Especificación funcional del protocolo de Sustitución de Certificados en Soporte Papel SCSPv3.3. Agencia Estatal de Administración Digital





HISTÓRICO DE VERSIONES

Fecha	Versión	Descripción
21/07/2011	1.0	Creación 1ª versión consolidada de SCSPv3 partiendo de la Especificación funcional y técnica de SCSPv2
18/07/2016	1.1	Se hace referencia a la norma NIT para la seguridad y trazabilidad
08/03/2017	1.2	Ampliación protocolo SCSPv3
11/01/2018	1.3	Se corrige el patrón del código de Unidad Tramitadora (DIR3)
30/05/2018	1.4	Se establece como obligatorios los tags CodigoUnidadTramitadora y UnidadTramitadora
11/02/2019	1.5	Se añaden los nodos ClaseTramite y Automatizado
10/04/2019	1.6	Se añade el tipo de consentimiento “NoOpo”
02/09/2019	1.7	Se especifica de una forma más clara el tipo de algoritmo para el nodo transform de las firmas WsSecurity
16/09/2020	1.8	Cambio en el NifFuncionario
24/11/2020	1.9	Se modifica el nombre del fichero
11/11/2021	1.10	• Se corrigen erratas • Se especifica el tag Automatizado y ClaseTramute como opcional • Se ajustan los códigos de ClaseTramite de acuerdo a la codificación SIA • Aclaración acerca de los tags opcionales/obligatorios
22/11/2021	1.11	• Se añade la ClaseTramite 0 • Se añade la ClaseTramite 99
09/12/2024	1.12	Se aumenta a 250 caracteres el tag NombreProcedimiento
17/07/2025	1.13	Se corrigen erratas
21/01/2026	1.14	• Se añade la ClaseTramite 35 • Se añade la ClaseTramite 36

DOCUMENTACIÓN RELACIONADA

Nombre del documento	Versión	Descripción
Especificacion tecnica esquemas formatos SCSPv3.3.pdf	1.22	Especificación técnica SCSPv3.3
NTI_PID_BOE-A-2012-10049.pdf		Norma Técnica de Interoperabilidad
EF_elimin_certificados_4-2.pdf	4.2	Especificación functional SCSPv2

Índice

INDICE DE FIGURAS **4**

1. INTRODUCCIÓN **5**

2. DESCRIPCIÓN DEL PROTOCOLO SCSP **6**

2.1 Características generales del protocolo SCSPv3.3 7
2.2 Roles definidos en el protocolo SCSPv3.3 8
2.3 Modos de funcionamiento del protocolo 9
2.4 Tratamiento de las transmisiones de datos por parte de los requirentes/emisores 10
2.4.1 Funcionamiento síncrono *10*
2.4.2 Funcionamiento asíncrono *11*

3. ELEMENTOS estándar DEL SISTEMA **14**

3.1 Red SARA 14
3.2 Protocolo de comunicaciones HTTPS 14
3.3 Uso de la firma digital para identificación 14
3.3.1 Certificados X.509 v3 reconocidos y aceptado por @Firma *14*
3.3.2 Formato de firma *14*
3.3.3 Modificación del formato de firma *15*
3.4 Uso de esquemas 16
3.4.1 Espacio de nombres *16*
3.5 Mecanismo de autorización 17
3.5.1 Alternativas de autorización *17*
3.5.2 Nodos de interoperabilidad *17*
3.6 Identificadores de petición 18
3.6.1 Identificadores de solicitud *18*
3.6.2 Identificadores de transmission *18*
3.7 Seguridad y trazabilidad 19
3.8 Obligaciones en interoperabilidad 20
3.9 Cifrado de mensajes 21
3.9.1 Tokens de seguridad WS-Security *22*

4. MENSAJES INTERCAMBIADOS **24**

4.1 Mensaje de petición SCSPv3.3 24
4.1.1 Emisor *25*
4.1.1 Solicitante *25*
4.1.2 Titular *29*
4.1.3 Transmisión *30*
4.2 Mensaje de respuesta SCSPv3.3 31
4.2.1 Emisor *32*
4.2.2 Solicitante *32*
4.2.3 Titular *32*
4.2.4 Transmisión *32*
4.3 Mensaje de confirmación de petición SCSPv3.3 33
4.4 Mensaje de solicitud de respuesta SCSPv3.3 34
4.5 Datos específicos 35

5. GESTIÓN DE ERRORES **36**

6. ANEXO I: WSDL Y XSD (FORMATOS Y ESQUEMAS) **37**

7. ANEXO II: DEFINICIONES RELEVANTES **38**

INDICE DE FIGURAS

Imagen 1.- Diagrama de petición SCSPv3.3 24
Imagen 2.- Diagrama de petición SCSPv3.3 – Emisor 25
Imagen 3.- Diagrama de petición SCSPv3.3 - Solicitante 28
Imagen 4.- Diagrama de petición SCSPv3.3 – Titular 29
Imagen 5.- Diagrama de petición SCSPv3.3 – Transmisión 30
Imagen 6.- Diagrama de respuesta SCSPv3.3 31
Imagen 7.- Diagrama de respuesta SCSPv3.3 - Transmisión 32
Imagen 8.- Diagrama de confirmación de petición SCSPv3.3 33
Imagen 9.- Diagrama de solicitud de respuesta SCSPv3.3 34
Imagen 10.- Diagrama de datos específicos SCSPv3.3 35

1. INTRODUCCIÓN

El presente documento describe la especificación funcional del protocolo Sustitución de Certificados en Soporte Papel, adelante SCSP, Versión 3.3.

