Informe de Auditoría

Servicio de verificación y consulta de datos: Plataforma de Intermediación

Índice

Introducción

En la política de simplificar la relación del ciudadano con la Administración General del Estado, el artículo 35.f) de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común establece el derecho del ciudadano a no presentar aquellos documentos que ya se encuentren en poder de la Administración.

En el año 2003 se formó un grupo de trabajo coordinado por el Ministerio de Administraciones Públicas (actual Ministerio de Hacienda y Administraciones Públicas) con el objetivo de definir y especificar el mecanismo de intercambio de información entre AAPP para eliminar

certificados administrativos en papel del que nace el protocolo SCSP (sustitución de certificados en soporte papel).

SCSP es un conjunto de especificaciones orientadas al intercambio de documentación y datos entre Administraciones Públicas con el objetivo de eliminar los certificados administrativos en papel, evitando al ciudadano presentar ante las AA.PP documentación que ya obra en poder de las mismas, sustituyéndolos por un intercambio de datos entre Administraciones que se realiza de forma electrónica, estandarizada y rápida y actualmente con las garantías jurídicas descritas en el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

En 2004 se realizaron las primeras versiones de la especificación dando como resultado en el año 2005 la primera versión estable que se denominó SCSPv2. Igualmente, se trabajó desde el Ministerio de Administraciones Públicas en unas librerías (J2EE y .NET) compatibles con el estándar para que pudieran ser utilizadas por todas las Administraciones Públicas españolas en el intercambio de certificados administrativos.

En los procedimientos administrativos ha sido habitual pedir documentos acreditativos de la identidad y del lugar de residencia a efectos de verificar estos datos personales. El Real Decreto 522/2006 y el Real Decreto 523/2006, de 28 de abril, suprimen la necesidad de aportar fotocopias de estos documentos en todos los procedimientos de la AGE y de sus organismos públicos vinculados o dependientes. No obstante, la verificación de estos datos sigue siendo esencial para la tramitación de los procedimientos.

Las órdenes ministeriales PRE/2949/2006 y PRE/4008/2006, publicadas en diciembre de 2006, establecen la configuración y características de acceso al sistema de verificación y establecen como fecha de entrada en producción de los sistemas el 1 de enero de 2007.

En el artículo 6 de la Ley 11/2007, de 22 de Junio, de Acceso Electrónico de los ciudadanos a los Servicios Públicos, se recoge como derecho de todo ciudadano a no aportar dato o documento que obre en poder de las Administraciones Públicas que utilizarán medios electrónicos para recabar dicha información siempre que, en el caso de datos de carácter personal, se cuente con el consentimiento de los interesados.

En 2009 se vio la necesidad de ampliar las especificaciones para permitir la interoperabilidad con Nodos de Interoperabilidad dando lugar a la Resolución de 28 de junio de 2012 de la Secretaría de Estado de Administraciones Públicas por la que se aprueba la Norma Técnica de Interoperabilidad de protocolos de intermediación de datos y recomienda el uso del protocolo de sustitución de certificados en soporte papel versión 3 (SCSPv3). Esta última versión no tiene previsión de cambio a corto plazo.

Por otra parte, en respuesta al mandato del artículo 46 de la Ley 11/2007 y del artículo 17 del Real Decreto 4/2010 por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la administración electrónica, se establece la existencia de nodos de interoperabilidad que son organismos que prestan servicios de interconexión técnica, organizativa y jurídica entre sistemas de información para un conjunto de Administraciones

Públicas bajo las condiciones que éstas fijen, dando carta de naturaleza a la Plataforma de Intermediación. Además, se crea el Centro de Transferencia de Tecnología que también se encuentra recogido en el artículo 158 de la Ley 40/2015.

Finalmente, la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas, en su artículo 28 dispone que "…las Administraciones Públicas deberán recabar los documentos electrónicamente a través de sus redes corporativas o mediante consulta a las plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto".

Centro de Transferencia de Tecnológia (CTT)

Este Centro publica un directorio general de aplicaciones y/o soluciones para su reutilización en la Administración General del Estado e interopera con los directorios establecidos por otras Administraciones Públicas. A través de su portal informa de proyectos, servicios, activos semánticos, normativa y soluciones que se están desarrollando en material de administración electrónica.

Sus principales objetivos son:

- ✓ Crear un repositorio común de software y de servicios para su reutilización en las Administraciones Públicas.
- ✓ Crear una base de conocimiento común sobre las diversas soluciones técnicas (normativas, servicios, activos semánticos, infraestructura, etc) en el ámbito de la Administración electrónica.
- ✓ Crear un espacio donde se puedan compartir experiencias y cooperar en el ámbito de la administración electrónica.

