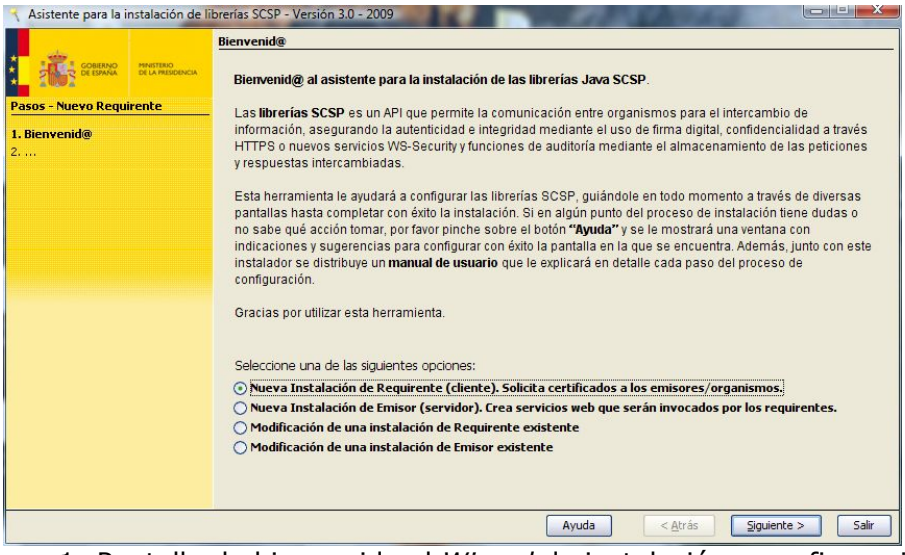

Figura 1: Pantalla de bienvenida al *Wizard* de instalación y configuración

Dependiendo del tipo de instalación se mostrarán distintas opciones de configuración. No obstante, tanto para el caso de un nuevo requirente como de un nuevo emisor se tendrán que realizar las siguientes acciones:

- **Configuración del servidor de aplicaciones:** se seleccionará el tipo de servidor (Tomcat, WebLogic, JBoss, otros) en el cual se va a desplegar la aplicación generada una vez terminado el proceso y, se indicará la ruta raíz del servidor.
- **Configuración de la conexión al servidor de base de datos:** se seleccionará el tipo de servidor de base de datos (MySQL, Oracle o PostgreSQL) y se introducirán la dirección del servidor, el puerto, el nombre de la base de datos, el usuario y el password. Una vez introducidos todos los datos se comprobará automáticamente que existe conexión a la base de datos.
- **Configuración de certificados de firma y cifrado:** se seleccionará la ruta donde se creará un almacén de certificados en el que el usuario podrá introducir o borrar los certificados que serán empleados para firmar el contenido de los mensajes o para el cifrado de los mismos.
- **Configuración de certificados de confianza:** en este almacén se encuentran los certificados de las distintas autoridades de certificación (CA's) que son de confianza para el usuario. Para realizar conexiones SSL (https) deberá asegurarse de que el certificado con clave pública del organismo al que va a invocar se encuentra en este listado.
- **Configuración de autoridades de certificación:** Aunque se incluyen, por defecto, las autoridades de certificación (CA's) más utilizadas, se da al usuario la posibilidad de editar, borrar o añadir las CA's que requiera.
- **Configuración de @Firma y LDAP:** permite al usuario configurar la conexión con @Firma para la validación de certificados. Si no se dispone de conexión a @firma y si dispone de acceso al LDAP de la FNMT, podrá configurar el acceso al mismo. En caso de que no se configure ninguno de los dos no será posible validar certificados.
- **Realizar test de toda la configuración:** permite al usuario realizar un test de la configuración realizada, indicando para cada opción configurada si está ok o no.
- **Exportación de la aplicación Web:** esta opción permite guardar toda la configuración realizada para el funcionamiento de las librerías, en un fichero .war o .ear especificado. También es posible la integración con una aplicación web de la que ya se disponga y a la que se quiera añadir la funcionalidad de las librerías. En este caso, el usuario seleccionará la aplicación con la que se desea la integración y, el *wizard* de forma automática añadirá todos los elementos necesarios para utilizar las librerías SCSP en la aplicación indicada.