El objetivo de este protocolo es la utilización de la transmisión de datos como medio estándar de sustitución de certificados en papel mediante la definición del formato de información tanto requerida como suministrada de manera general, y en la parte correspondiente a cada servicio de manera específica, entre AAPPs para cumplir con la normativa vigente en la que no se puede pedir documentación a los ciudadanos que ya obre en poder de las AAPPs. Tomando como referencia la versión de SCSPv3 vigente desde el año 2014 en su uso en muchos servicios se ha puesto en evidencia una serie de carencias o mejoras necesarias que han desembocado en una ampliación de la versión 3 de SCSP.

- La versión SCSPv3.1 ampliada incorpora las siguientes novedades con respecto a la versión SCSPv3:
  - ✓ Nuevo campo SeudonimoEmpleadoPublico, existe la necesidad en algunos casos de no identificar el funcionario que realiza la consulta sino enviar su seudónimo según el RD 668/2015 de 17 de Julio.
  - ✓ Nuevo campo CodigoUnidadTramitadora, existe la necesidad de identificar a la Unidad Tramitadora que realiza la consulta por ello se ha introducido este campo para identificarla con su código DIR3.
  - ✓ Se aumenta la longitud del campo IdExpediente hasta los 65 caracteres.
  - ✓ Se aumenta el campo LiteralError hasta 1024 posiciones para permitir descripciones más descriptivas de los estados o errores devueltos.
  - ✓ Se detallan los tipos de documentación admitidos y los formatos de documentación que corresponde a cada uno de ellos.
  - ✓ Se añaden los tipo de documentación **NumeroIdentificacion**, **Otros y CSV** (Código seguro de verificación)
  - ✓ Se aumenta el campo Documentacion hasta los 30 caracteres para permitir Pasaportes con esta longitud.
  - ✓ Obligatoriedad de la inclusión del procedimiento que permite la consulta, se ha especificado como obligatorio los campos que identifican el procedimiento que permite realizar la consulta de datos.
  - ✓ Se introduce los datos del Solicitante en la Solicitud de Respuesta para identificar el organismo que la realiza unívocamente en caso de Nodos de Interoperabilidad.
  - ✓ Se añaden recomendaciones a la hora de generar los datos específicos de cada uno de los servicios.
  - ✓ Se añaden recomendaciones a la hora de generar el WSDL de cada servicio ofrecido SCSPv3.1.
  - ✓ Se añade el tag ClaseTramite
  - ✓ Se añade el tag Automatizado

- La versión SCSPv3.2 ampliada incorpora las siguientes novedades con respecto a la versión SCSPv3.1:
  - ✓ Se aumenta el tag NombreProcedimiento a 250 caracteres

- La versión SCSPv3.3 ampliada incorpora las siguientes novedades con respecto a la versión SCSPv3.2:
  - ✓ Se añade la clase de trámite 35 – Plazas educativas, matrículas y otras gestiones académicas n.c.o.p.
  - ✓ Se añade la clase de trámite 36 – Plazas e inscripciones no académicas.

2. DESCRIPCIÓN DEL PROTOCOLO SCSP

La especificación del protocolo SCSP define los siguientes elementos:

- ✓ Descripción general del protocolo y su funcionamiento
  - Roles
    - Requirente (cliente)
    - Emisor (solicitante)
  - Modos de funcionamiento
    - Síncrono
    - Asíncrono
- ✓ Tratamiento de las solicitudes y transmisiones de datos por parte de los requirentes/emisores
  - Composición de los mensajes.
  - Validación del esquema.
  - Firma y validación de la firma y del certificado con el que se firmó.
  - Cifrado y descifrado del mensaje si procede.
- ✓ Descripción de los mensajes intercambiados que conforman el protocolo y de los formatos de campos especificados:
  - Petición
  - Respuesta
  - Confirmación de petición
  - Solicitud de respuesta
  - Datos específicos
  - SOAP Fault

Esta especificación persigue definir de manera exhaustiva un modelo de intercambio estandarizado de información entre administraciones públicas al objeto de suprimir los certificados en soporte papel.

Para complementar este documento se han generado también el siguiente documento específico:

- ✓ Especificacion-Funcional_Esquemas_formatos_SCSP_v3.doc ➔ Descripción de los esquemas (ficheros XSD) de los mensajes intercambiados, formatos de los tipos de datos de cada atributo y ejemplos de cada tipo de mensaje.

2.1 Características generales del protocolo SCSPv3.3

El protocolo SCSP establece las siguientes premisas.