El CTT está a disposición de cualquier administración pública y a cualquier perfil que trabaje en el entorno de la Administración Electrónica y su funcionamiento lo determinan dos aspectos fundamentales: las soluciones y los niveles de acceso siendo la solución la unidad básica de trabajo dentro del CTT en torno a la cual se orquestan todas las funcionalidades ofrecidas y los niveles de acceso que son los que permiten personalizar la información y los servicios ofrecidos por cada solución a cada usuario.

Conceptualmente una solución puede ser entre otras, los servicios horizontales puestos a disposición de todos los organismos para facilitar o simplificar la implantación de nuevos servicios, siendo uno de ellos el servicio de verificación y consulta de datos: plataforma de intermediación.

Plataforma de intermediación

El servicio de verificación de datos permite verificar los datos de un ciudadano que ha iniciado un trámite con la entidad, de este modo el ciudadano no tendrá que aportar documentos acreditativos por ejemplo de identidad ni de residencia, en los trámites que inicie.

Por tanto, el objetivo del servicio de verificación de datos es permitir que cualquier organismo de la Administración pueda verificar dichos datos sin necesidad de solicitar la aportación de los correspondientes documentos acreditativos a su titular, permitiendo hacer efectiva esta supresión y hacer posible que la validación se realice por medios electrónicos. Se trata de un servicio en red integrable en aplicaciones del cliente.

Con este servicio se pretende:

- ✓ Dar cumplimiento a los derechos reconocidos en la Ley 30/1992 de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común y en la Ley 11/2007 de Acceso Electrónico de los ciudadanos a los Servicios Públicos y, cuando entre en vigor, a lo dispuesto en la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas.
- ✓ Hacer más cómodo para el ciudadano el inicio de los trámites, evitando que tenga que adjuntar a la solicitud documentos que acrediten su identidad y su empadronamiento.
- ✓ Simplificar la tramitación de los procedimientos administrativos.
- ✓ Reducir el volumen de papel gestionado en la Administración.

Los tipos de servicios intermediados son:

- ✓ Servicio de cambio de domicilio.

  Las diferentes administraciones públicas pueden hacer uso de este servicio, integrándolo en sus sistemas para que el ciudadano les notifique automáticamente su cambio de domicilio.

- ✓ Servicios de verificación y consulta de datos. Plataforma de intermediación.

  Mediante webservices podrá integrar en sus diferentes aplicaciones de administración electrónica el uso de múltiples servicios de verificación y consulta de datos disponibles.

El Ministerio de Hacienda y Administraciones Públicas es el responsable de la plataforma de intermediación de datos usando el protocolo SCSPv3. A través de ella, una Administración puede consultar de forma automatizada, desde una aplicación de gestión de un trámite adaptada para invocar los Webservice proporcionados por el servicio, cualquiera de los más de 30 certificados ofrecidos tales como datos de identidad y de residencia de un ciudadano, datos relativos al desempleo, titulaciones oficiales, datos catastrales, estar al corriente con la AEAT y TGSS, datos de pensiones, nacimiento, defunción y matrimonio de los Registros Civiles. Conviene matizar que la lista de certificados está en constante expansión.

La plataforma ha demostrado su efectividad y ha tenido una gran acogida entre los organismos habiéndose tramitado desde su puesta en producción más de 75 millones de consultas de datos generando un ahorro estimado desde 2007 de más de 100 millones de euros.

Protocolo SCSPv3

Proporciona un abanico completo de soluciones, con el objetivo de liberar al resto de Organismos y Administraciones Públicas de las tareas de desarrollo de aplicaciones de intercambio de datos y permitirlas centrarse en su negocio.

Para consumir estos servicios de manera fácil y sencilla se han desarrollado varias aplicaciones que forman parte del porfolio de soluciones: librerías SCSP, cliente ligero SCSPv3, recubrimiento SCSPv3 y aplicación de Administración y configuración SCSP:

- **Librerías SCSPv3**

  Son las librerías que implementan el protocolo SCSP tanto para requirentes como emisores, en concreto son varias aplicaciones desarrolladas por la **Dirección de Tecnologías de la Información y las Comunicaciones** del **Ministerio de Hacienda y Administraciones Públicas** que se pueden integrar en las aplicaciones de backoffice de los distintos organismos públicos y consultar los datos ofrecidos por emisores que cumplan con las especificaciones SCSP.

  Las funciones de las librerías SCSPv3 es soportar a requirentes y emisores, siendo las funcionalidades comunes las siguientes:

  - Composición de mensajes SCSPvX (v2/v3 según el certificado requerido)
  - Firma de mensajes SCSP (XMLDsig o WS-Security)
  - Cifrado de mensajes SCSP (si procede)
  - Almacenamiento histórico de mensajes y transmisiones
  - Envío de la petición al Endpoint de cada servicio
  - Recepción de mensajes SCSP y validación de los mismos según diferentes políticas configurables
  - Mecanismo de aceleración de las peticiones (cache de validación de certificados electrónicos con @firma)
  - Generación de justificantes pdf firmados electrónicamente de las transmisiones de datos realizadas de manera nativa para las librerías para todas las transmisiones
  - La configuración puede ser compartida por diferentes aplicaciones y se pueden configurar desde una aplicación externa.