Para el caso de un nuevo requirente se habrán de configurar además:

- **Instalación del esquema de base de datos para un requirente:** instala, en la base de datos que se configuró, el esquema de base de datos necesario para que un requirente puede emplear las librerías SCSP.
- **Proxy:** Si se accede a Internet a través de un Proxy, en lugar de mediante conexión directa, se deberán añadir las opciones de Proxy.
- **Codificación de las peticiones:** permite al usuario configurar el formato que tendrán los identificadores de petición que enviarán los requirentes generados con el *Wizard*. Se podrá elegir codificación corta (16 caracteres) propia de v2 o codificación larga (29 caracteres) propia de v3.
- **Certificados solicitados:** el usuario configurará los certificados a solicitar a los organismos emisores indicando el CIF del organismo emisor, el nombre del certificado, su descripción y como mínimo un endpoint (síncrono o asíncrono).
- **Manejadores:** permite configurar las acciones a realizar antes de enviar la petición al organismo y después de recibir la respuesta. Antes del envío de la

petición esta se firma y se guarda en la base de datos, no siendo esto configurable por el usuario. Tras recibir la respuesta se podrá configurar que se validen la firma, el esquema, el certificado, y el almacenamiento del fichero de petición, y siempre se almacenará la respuesta recibida en base de datos.

Para el caso de un nuevo emisor se habrán de configurar además:

- **Datos del emisor:** el usuario configurará los parámetros propios de un emisor, como son el CIF, nombre y valor de sondeo (número máximo de veces que el emisor responde al requirente para una determinada petición de tipo asíncrona).
- **Instalación del esquema de base de datos para un emisor:** permite al usuario instalar, en la base de datos que configuró, el esquema de bases de datos que un emisor necesita para hacer uso de las librerías SCSP.
- **Certificados emitidos:** se establecen las características de los certificados que el emisor que se está configurando emitirá. Para cada certificado deberá indicar su nombre, formato de las peticiones v2 o v3, fecha a partir de la cual se podrá consultar el certificado emitido, fecha en la que se dejará de poder consultar el certificado emitido, Tiempo Estimado de Respuesta que se devolverá al requirente en las peticiones de tipo asíncrona y la caducidad, que indica el número de días a partir del cual ya no se puede hacer sondeo de las peticiones asíncronas.
- **Autorización de accesos a organismos:** permite añadir, editar y borrar organismos que van a tener acceso a los certificados emitidos y, a cuáles de ellos tendrá acceso.
- **Manejadores:** a través de esta pantalla se configurarán las acciones a realizar después de recibir la petición del organismo y antes de enviarle la respuesta. Tras la recepción de la petición siempre se Valida la firma, se autentica al organismo requirente y se almacena la petición en base de datos. Además se puede configurar también la validación del esquema, la del certificado, la comprobación del sondeo y la autorización del organismo. Antes de enviar la respuesta siempre se deben firmar la respuesta, guardarla en la base de datos y, guardar en un fichero la respuesta enviada.

Para la modificación tanto de un requirente como de un emisor se mostrara una pantalla con las distintas opciones de configuración de cada uno y, el usuario podrá seleccionar cualquiera de ellas y modificarla. Después de la modificación de cualquiera de las opciones, deberá realizar una exportación para poder guardar todos los cambios realizados.

En la siguiente pantalla se ven las distintas opciones de configuración que podrá modificar un requirente:

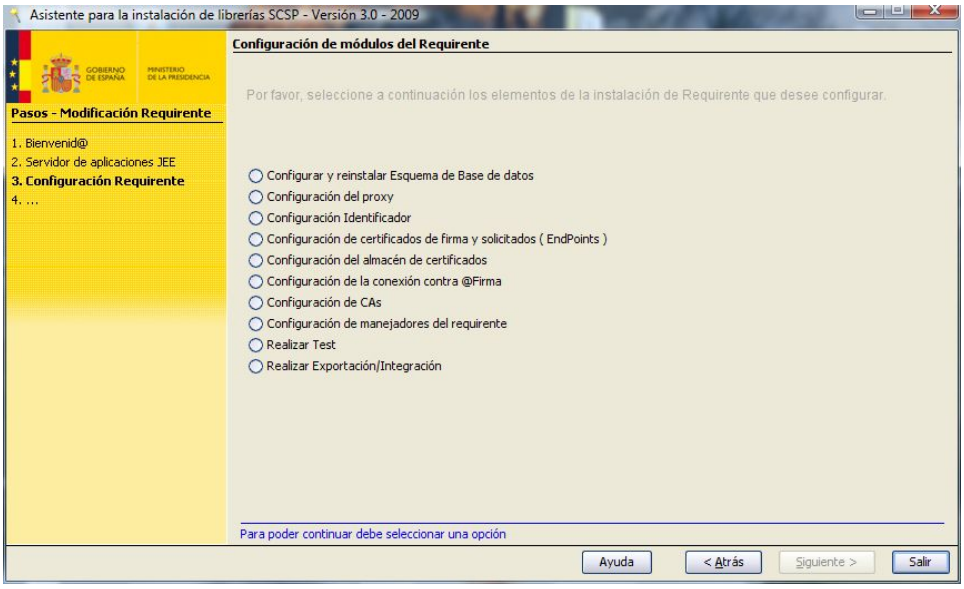

Figura 2: Modificación de un requirente

Este *Wizard* está disponible tanto para Linux como para Windows y tanto en modo grafico como en modo texto para aquellos entornos en que se carezca de interfaz gráfica.

6. Aplicación cliente SCSP 3.0

Con objeto de fomentar y facilitar que los organismos con pocos recursos puedan obtener información de otros organismos para la realización de sus trámites, tras la instalación de las librerías con el *Wizard* se obtiene una aplicación Web final. De forma que usarla resultará tan sencillo como elegir el certificado a consultar, introducir los datos del ciudadano, y obtendrá online el certificado firmado digitalmente, sin que el ciudadano haya tenido que aportarlo. De esta forma se pretende incrementar la participación de estos organismos en la supresión de certificados en soporte papel.

Se trata de una aplicación Web que consta de un conjunto de formularios, uno por cada certificado a solicitar, que recogen la información necesaria para realizar las consultas a los organismos emisores de esos certificados. También cuenta con una plantilla Excel por cada certificado, que permite el envío de múltiples peticiones de una sola vez.

El control de accesos a certificados, a través de la aplicación, será responsabilidad de cada uno de los organismos requirentes.

Acceso a la aplicación

El acceso a la aplicación se realiza mediante un navegador Web y un certificado electrónico. En la pantalla de acceso al sistema se solicita la autenticación del usuario mediante su certificado electrónico (cualquiera de los soportados por @Firma) aceptándose el DNI electrónico.

Una vez realizada la autenticación del usuario aparecerá una pantalla con tres secciones:

- Una con los distintos servicios de petición de certificados que tiene habilitados el organismo requirente tanto de forma síncrona como asíncrona.

- Otra que permitirá obtener el resultado de las peticiones realizadas de forma asíncronas una vez transcurrido el Tiempo Estimado de Respuesta.
- Una última sección que permitirá al usuario recuperar todos los Certificados que se le emitieron para una fecha de determinada o bien para una determinada petición.

Figura 3: Menú principal del cliente ligero SCSPv3

Servicios de petición de certificados

Para realizar la petición de un certificado, se pulsará sobre "Consultar" del servicio síncrono o asíncrono del correspondiente certificado. En el caso de realizar la consulta sobre el servicio síncrono se mostrará la siguiente pantalla

Figura 4: Petición síncrona mediante formulario

donde se rellenarán los datos que se solicitan y a continuación se dará a "Consultar" para enviar la petición.

También será posible enviar la petición rellenando la pestaña "XML con datos específicos" de la pantalla anterior en lugar de usar el formulario. En este caso los datos a introducir serán los mismos, pero se hará a través de un fichero XML que tendrá la estructura del esquema XSD de datos específicos publicado por el organismo emisor del certificado.

Así por ejemplo para el servicio de Verificación de datos de Residencia, será necesario introducir el fichero XML con los datos específicos de este servicio tal y como se muestra en la siguiente pantalla.