- ✓ Formato estandarizado XML para las transmisión de estos datos, y protocolo SOAP para su transmisión. Estandarización de formatos para datos comunes a todos los certificados a sustituir, libertad de formato para los datos específicos de cada uno. Se definen en concreto en el apartado de mensajes.
- ✓ El protocolo de transporte será HTTP(**S**).
- ✓ La confidencialidad de la información se realizará en base a interconexión de servidores utilizando protocolo TLS/SSL.
- ✓ Servicios Web XML para el acceso a los datos, estilo de llamada basada en documentos XML.
- ✓ La publicación y realización de los esquemas (XSD) y descripción de los servicios (WSDL) para cada servicio web, será responsabilidad de cada Organismo Emisor. Debe respetarse los mensajes estándar, petición, respuesta, confirmación de petición, solicitud de respuesta y Soap Fault. De cara a facilitar la distribución, y complementario al directorio de servicios responsabilidad de cada organismo emisor, existirá un Directorio adicional centralizado en el MINHAFP.
- ✓ Control de acceso al sistema mediante certificados X.509 v3 reconocidos y firma electrónica avanzada, para asegurar los siguientes aspectos: autenticidad, confidencialidad, disponibilidad y conservación de la información.
- ✓ El protocolo permitirá funcionamiento tanto síncrono como asíncrono.
- ✓ El modelo de peticiones simples podrá utilizar el modelo asíncrono de trasmisión como mecanismo de contingencia, pero nunca al contrario.
- ✓ El mecanismo de llamada y obtención de respuesta, para el proceso asíncrono, estará basado en polling.
- ✓ El modelo de peticiones múltiples-asíncronas hará referencia a un único tipo de certificado en cada petición.
- ✓ La respuesta recibida en el modelo de peticiones múltiples-asíncronas es única para cada petición. Las respuestas deben contener tantas transmisiones como solicitudes contuviera la petición, con independencia del número de ellas que se hayan resuelto correctamente.
- ✓ Los errores que se puedan generar durante la utilización del sistema se transmitirán utilizando el estándar SOAP Fault. Es decir, si alguna solicitud provoca un error SOAP Fault entonces únicamente se devuelve éste objeto, no un mensaje de respuesta (No se retorna el valor de las que se procesaron correctamente). En caso de que alguna de las solicitudes incluidas dentro de la petición conlleve la asignación de un nuevo Tiempo Estimado de Respuesta (TER), entonces se devolverá un mensaje de respuesta sin transmisiones con el nuevo TER y en donde el nodo **NumElementos** tendrá el valor 0.

  Las transmisiones con errores que vayan incluidas en respuestas asíncronas correctas lo indicarán en el campo de datos específicos.

  - Si alguna de las transmisiones devolviera un código de error SOAP Fault en la respuesta asíncrona, este se devolverá como código de respuesta.
  - Si todas las transmisiones devolvieran el **mismo** SOAP Fault, únicamente se devolverá un SOAP Fault correspondiente a todas las transmisiones.

2.2 Roles definidos en el protocolo SCSPv3.3

El protocolo SCSP contempla dos roles fundamentales, el rol de **emisor** y el de **requirente**.
Se entiende por Emisor al organismo encargado de suministrar la información y 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 (backoffice) según las condiciones del servicio y devolverla en el mensaje de respuesta.
- ✓ Generación del Identificador de la transmisión efectuada y su marca de tiempo.
- ✓ En el caso de ofrecer un servicio asíncrono definir en número de Solicitudes máximo que acepta el servicio. Se recomienda no superar las 1000 solicitudes. En algunos casos hay emisores que han fijado su valor a 100 solicitudes.
- ✓ Registrar las solicitudes recibidas y las transmisiones enviadas y almacenarlas el tiempo que requiere la ley.

Se entiende por Requirente al organismo encargado de pedir la información. Se adaptará a las condiciones definidas por el Emisor. 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 tal y como se desarrolla en los siguientes apartados.
- ✓ Registrar las solicitudes enviadas y las transmisiones recibidas y almacenarlas el tiempo que requiere la ley.

2.3 Modos de funcionamiento del protocolo

El protocolo de Sustitución de Certificados en soporte Papel (SCSP) está pensado para funcionar tanto de manera síncrona como de manera asíncrona. El funcionamiento síncrono es una simplificación del funcionamiento asíncrono.

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

Una petición estará compuesta por un 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 y nodo Estado con la descripción del estado correspondiente a esa petición) y el nodo Solicitudes.

El nodo solicitudes estará compuesto por la lista de solicitudes de transmisión, "**SolicitudTransmision**" que contendrá los datos genéricos de cada Solicitud y los datos específicos de las mismas.

La estructura de los datos genéricos será común a todos los servicios que usen SCSP como protocolo de intercambio de datos, mientras que los datos específicos serán particulares de cada Emisor/Servicio.

En general una petición estará identificada con un ID único que cada Emisor validará que no esté repetido. (Atributos➔IdPeticion)

Cada petición podrá tener tantas solicitudes (Identificadas unívocamente dentro de la petición) como soporte el servicio, y se indicará en el campo "NumElementos".
Cada respuesta tendrá tantas transmisiones como solicitudes haya recibido.

Cada transmisión de datos contendrá la siguiente información:

1. Identificador único de la trasmisión generados por el emisor y el timestamp de cuando se ha generado.
2. Datos de negocio de la respuesta (Datos específicos).