  Las funcionalidades específicas del emisor son:

  - Autorización y Autentificación de Organismos Requirentes/Cesionarios
  - Comunicación con el BackOffice

  Los requisitos de funcionamiento son:

  - **Tecnología Java y Microsoft .net**
  - **Sistema operativo**: Windows 2000, Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows Server2008, Linux, MacOS X 10.5 y Sun Solaris / OpenSolaris 10.

- **Navegador web**: Firefox 2.0.20 o superior, Internet Explorer 5.5 o superior.
- **JRE** 1.6 o superior.
- **Bases de Datos**: Oracle 9, 10 o superior, SQLserver 2005 y 2008, Mysql 5 o superior, Postgresql 9 o superior.
- **Servidores de aplicación**: Tomcat 6.0.29 o superior, JBOSS 4.1, 5 o superior (a evaluar según las distintas versiones), IIS, Oracle OS. Para otros servidores de aplicación y versiones se puede evaluar por parte del equipo de desarrollo.
- **Certificados X509 reconocidos**: Se necesita conexión con la plataforma @firma y usar certificados reconocidos por esta plataforma. Para usar las librerías se recomienda un certificado de sello de órgano como se recoge en la Ley 11/2007. En el caso de usar el Cliente Ligero será necesario un certificado de servidor.

➢ **Cliente ligero web**

Complementariamente a las librerías se suministra (en la versión J2EE) una aplicación web completa, sencilla y funcional que permite a cualquier organismo consultar los certificados SCSPv3 disponibles sin necesidad de desarrollar nada, con las siguientes funcionalidades:

- Auditable, trazabilidad del funcionario que consulta
- Control detallado de usuarios y autorizaciones
- Control detallado de los procedimientos del organismo y matriz de autorización del organismo de los usuarios
- Transmisiones asíncronas por lotes mediante uso de plantillas excel adaptadas a cada certificado
- Exportación de los resultados de las transmisiones realizadas
- Obtención de Justificantes PDFs de las transmisiones realizadas
- Permite crear procedimientos en base a los cuales se realizan las consultas a los servicios SCSP, teniendo en cuenta que cualquier consulta se hará en base a un procedimiento administrativo
- Envío de peticiones síncronas y asíncronas a los servicios SCSP autorizados
- Envío de Peticiones Asíncronas "**MULTISOLICITUD**"
- Envío de Lotes de peticiones síncronas en aquellos servicios que no se implementan de manera asíncrona (AEAT, TGSS, INSS)
- Permite obtener respuestas a las peticiones asíncrona que ha realizado
- Consultar peticiones que se han realizado en un momento posterior
- Obtener justificantes pdf firmados electrónicamente de las transmisiones de datos realizadas
- Exportar las transmisiones a ficheros Excel

- **Recubrimiento SCSPv3**

  Permite que cualquier tipo de aplicación, independientemente de su tecnología, pueda usar las librerías SCSPv3 para consultar datos.

  Las ventajas del recubrimiento son

  - Simplificación del funcionamiento SCSP, firma y cifrado
  - Validación de esquemas
  - Registro de peticiones
  - Detección automática de las versiones configuradas de los servicios (versión SCSP, firma, cifrado)
  - Compatible con cualquier tipo de tecnología
  - Fácil y sencillo de usar

- **Aplicación de administración y configuración SCSP**

  Es una herramienta que permite la Instalación y configuración de las librerías SCSPv3 vía web desde cualquier equipo con conectividad a aquel en el que está desplegada la aplicación de administración.

  Los roles de administración son:

  - Administrador: Gestión de usuarios, configuración de emisores y requirentes SCSP y consulta de peticiones enviadas a los servicios.
  - Auditor: Consultar y controlar todas las operaciones que realizan los usuarios en el sistema y las peticiones realizadas a los servicios.
  - Interventor: Consultar las transmisiones de datos realizadas por el emisor o las recibidas en el caso de un requirente, que se han llevado a cabo por parte de cualquier funcionario.

  Las operaciones de cifrado y descifrado son opcionales en función de las características de los servicios, según requieran confidencialidad extremo a extremo y así haya sido definido por el emisor.

Elementos estándar del sistema

Para realizar todas las comunicaciones se plantea la utilización preferente de la red SARA entre organismos requirentes y emisores ya que todas las comunicaciones van encriptadas a nivel de enlace. Un organismo Emisor podría, por necesidades de su negocio, ofrecer los servicios a través de otras redes, públicas o privadas siendo el responsable de los mecanismos de seguridad que deba exigir.