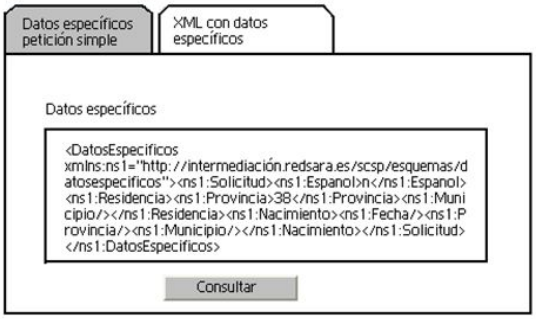

Figura 5: Pestaña "XML con datos específicos" para una petición síncrona

Al seleccionar "Consultar", en cualquiera de los dos casos, se realizará telemáticamente la consulta de los datos y tras un breve instante se mostrarán los resultados de la misma:

Figura 6: Respuesta al envío de una petición síncrona

La aplicación ofrece también la posibilidad de guardar la respuesta en un archivo Excel y en un fichero XML.

Para realizar una petición de datos con múltiples solicitudes, se debe acceder al servicio en cuestión en modo asíncrono y seleccionar la pestaña "Datos específicos

múltiples peticiones". A través de esta pestaña se descarga una plantilla Excel que tendrá la estructura adecuada al certificado a solicitar, se rellena con los datos de las solicitudes y se importa en la aplicación.

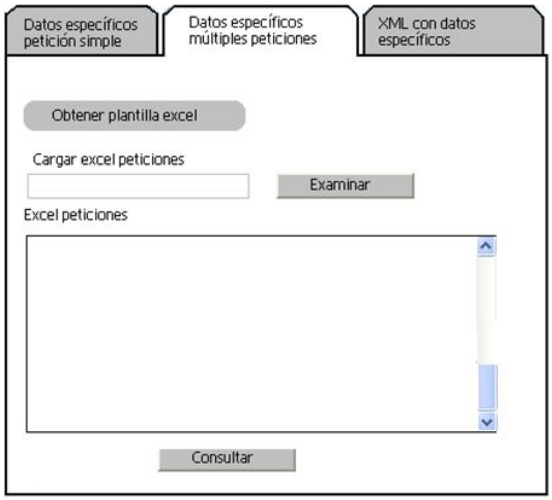

Figura 7: Pestaña datos específicos para múltiples peticiones

Al seleccionar "Consultar" se realizará telemáticamente la consulta de los datos y posteriormente y transcurrido el Tiempo Estimado de Respuesta se solicitará la respuesta a través de la "Solicitud de respuestas asíncronas" del Menú Principal.

Figura 8: Solicitud de respuestas asíncronas

Los resultados obtenidos se mostrarán de la siguiente forma:

Figura 9: Respuesta a una petición asíncrona con múltiples peticiones

La aplicación ofrece también la posibilidad de guardar la respuestas obtenidas en un archivo Excel y en un fichero XML.

Consulta de certificados emitidos

Mediante esta opción la aplicación permite la recuperación de un certificado ya emitido, a partir de la introducción del identificador de petición (código único) del mismo. Se trata de una cadena de dígitos y letras que sirve como código de recuperación y verificación de la existencia del certificado. Al seleccionar "Consultar" se recuperará el certificado con el código o identificador introducido.
También existe la posibilidad de recuperar todos los certificados que fueros solicitados por un determinado funcionario en una fecha dada, a partir de su NIF y la fecha de solicitud.

Figura 10: Consulta de certificados emitidos

7. Referencias y enlaces

La Información del proyecto está disponible en http://www.ctt.map.es/web/scsp

8. Conclusiones

El Ministerio de la Presidencia en su compromiso por sustituir los certificados en soporte papel por transmisiones de datos, va más allá de la creación de unas librerías que puedan instalarse los organismos requirentes y emisores, desarrollando un Wizard que asista al usuario durante la instalación de las librerías permitiendo una rápida y fácil instalación y configuración de las mismas.

Con el objeto de que la Sustitución de certificados en soporte papel llegue hasta los organismos que cuenta con pocos recursos, se ha desarrollado una aplicación final que permitirá a un organismo requirente, solicitar certificados de manera sencilla sin tener que realizar por su parte ningún desarrollo.