2.4 Tratamiento de las transmisiones de datos por parte de los requirentes/emisores

Las transmisiones de datos realizadas deben de adoptar medidas técnicas y de organización necesaria que aseguren los aspectos siguientes:

- Autenticidad
- Confidencialidad
- Integridad
- No Repudio
- Disponibilidad
- 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

2.4.1 Funcionamiento síncrono

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

1. Composición del mensaje.
2. Validación del esquema de petición (salida).
3. Cifrado del mensaje si procede.
4. Firma de la petición a enviar.
5. Registro de la petición.
6. Envío de la petición.
7. 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:

1. Recepción del mensaje.
2. Validación de la firma (autenticación y autorización del requirente).
3. Descifrado del mensaje si procede.
4. Validación del esquema de petición (entrada).
5. Registro de la petición recibida.
6. Gestión de la petición recibida (tratamiento de la solicitud).
7. Generación de la respuesta con el identificador de cada transmisión.
8. 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:

1. Generación de la respuesta con el identificador de la transmisión.
2. Composición del mensaje de respuesta.
3. Validación del esquema de respuesta (salida).
4. Cifrado del mensaje si procede (ver información a cifrar).
5. Firma de la respuesta a enviar (se firma la respuesta íntegra, nunca partes de ella).
6. Registro de la transmisión (generación de la traza correspondiente).
7. Envío de la respuesta.

En el caso en el que se produzca un error en cualquiera de los pasos indicados por parte del emisor se devolverá una respuesta de tipo SOAP Fault. La especificación de los errores posibles se detalla en el documento de Especificación de errores SOAPFAULT SCSP v3. Si el procesamiento ha sido correcto se devolverá en el nodo peticion➔Atributos➔CodigoEstado el valor “0003” TRAMITADA.

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

1. Recepción del mensaje de respuesta.
2. Validación de la firma (autenticación y autorización del emisor).
3. Descifrado del mensaje si procede.
4. Validación del esquema de respuesta (entrada).
5. Gestión de la respuesta recibida (tratamiento de la respuesta por el organismo requirente).
6. 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 cuál es su Tiempo Máximo de Respuesta en el funcionamiento síncrono, tal que superado el mismo, si se diera el caso, no generaría una transmisión válida, sino un error.

2.4.2 Funcionamiento asíncrono

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

1. Composición del mensaje.
2. Validación del esquema de petición (salida).
3. Cifrado del mensaje si procede.
4. Firma de la petición a enviar.
5. 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:

1. Recepción del mensaje.
2. Validación de la Firma (autenticación y autorización del requirente).
3. Descifrado del mensaje si procede.
4. Validación del esquema de petición (entrada).
5. Registro de la petición.
6. Gestión de la petición recibida (tratamiento de la solicitud y validaciones específicas).
7. 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"**.
8. Composición del mensaje de confirmación de petición.
9. Validación del esquema de confirmación de petición (salida).
10. Firma mensaje de confirmación de petición a enviar.
11. Registro del mensaje (generación de la traza correspondiente).
12. 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:

1. Recepción del mensaje.
2. Validación de la Firma (autenticación y autorización del requirente).
3. Validación del esquema de petición (entrada).
4. Registro de la petición.
5. Gestión de la petición recibida (Tratamiento de la solicitud y validaciones específicas).
   5.1. Actualizar el estado de la petición a "**0002**", "**EN PROCESO"**.
   5.2. 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:

1. Verificar que ha vencido el Tiempo Estimado de Respuesta.
2. Composición del mensaje de Solicitud de respuesta.
3. Validación del esquema de Solicitud de respuesta (salida).
4. Firma de la Solicitud de respuesta a enviar.
5. Registro de la Solicitud de respuesta (Generación de la traza correspondiente).
6. 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:

1. Recepción del mensaje de Solicitud de Respuesta.
2. Validación de la Firma (autenticación y autorización en el caso en el que requirente es el mismo que hizo la petición).
3. Descifrado del mensaje si procede.
4. Validación del esquema de Solicitud de Respuesta (entrada).
5. Registro del mensaje (generación de la traza correspondiente).
6. Gestión de la Solicitud de Respuesta recibida (verificación tratamiento de la respuesta por el organismo requirente).
   6.1. Si la respuesta está disponible, se genera la respuesta completa. El valor del atributo Atributos➔Estado➔CodigoEstado ira fijado a "**0003**", "**TRAMITADA**".
   6.2. 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**".
7. Registro de la Transmisión (generación de la traza correspondiente).
8. 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:

1. Recepción del mensaje de respuesta.
2. Validación de la Firma (autenticación y autorización del emisor).
3. Descifrado del mensaje si procede.
4. Validación del esquema de respuesta (entrada).
5. Registro de la Transmisión (generación de la traza correspondiente).
6. Gestión de la respuesta recibida (tratamiento de la respuesta por el organismo requirente).
   6.1. 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**".
   6.2. 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**".
   6.3. 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...)

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.

3. ELEMENTOS ESTÁNDAR DEL SISTEMA

Conforme a la especificación funcional el sistema requiere de la definición de una serie de características esenciales que cualquier organismo ha de cumplir independientemente de que realice su propia implementación de la especificación o utilice las librerías ya desarrolladas por la AEAD.

Estas características esenciales abarcan desde especificaciones de arquitectura de sistema, especificaciones de interoperabilidad en las comunicaciones hasta requisitos de seguridad y trazabilidad. Seguidamente se resumen las características estándar y posteriormente se detallarán en mayor medida.

3.1 Red SARA

Se plantea la opción utilización preferente de la Red SARA para realizar todas las comunicaciones entre organismos requirentes y emisores. El uso de esta red es debido a la seguridad ofrecida en las comunicaciones debido a 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.

3.2 Protocolo de comunicaciones HTTPS

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 SOAP se realizarán a través de TLS/SSL. Siendo el protocolo de transporte elegido HTTPS.