Adicionalmente al uso de la red SARA para asegurar las comunicaciones a nivel de transporte entre los organismos, y permitir adicionalmente la identificación de las partes intervinientes en

la comunicación, las comunicaciones de los mensajes se realizarán a través de SSL, siendo el protocolo de transporte elegido HTTP.

Todas las comunicaciones realizadas entre un requirente y un emisor van firmadas digitalmente con el objetivo de garantizar la autenticación (identificación), no repudio e integridad de la información intercambiada.

Procedimiento de autorización de acceso a servicio de verificación y consulta de datos

Los participantes o roles son:

- ✓ Cedente: Será cualquier organización que posea datos relativos a los ciudadanos que otra pueda necesitar consultar en el ámbito del ejercicio de sus competencias; es el responsable de los mismos según la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y los ofrecerá a posibles Cesionarios a través de un Emisor.
- ✓ Emisor: Es el organismo público que ofrece el servicio o transmisión de datos. (Servidor), el que facilita la cesión de los datos desde un punto de vista tecnológico. Normalmente coincidirá con el cedente aunque no siempre.
- ✓ Cesionario: Cualquier organización autorizada a consultar determinados datos de los ciudadanos en poder de un Cedente.
- ✓ Requirente: Organismo que facilita la consulta de los datos desde un punto de vista tecnológico a un cesionario.
- ✓ Plataforma de Intermediación del MHAP: nodo de interoperabilidad que prestará funcionalidades comunes para el intercambio de información entre Emisores y Requirentes según el Real Decreto 4/2010, de 8 de enero.

Un organismo (cesionario) quiere consultar datos a través de un nodo de interoperabilidad que ofrece servicios como requirente. A nivel de SCSPv3 se dispone de la siguiente Información:

- Identificador de Solicitante: NIF del solicitante (cesionario)
- Nombre de Solicitante: Nombre del Solicitante (cesionario)
- Unidad Tramitadora: Nombre de la Unidad Tramitadora (cesionario)
- ID Expediente: Identificador del Expediente que genera o justifica la consulta
- Procedimiento: Código y Nombre del Procedimiento que genera o justifica la consulta

Al venir la petición firmada electrónicamente como mecanismo para garantizar la integridad, se dispone del NIF del "Requirente" que firmó la petición.

Por tanto, el requirente de la información pone la plataforma tecnológica y la aplicación que la soporta, implantará el control de acceso y autorizaciones de los usuarios de los organismos cesionarios y cada organismo cesionario solicitará la autorización de acceso en base a un procedimiento al servicio correspondiente.

Hay que tener en cuenta que obligatoriamente debe existir un procedimiento en el cual se requiere la aportación del dato a consultar por parte de los ciudadanos vinculado al organismo cesionario (cada procedimiento es individual para cada cesionario como responsable del mismo) y que se debe identificar a la aplicación que presta el servicio para el procedimiento y organismo cesionario concreto (este cesionario debe estar registrado en la tabla de autorizaciones).

Actualmente en la plataforma se valida lo siguiente en el emisor / cedente:

- Que el NIF del certificado con el que se firma está autorizado a acceder al servicio
- Que el NIF del certificado con el que se firma está autorizado a establecer conexión con el servicio SSL-Handshake.
- Que el NIF del certificado con el que se firma coincide con el valor del campo Identificador Solicitante para un servicio dado.
- Que el cesionario está autorizado al servicio
- Opcionalmente, que el procedimiento de la consulta está autorizado al servicio.

Para que el modelo funcione, adicionalmente a los requisitos que deben cumplir cada uno de los intervinientes, recogidos en la Norma Técnica de Interoperabilidad de Protocolos de intermediación de datos deberá establecerse un convenio de prestación de servicios entre el Requirente y los distintos cesionarios que deberá estar a disposición del Organismo Cedente, y del Emisor si así lo considera necesario el Cedente. Este convenio es el que da validez legal a la prestación de servicio, y permitirá que el Requirente preste servicios técnicos y se pueda considerar que solo existirá la cesión de datos a cada cesionario.

Funcionamiento:

El emisor (organismo encargado de suministrar la información) es responsable de:

- La definición y publicación de los servicios web (WSDL, XSD, etc.) cumpliendo con las especificaciones SCSP.
- Obtener la información de sus sistemas según las condiciones del servicio y devolverla en el mensaje de respuesta.
- Generación del Identificador de la transmisión efectuada y su marca de tiempo.
- Registrar las solicitudes recibidas y las transmisiones enviadas y almacenarlas el tiempo que requiere la ley.

El requirente (organismo encargado de pedir la información) se adaptará a las condiciones definidas por el emisor y será el responsable de:

- Consumir los servicios web (WSDL, XSD,...) cumpliendo con las especificaciones definidas.
- Generación del identificador de la petición enviada y de las solicitudes a incluir en dicha petición.
- Cumplimentar adecuadamente las peticiones enviadas garantizando la veracidad de los datos enviados, y la adecuación de los mismos.

- Registrar las solicitudes enviadas y las transmisiones recibidas y almacenarlas el tiempo que requiere la ley.

El protocolo SCSP está pensado para funcionar de manera síncrona o asíncrona. El funcionamiento síncrono es una simplificación del funcionamiento asíncrono.

En el modo síncrono se intercambian dos mensajes, petición y respuesta.

Una petición está compuesta por:

- Nodo Atributos, donde se describirán los datos de cada petición
  - Identificador de la petición
  - número de elementos
  - Marca de tiempo - timestamp-
  - Código único de certificado al que hace referencia la petición
- Nodo Estado, donde se describe el estado correspondiente a esa petición
- Nodo Solicitudes compuesto por
  - Lista solicitudes de transmisión
  - Solicitud de Transmisión que contendrá
    - los datos genéricos de cada solicitud. La estructura es común a todos los servicios que usen SCSP como protocolo de intercambio de datos
    - datos específicos de las mismas, particulares de cada Emisor/servicio

Las transmisiones de datos realizadas por los emisores deben de adoptar medidas técnicas y de organización necesaria que aseguren los aspectos siguientes: autenticidad, confidencialidad, integridad, no repudio, disponibilidad y conservación de la información.

Para hacerlo se hará uso del principio de proporcionalidad, es decir, que las medidas de seguridad deberán tener en cuenta el estado de la tecnología y ser proporcionadas a la naturaleza de los datos y de los tratamientos a proteger y a los riesgos a los que estén expuestos.

- La autenticidad de la información se garantizará por el uso de certificados X509v3 reconocidos y aceptados por todas las partes.
- La confidencialidad se conseguirá mediante el uso de SSL en las comunicaciones.
- Se podrá, adicionalmente garantizar la confidencialidad extremo a extremo mediante mecanismos de cifrado.
- La autenticidad y el No repudio se conseguirán mediante mecanismos de huella y firma electrónica.
- La disponibilidad se conseguirá mediante redundancia de los equipos
- La conservación de la información mediante mecanismos de almacenamiento y recuperación de información adecuados

Síncrono

Los tratamientos que se realizarán a la hora de enviar una petición/solicitud de datos por parte del requirente serán:

- Composición del mensaje

- Validación del esquema de petición (salida)
- Cifrado del mensaje si procede
- Firma de la petición a enviar
- Registro de la petición
- Envío de la petición
- Gestión de la respuesta (a definir en detalle)

Los tratamientos que se realizarán a la hora de recibir y procesar una petición/solicitud de datos por parte del emisor serán:

- Recepción del mensaje
- Validación de la Firma (autenticación y autorización del requirente)
- Descifrado del mensaje si procede
- Validación del esquema de petición (entrada)
- Registro de la petición recibida
- Gestión de la petición recibida (Tratamiento de la solicitud)
- Generación de la respuesta con el Identificador único de cada transmisión.
- Envío de la respuesta (a definir en detalle)

Los tratamientos que se realizarán a la hora de enviar una respuesta/transmisión de datos por parte del emisor serán:

- Generación de la respuesta con el Identificador único la transmisión
- Composición del mensaje de respuesta
- Validación del esquema de respuesta (salida)
- Cifrado del mensaje si procede (Ver información a cifrar)
- Firma de la respuesta a enviar (se firma la respuesta integra, nunca partes)
- Registro de la Transmisión (Generación de la traza correspondiente)
- Envío de la respuesta

Los tratamientos que se realizarán a la hora de recibir y procesar una respuesta/transmisión de datos por parte del requirente serán:

- Recepción del mensaje de respuesta
- Validación de la Firma (autenticación y autorización del emisor)
- Descifrado del mensaje si procede
- Validación del esquema de respuesta (entrada)
- Gestión de la respuesta recibida (Tratamiento de la respuesta por el organismo requirente)

Registro de la Transmisión (Generación de la traza correspondiente)

Las operaciones de cifrado y descifrado son opcionales en función de las características de los servicios, según requieran confidencialidad extremo a extremo por parte del emisor.

El Organismo Emisor definirá cual el su Tiempo Máximo de Respuesta en el funcionamiento síncrono, una vez superado el mismo, si se diera el caso, no generaría una transmisión válida, sino un error.