3.3 Uso de la firma digital para identificación

Todas las comunicaciones realizadas entre un requirente y un emisor irán firmadas digitalmente con el objetivo de garantizar la autenticación (identificación), no repudio e integridad de la información intercambiada. El proceso de firma a realizar seguirá las siguientes pautas.

3.3.1 Certificados X.509 v3 reconocidos y aceptado por @Firma

La firma se realizará utilizando certificados X.509 v3 según la normativa vigente. Estos certificados identificarán a las máquinas de cada organismo (requirente o emisor) intervinientes en la comunicación. Siendo responsabilidad por tanto de cada organismo de su uso.

Estos certificados podrán ser emitidos por cualquier Autoridad de Certificación reconocida tanto por el emisor como por el requirente.

3.3.2 Formato de firma

Por motivos de interoperabilidad con los estándares actuales más modernos, se ha optado por sustituir el mecanismo de firma basado en XML-DSig puro, por el especificado dentro de la familia WS-Security. Se permitirá, en caso de no necesitar cifrado, por temas de compatibilidad hacia atrás, el usar versión 3 de SCSP con XMLDsig aunque no es la opción recomendada.

Se seguirán utilizando los mismos algoritmos matemáticos que en la versión 2 si bien los sistemas deberán estar preparados para soportar algoritmos más seguros de firma y huella digital (digest).

A continuación se detallan los algoritmos usados para el proceso de firmado, incluyendo los algoritmos relacionados con las transformaciones, procesos de canonicalización, etc... involucrados en la misma.

Se firmará todo el body, no descartándose, que por motivos de cada servicio, adicionalmente se deba firmar algún otro elemento. Los objetos firmados serán la Petición, y la Respuesta.

Los algoritmos utilizados en el proceso de firma serán:

```
DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"
CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
```

Aunque existen otros mecanismos definidos por el estándar WS-Security, el mecanismo de acceso a los elementos de seguridad (utilizados para la firma y el cifrado en WS-security) será por referencia a un **BinarySecurityToken** (**wsse:SecurityTokenReference**).

El formato de firma digital, en el caso de utilizar XML-Dsig será el XML Digital Signature definido por la W3C (http://www.w3.org/TR/xmldsig-core). Donde el algoritmo de canonicalización y transformación a utilizar por razones de interoperabilidad será **http://www.w3.org/2001/10/xml-exc-c14n**.

3.3.3 Modificación del formato de firma

Por motivos de seguridad se podrían cambiar los mecanismos relativos a la firma, algoritmos de huella, firma, etc.
En caso de que sea necesario este cambio se acordará mediante el grupo de trabajo de Sustitución de certificados/intercambio de datos buscando una amplia aceptación.

En cualquier caso, los formatos de firma indicados son un conjunto mínimo, pudiendo un emisor aceptar libremente más formatos de firma, siempre que sean reconocidos por la política de firma del organismo, siendo igualmente válidos.

3.4 Uso de esquemas

Cualquier organismo que decida realizar la implementación de estas especificaciones deberá adecuar el formato de los mensajes intercambiados a los esquemas definidos en el presente documento. Dicha definición se encuentra en el apartado 9 de este documento. El objeto de estos esquemas es determinar el formato de los mensajes intercambiados y supone un estándar de comunicación para el intercambio de datos entre requirentes y emisores.

3.4.1 Espacio de nombres

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 decidido sustituir los namespaces referentes a **www.map.es** por intermediacion.redsara.es para hacerlos independientes de la nomenclatura de los organismos que los usan, e indicar el hecho de que la versión soportada es adecuada para la intermediación.
También se ha cambiado el versionado de los esquemas, dejándose intactos los datos específicos, que dependen de cada negocio.

A este objeto se ha elegido como raíz la siguiente URI:

http://intermediacion.redsara.es/scsp/esquemas/

A partir de esta referencia, y actualizando el índice de versión V3 (versión 3) de los esquemas, se tienen los siguientes namespaces de uso obligatorio:

Mensajes generales:

Petición ➔ http://intermediacion.redsara.es/scsp/esquemas/V3/peticion/
Confirmación de petición ➔ http://intermediacion.redsara.es/scsp/esquemas/V3/confirmacionPeticion/
Solicitud de respuesta➔ http://intermediacion.redsara.es/scsp/esquemas/V3/solicitudRespuesta/
Respuesta ➔ http://intermediacion.redsara.es/scsp/esquemas/V3/respuesta
SOAP Fault Atributos ➔ http://intermediacion.redsara.es/scsp/esquemas/V3/soapfaultatributos/

Mensajes específicos:

Datos específicos ➔ http://intermediacion.redsara.es/scsp/esquemas/datosespecificos

3.5 Mecanismo de autorización

Los organismos emisores tienen que disponer de mecanismos que permitan la definición de políticas de autorización para el control de los requirentes a la hora de solicitar un certificado. De tal forma se define la necesidad de la existencia dentro del organismo emisor de un sistema para la autorización de los requirentes, ya sea a través de una tabla de autorizaciones o haciendo uso de cualquier otro mecanismo.

El objetivo es autorizar a los requirentes a pedir sólo los certificados a los cuales se les habilita y no a otros.