Asíncrono

Los tratamientos que se realizarán a la hora de enviar una petición/solicitud de datos asíncrona por parte del requirente serán:

- Composición del mensaje
- Validación del esquema de petición (salida)
- Cifrado del mensaje si procede
- Firma de la petición a enviar
- Envío de la petición

Los tratamientos que se realizarán a la hora de recibir y procesar una petición/solicitud asíncrona de datos por parte del emisor serán:

- Recepción del mensaje
- Validación de la Firma (autenticación y autorización del requirente)
- Descifrado del mensaje si procede
- Validación del esquema de petición (entrada)
- Registro de la petición
- Gestión de la petición recibida (Tratamiento de la solicitud y validaciones específicas) Generación de mensaje de confirmación de petición indicando el Tiempo Estimado de Respuesta (TER) en horas en las que podrá estar disponible la respuesta. El estado de la petición devuelto será “0002”, EN PROCESO.
- Composición del mensaje de confirmación de petición
- Validación del esquema de confirmación de petición (salida)
- Firma mensaje de confirmación de petición a enviar
- Registro del mensaje (Generación de la traza correspondiente)
- Envío del mensaje de confirmación de petición

Los tratamientos que se realizarán a la hora de gestionar la confirmación de petición remitida por el Emisor, por parte del requirente serán:

- Recepción del mensaje
- Validación de la Firma (autenticación y autorización del requirente)
- Validación del esquema de petición (entrada)
- Registro de la petición
- Gestión de la petición recibida (Tratamiento de la solicitud y validaciones específicas) Actualizar el estado de la petición a “0002”, EN PROCESO

Actualizar el valor de TER (Tiempo Estimado de Respuesta) para que el módulo de polling (del organismo requirente) solicite la respuesta.

Los tratamientos que se realizarán a la hora de solicitar una respuesta/transmisión de datos por parte del requirente serán:

- Verificar que ha vencido el Tiempo Estimado de Respuesta
- Composición del mensaje de Solicitud de respuesta
- Validación del esquema de Solicitud de respuesta (salida)
- Firma de la Solicitud de respuesta a enviar
- Registro de la Solicitud de respuesta (Generación de la traza correspondiente)
- Enviar un mensaje de Solicitud de Respuesta

Los tratamientos que se realizarán a la hora de recibir y procesar una Solicitud de Respuesta por parte del emisor serán:

- Recepción del mensaje de Solicitud de Respuesta
- Validación de la Firma (autenticación y autorización en el caso en el que requirente es el mismo que hizo la petición)
- Descifrado del mensaje si procede
- Validación del esquema de Solicitud de Respuesta (entrada)
- Registro del mensaje (Generación de la traza correspondiente)
- Gestión de la Solicitud de Respuesta recibida (verificación Tratamiento de la respuesta por el organismo requirente)

  Si la respuesta está disponible, se genera la respuesta completa. El valor del atributo Atributos\Estado\CodigoEstado ira fijado a “0003”, TRAMITADA.

  Si la respuesta no está disponible se genera una respuesta con el nodo Transmisiones vacío y se indicará un nuevo TER. El valor del atributo Atributos\Estado\CodigoEstado ira fijado a “0002” EN PROCESO.

- Registro de la Transmisión (Generación de la traza correspondiente)
- Envío de la Respuesta

Los tratamientos que se realizarán a la hora de recibir y procesar una respuesta/transmisión de datos por parte del requirente serán:

- Recepción del mensaje de respuesta Validación de la Firma (autenticación y autorización del emisor)
- Descifrado del mensaje si procede
- Validación del esquema de respuesta (entrada)
- Registro de la Transmisión (Generación de la traza correspondiente)
- Gestión de la respuesta recibida (Tratamiento de la respuesta por el organismo requirente)

Si la respuesta es definitiva, procesaremos la respuesta entera y se marcará como tramitada. En este caso el valor del atributo Atributos\Estado\CodigoEstado ira fijado a "0003" , TRAMITADA,
Si la respuesta no está disponible, actualizará la fecha del último sondeo y registrará el valor del nuevo TER que indica cuando deberá volver a enviar una nueva solicitud de respuesta. El valor del atributo Estado\CodigoEstado ira fijado a "0002" en proceso.
En caso de error se registrará en el sistema. Los requirentes podrán habilitar mecanismos de gestión de errores para reintentar una comunicación cuando el error obtenido sea subsanable (Error de comunicaciones, errores temporales de sistemas, etc..)

Mensajes intercambiados:

- **Mensaje de Petición SCSPv3**

Una petición está compuesta de:

- Atributos: contiene los datos de control relativos a toda la petición
- Solicitudes: contiene las Solicitudes de Transmisión (Nodo SolicitudTransmision) formadas por el bloque DatosGenericos y el bloque DatosEspecíficos.

La estructura de DatosGenericos recoge todas las consideraciones legales a tener en cuenta en la transmisión de datos entre Administraciones, registrando la información relativa a emisor, solicitante, titular y transmisión.

La estructura de DatosEspecíficos en la entrada contendrá los parámetros específicos de cada servicio, y será definida por el emisor.