3.5.1 Alternativas de autorización

Con el fin de tener una amplia capacidad de autorización se tendrán en cuenta los siguientes elementos a la hora de autorizar el acceso a un servicio.

- ✓ Canal de comunicación mediante identificación TLS/SSL de cliente.
- ✓ Firma electrónica de las peticiones.
- ✓ Atributos específicos del solicitante definidos en el protocolo (*IdentificadorSolicitante*)
- ✓ Otros atributos contemplados en el mensaje de petición.

Se recomienda ser lo suficientemente flexibles como para permitir la prestación de servicios por Nodos de Interoperabilidad.

3.5.2 Nodos de interoperabilidad

Cuando un Organismo preste servicios como "**Nodo de Interoperabilidad**" reconocido en el *ENI RD 4/2010*, firmará las peticiones con un certificado que le identifique a él como requirente o emisor según el caso.
En el caso de comportarse como requirente, el campo *IdentificadorSolicitante* llevará el NIF/CIF del organismo cesionario que usa los servicios del nodo de interoperabilidad.
En las etiquetas:

- ✓ NombreSolicitante ➔ Nombre del organismo cesionario que solicita los datos
- ✓ UnidadTramitadora ➔ Unidad gestora del Organismo Cesionario
- ✓ CodigoUnidadTramitadora ➔ Código de la unidad gestora del Organismo Cesionario (DIR3)

3.6 Identificadores de petición

Para poder realizar una trazabilidad de las peticiones tanto recibidas como emitidas en un requirente o emisor, se define un identificador de petición que servirá cómo identificador único de una transmisión emitidas desde un requirente a un emisor o a la inversa.
Para garantizar la unicidad de los identificadores de petición para todos los organismos requirentes de un servicio este Identificador deberá tener una parte que identifique unívocamente al organismo.

Como recomendación, dicho identificador de petición estará formado por la concatenación de:

- ✓ Un identificador único del organismo (por ejemplo el acrónimo del organismo)

Y un número secuencial de petición y cuya longitud total no exceda de la longitud del campo, el número secuencial podrá ser alfanumérico.

Éste identificador de petición "***único***" será generado por el organismo requirente para identificar sus peticiones siendo necesario que el organismo emisor almacene dicho identificador junto con la petición para mantener la trazabilidad de las peticiones.

3.6.1 Identificadores de solicitud

Dentro de cada petición, podrán ir una o más solicitudes. En el caso de peticiones síncronas solo habrá una solicitud. En el caso de peticiones asíncronas, podrán ir más solicitudes y existirá un identificador único de cada solicitud por cada petición generada.

3.6.2 Identificadores de transmission

En la petición, dentro de cada solicitud, este valor será nulo, en caso de no serlo no se tendría en cuenta por el emisor.

En la respuesta, para garantizar los mecanismos de auditoría y trazabilidad, el emisor generará un Identificador único de cada transmisión realizada por él, para cada tipo de certificado. Este identificador único se podrá usar a modo de "***Código Seguro de Verificación***" o referencia de la transmisión realizada por el emisor y podrá ser verificada por los órganos de fiscalización, control y auditoría correspondientes.

3.7 Seguridad y trazabilidad

Todos los organismos tanto requirentes como emisores mantendrán trazabilidad de los intercambios de datos producidos, para lo cual podrán apoyarse en funcionalidades prestadas por la Plataforma de intermediación de la Agencia Estatal de Administración Digital, y en lo previsto sobre trazabilidad en la *Norma Técnica de Interoperabilidad de Protocolos de intermediación de datos*, aprobada por Resolución de 28 de junio de 2012, de la Secretaría de Estado de Administraciones Públicas.

3.8 Obligaciones en interoperabilidad

Debido a las diferentes tecnologías existentes en la actualizar cualquiera de los servicios ofrecidos por un emisor han de cumplir con una serie de requisitos de interoperabilidad.

Los requisitos mínimos que han de ofrecer los servicios son:

- ✓ Dentro del fichero de definición del servicio (WSDL) se incluirán las referencias import a los esquemas petición, respuesta, solicitud de respuesta, confirmación de petición y datos específicos. Igualmente los esquemas que definen el formato de los mensajes intercambiados no deberán incluir sentencias import a otros esquemas distintos de los especificados en este documento.

- ✓ Algoritmo de transformación y canonicalización. Es necesario que el algoritmo sea:

http://www.w3.org/2001/10/xml-exc-c14n

- ✓ Los servicios publicados cumplirán el estándar WS-I de interoperabilidad de servicios.

3.9 Cifrado de mensajes

Los mecanismos de cifrado se utilizarán en aquellas situaciones que el emisor lo considere necesario por motivos de confidencialidad de la información a intercambiar. En el caso de ser necesario cifrar los mensajes, el mecanismo de firma será obligatoriamente WS-Security y el de cifrado WS-Encryption

Por defecto, el cifrado irá siempre en la respuesta cuando se considere necesario, 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> en peticiones síncronas con una única solicitud***, tal y como se muestra en los ejemplos posteriores, no siendo obligatorio el cifrado en ningún caso sino potestad del organismo que presta el servicio.

En la peticiones/respuestas asíncronas (usadas generalmente para una petición con múltiples solicitudes) se cifrará el nodo Solicitudes/Transmisiones, respectivamente.