Emisor: Organismo que proporciona la información. La identificación del Emisor estará formada por el NIF del emisor y su Nombre.

Es responsabilidad del requirente completar adecuadamente esta información ya que podría ser validada por el emisor y causa de rechazo de peticiones.

Solicitante: Organismo que solicita la información. La identificación del Solicitante estará formada por:

- Identificador del solicitante: NIF del organismo solicitante de la Información
- NombreSolicitante: Nombre del Organismo que solicita los datos.
- UnidadTramitadora: Se corresponde con la unidad de gestión autorizada a realizar la consulta y responsable de la tramitación administrativa a la que se refiere la consulta y la transmisión de datos. Tiene que tener la competencia del Procedimiento indicado en la solicitud.
- IdExpediente: Número de expediente, si lo hay, por el cual se realiza la consulta.
- CodProcedimiento: Código del Procedimiento para el que se autoriza al usuario/organismo a efectuar la consulta. Se recomienda usar códigos estandarizados

(SIA en el caso de la AGE, aunque dependerá del criterio del organismo emisor en función de los procedimientos de autorización que pudiera implementar)
- Nombre Procedimiento: Nombre del Procedimiento para el que se autoriza al organismo a efectuar la consulta
    - Funcionario: Datos identificativos del Funcionario
    - **Consentimiento**: Indica si se tiene consentimiento o no es necesario (consulta por ley)
    - Finalidad: Indica la descripción de la finalidad de la consulta.

Titular: Se refiere al "administrado" sobre quien se recaba Información. La identificación del titular estará formada por los siguientes campos en la parte genérica:

- Tipo Documentación: Tipo de documentación identificativa (Los valores aceptados a fecha 31-07-2011 son DNI, NIE, CIF, NIF o pasaporte) En caso de que se considerara otro valor se tendría que evaluar. No todos los valores están soportados por los distintos servicios/negocios teniendo que concretar en cada caso.
- Documentación: Indicará el valor de la documentación identificativa del titular sobre el que se quiere consultar la información. Los formatos serán los oficiales en cada caso concreto, según se indica en la tabla referente a formatos de los mensajes.
- Nombre Completo: Se recomienda usarlo sólo en el caso de Personas Jurídicas. En el caso de personas físicas se recomienda usar las etiquetas Nombre, y Apellido[1|2]. El organismo emisor puede establecer la obligatoriedad de incluir estos campos.
- Nombre: Nombre del titular de la solicitud. Se recomienda usar el mismo nombre que aparece oficialmente en la documentación acreditativa de la identidad de la persona, DNI, NIE, etc..
- Apellido1: Primer Apellido del titular de la solicitud. Se recomienda usar el mismo nombre que aparece oficialmente en la documentación acreditativa de la identidad de la persona, DNI, NIE, etc..
- Apellido2: Segundo Apellido del titular de la solicitud. Se recomienda usar el mismo nombre que aparece oficialmente en la documentación acreditativa de la identidad de la persona, DNI, NIE, etc.. si existe.

En caso de necesitar más elementos identificativos del Titular u otro dato de interés se tendrá que recoger en la parte de datos específicos.

Transmisión: Se refiere a la transmisión concreta realizada. La identificación de la transmisión efectivamente realizada estará formada por los siguientes campos en la parte genérica:

- Código Certificado: Código único que identifica el certificado o trasmisión de datos solicitada. Debe coincidir con el indicado en el nodo atributos.
- IdSolicitud: Identificador único de la solicitud incluido en la transmisión de datos. Lo indica el Requirente.
- IdTransmisión: Identificador único de la transmisión enviada por el emisor. En la petición vendrá vacío siendo ignorado por el emisor en otro caso. Permitirá acceder

a los datos de las transmisiones efectuadas por parte de los órganos de fiscalización a modo de CSV.

- FechaGeneracion: Indica la fecha en la que se generó la transmisión de datos.

➢ **Mensaje de Respuesta SCSPv3**

La respuesta estará formada por dos ramas de información, la rama definida como Atributos que contienen los datos de control relativos a toda la respuesta y la de Transmisiones.

La rama Transmisiones contiene las Transmisiones de Datos (Nodo Transmisión Datos) formadas por:

- Bloque Datos Específicos: La estructura en la respuesta contendrá los parámetros específicos de cada servicio, y será definida por el emisor.
- Bloque Datos Genéricos: La estructura de Datos Genéricos recoge todas las consideraciones legales a tener en cuenta en la transmisión de datos entre Administraciones, registrando la información relativa a:
    1. Emisor: Se refiere al organismo que proporciona la información. Igual que en petición
    2. Solicitante: Se refiere al Organismo que solicita la información. Igual que en petición
    3. Titular: Se refiere al "administrado" sobre quien se recaba Información. Igual que en petición.
    4. Transmisión: Se refiere a la transmisión concreta realizada. Igual que en petición.