Los nodos posibles para ser cifrados son los siguientes:

- peticion.xsd ➔ Solicitudes
- respuesta.xsd ➔ Transmisiones
- datos-especificos.xsd ➔ DatosEspecificos
- solicitud-respuesta.xsd ➔ SolicitudRespuesta
- confirmación-peticion.xsd ➔ Confirmacionpetición.

Se incluye un atributo opcional (Id) en estos elementos susceptibles de ser cifrados para agilizar las búsquedas por referencia en lugar de por Xpath.

```
<xs:attribute name="Id" type="xs:string" use="optional"/>
```

Ya que todos los mensajes intercambiados son bilaterales, el mensaje irá cifrado para un único destinatario, no soportándose el cifrado para varios destinatarios en un mismo mensaje.

El mecanismo de cifrado es el siguiente:

1. El organismo que deba cifrar la información, generará una clave simétrica utilizando el algoritmo AES 128. (Las implementaciones deberán soportar longitudes mayores para cuando se recomiende el cambio por motivos de seguridad, por ejemplo AES 256)

   Algorithm= http://www.w3.org/2001/04/xmlenc#aes128-cbc

2. Se cifrará el contenido del nodo datos específicos en el caso de peticiones síncronas. En la peticiones/respuestas asíncronas (usadas generalmente para una petición con múltiples solicitudes) se cifrará el nodo Solicitudes/Transmisiones.

3. El organismo cifrará la clave simétrica anteriormente generada, utilizando el algoritmo asimétrico rsa, para garantizar la confidencialidad hacia el solicitante de la información. Para ello utilizará la clave pública extraída del certificado con el que se firmó la petición. No se soportará enviar otra información adicional no relacionada con el requirente. El algoritmo utilizado será:

Algorithm= http://www.w3.org/2001/04/xmlenc#rsa-1_5

4. Se compondrán los tokens de seguridad necesarios y el mensaje según el formato acordado como se describe a continuación.

5. Una vez cifrado el mensaje, es cuándo se procede a la firma del mismo (***y no antes***). De esta forma se garantiza la integridad de la transmisión y la confidencialidad extremo a extremo de la misma.

   De una forma gráfica el diagrama de cifrado es el siguiente.

3.9.1 Tokens de seguridad WS-Security

El mecanismo de acceso a los elementos de seguridad utilizados para la firma y el cifrado en WS-Security será por ***referencia*** a un BinarySecurityToken.

A continuación se recoge el formato de estos elementos:

SecurityTokenReference

```
<wsse:SecurityTokenReference xmlns:wsu=http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd wsu:Id="STRId-2056288912">
<wsse:Reference URI="#CertId-15915065" ➔ VALOR DE LA REFERENCIA DEL CERTIFICADO
ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3"/>
</wsse:SecurityTokenReference>
```

BinarySecurityToken

```
<wsse:BinarySecurityToken xmlns:wsu=http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd
 EncodingType=http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary
ValueType=http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3
 wsu:Id="CertId-15915065" ➔ "Referencia del certificado"> VALOR DEL CERTIFICADO USADO PARA LA FIRMA
</wsse:BinarySecurityToken>
```

EncryptedKey- Clave simétrica cifrada asimétricamente

```
<xenc:EncryptedKey Id="EncKeyId-22EFAB4BB8C7B31B6612452246585372">
            <xenc:EncryptionMethod Algorithm=http://www.w3.org/2001/04/xmlenc#rsa-1_5/>
           <ds:KeyInfo xmlns:ds=http://www.w3.org/2000/09/xmldsig#>
            <wsse:SecurityTokenReference>
               <wsse:Reference URI="#22EFAB4BB8C7B31B6612452246584411"
ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3"/>
</wsse:SecurityTokenReference>
</ds:KeyInfo><xenc:CipherData>
   <xenc:CipherValue>KJSAriyP ➔ VALOR DE LA CLAVE CIFRADA  teBoE=</xenc:CipherValue>
```

```
</xenc:CipherData>
    <xenc:ReferenceList>  ➔ LISTA DE ELEMENTOS CIFRADOS CON ESTA CLAVE
        <xenc:DataReference URI="#EncDataId-632300976"/></xenc:ReferenceList>
        </xenc:EncryptedKey>
```

4. MENSAJES INTERCAMBIADOS

4.1 Mensaje de petición SCSPv3.3

A continuación se recoge el esquema de petición SCSPv3.3.

Como se aprecia en la *Imagen 1.- Diagrama de petición SCSPv3.3,* la petición estará formada por dos ramas de información, la rama definida como ***Atributos***, y la de ***Solicitudes***.