La identificación de la transmisión efectivamente realizada estará formada por los siguientes campos en la parte genérica:

- Código Certificado: Código único que identifica el certificado o trasmisión de datos solicitada. Debe coincidir con el indicado en el nodo atributos.
- IdSolicitud: Identificador único de la solicitud incluido en la transmisión de datos. Lo indica el Requirente.
- IdTransmisión: Identificador único obligatorio de la transmisión enviada por el emisor. En la petición vendrá vacío siendo ignorado por el emisor en otro caso. Permitirá acceder a los datos de las transmisiones efectuadas por parte de los órganos de fiscalización a modo de CSV.
- Fecha Generación: Indica la fecha en la que se generó la transmisión de datos.

➢ **Mensaje de Confirmación de petición y de solicitud de respuesta SCSPv3**

Ambos mensajes, de confirmación de petición y de solicitud de respuesta se usarán en los servicios asíncronos como respuesta al mensaje de petición para indicar el tiempo en el que podría estar disponible la respuesta con las transmisiones de datos solicitadas.

La respuesta estará formada por la rama de información definida como Atributos que son los relativos a la petición recibida en caso de confirmación de petición y atributos relativos a la petición enviada en caso de solicitud de respuesta.

El mensaje de solicitud de

- IdPetición: Identificador de la petición realizada de transmisión de datos.
- NumElementos: Indica el número de elementos que forman parte de la petición. Debe coincidir con los indicados en la petición, en la respuesta y con el número de solicitudes y transmisiones a intercambiar.
- TimeStamp: Marca de tiempo en la que se ha realizado la solicitud de respuesta en formato: AAAA-MM-DDThh:mm:ss.mmm±hh:mm
- Estado: Bloque con la información de control.
- CódigoCertificado: Se refiere al Certificado de datos al que sustituye la transmisión.

Conclusiones

La auditoría se ha realizado en dos fases. En la primera se ha revisado toda la documentación jurídica y técnica relativa al establecimiento, finalidades, estándares y funcionamiento de la Plataforma de Intermediación.

En la segunda fase, se ha mantenido una reunión con los representantes de la Dirección de Tecnologías de la Información y las Comunicaciones, del Ministerio de Hacienda y Administraciones Públicas, que es la unidad responsable de la gestión y mantenimiento de la Plataforma de Intermediación, al objeto de aclarar algunas dudas extraídas de la revisión realizada y comprender el funcionamiento de la plataforma.

Como conclusiones, en primer lugar hay que señalar que la creación y los servicios ofrecidos en la Plataforma de Intermediación tienen la cobertura legal necesaria a través de las distintas normas que se han indicado en la introducción del presente documento y a lo largo del mismo.

Además, se ha constatado que los procedimientos de adhesión a los servicios de la plataforma están formalmente definidos y, cuando se trata de Administraciones distintas de la AGE, conllevan la firma de un convenio en el que claramente se especifica que cuando se requieran datos a través de la Plataforma, la Administración cesionaria, bien por sí misma o a través de un requirente, ha de verificar que se dan todas las condiciones legales para que la consulta sea correcta, y en particular consta que es necesario el consentimiento del ciudadano sobre el que se va a realizar la consulta electrónica de verificación de datos antes de que se ejecute el proceso. Esta verificación es la que se realiza a través de la plataforma.

En este punto merece la pena resaltar que a partir de la entrada en vigor de la nueva Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas, y de acuerdo con lo establecido en su artículo 28 "… 2. *Los interesados no estarán obligados a aportar documentos que hayan sido elaborados por cualquier Administración, con*

independencia de que la presentación de los citados documentos tenga carácter preceptivo o facultativo en el procedimiento de que se trate, siempre que el interesado haya expresado su consentimiento a que sean consultados o recabados dichos documentos. Se presumirá que la consulta u obtención es autorizada por los interesados salvo que conste en el procedimiento su oposición expresa o la ley especial aplicable requiera consentimiento expreso. En ausencia de oposición del interesado, las Administraciones Públicas deberán recabar los documentos electrónicamente a través de sus redes corporativas o mediante consulta a las plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto".

Por lo tanto, las Administraciones que actúen como cesionarias (bien por sí mismas o a través de las Administraciones requirentes) deberán adecuar sus procedimientos y formularios para que en ellos figure, de forma expresa, la opción para que el ciudadano pueda manifestar su oposición a la consulta u obtención de los documentos obrantes en otras Administraciones e indicando que desea aportarlos él mismo al procedimiento.

Así pues, como conclusión final, tras la revisión de la documentación relevante y las entrevistas mantenidas con los responsables de la Plataforma de Intermediación, se puede concluir que en el momento actual y según la información aportada por los responsables de la plataforma, los procedimientos y operaciones de la misma se desarrollan respetando la legislación española de protección de datos.