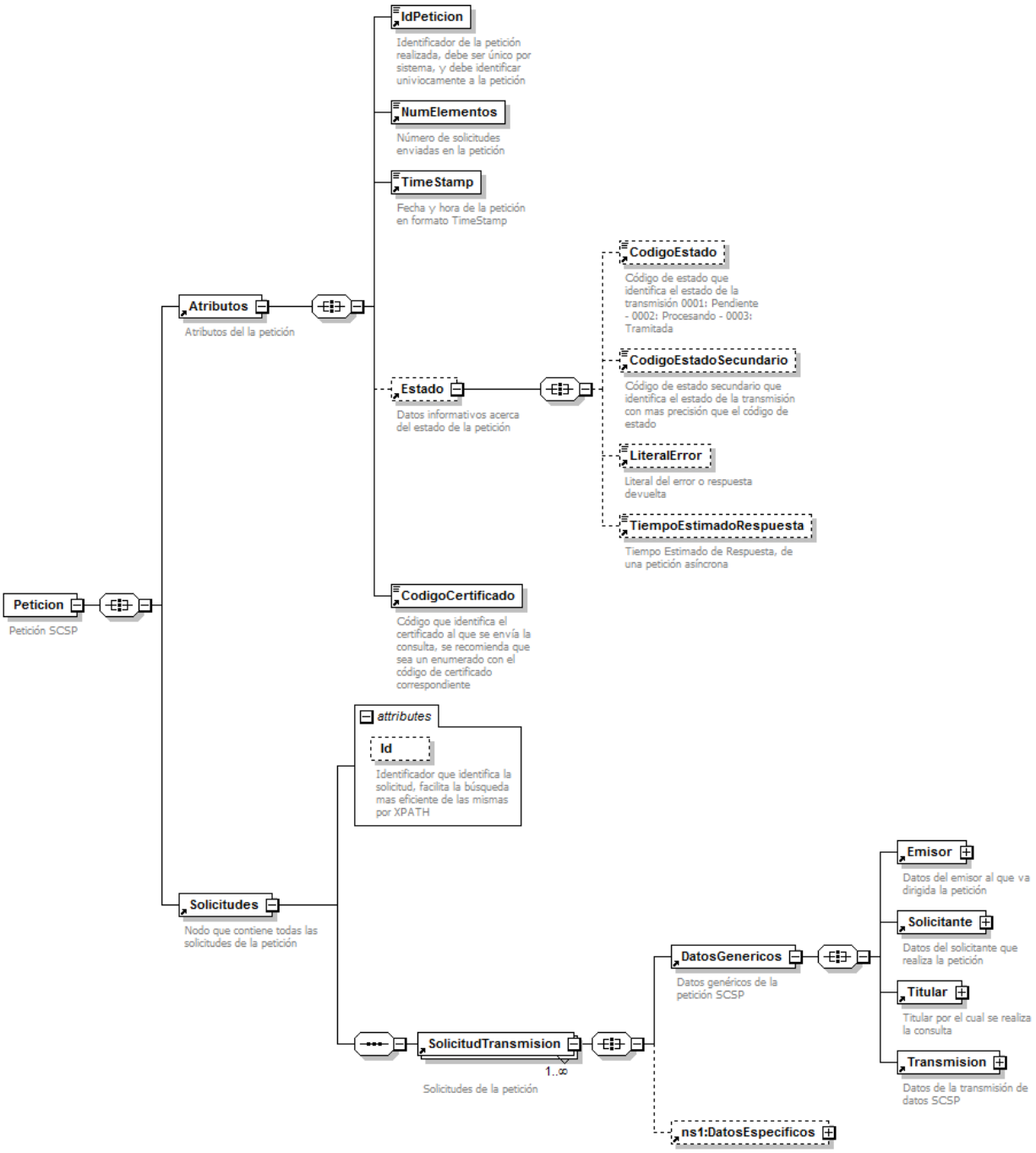


Imagen 1.- Diagrama de petición SCSPv3.3

La rama ***Atributos***, contiene los datos de control relativos a toda la petición.
La rama ***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**: Se refiere al organismo que proporciona la información
- ✓ **Solicitante**: Se refiere al Organismo que proporciona la información
- ✓ **Titular**: Se refiere al "administrado" sobre quien se recaba Información
- ✓ **Transmisión**: Se refiere a la transmisión concreta realizada

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

4.1.1 Emisor

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.

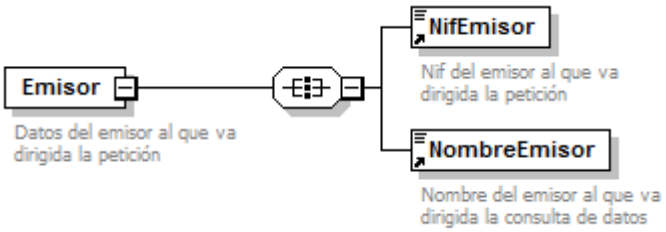


Imagen 2.- Diagrama de petición SCSPv3.3 – Emisor

4.1.1 Solicitante

La identificación del Solicitante estará formada por los siguientes campos:

- ✓ **IdentificadorSolicitante**: NIF del organismo solicitante de la Información
- ✓ **Nombre del Solicitante**: Código del Organismo que solicita los datos. Sería el CIF/NIF de la Entidad en la que está el Órgano Administrativo.
- ✓ **Unidad Tramitadora**: Se corresponderá 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.
- ✓ **Código Unidad Tramitadora**: Se corresponderá con el código de 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. Este código será el código DIR3 correspondiente a la Unidad.
- ✓ **IdExpediente**: Número de expediente, si lo hay, por el cual se realiza la consulta.
- ✓ **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 del Procedimiento**: para el que se autoriza al organismo a efectuar la consulta.

- ✓ **Clase de trámite**: Indicará la clase o tipo de trámite que se realiza y propicia la consulta de datos, la codificación utilizada es codificación SIA.

Se definen las siguientes clases de trámite:

- 0 → Pruebas (***Destinado exclusivamente a entornos distintos de producción***)
- 2 → Recursos Humanos
- 3 → Tributario
- 14 → Sancionador
- 19 → Afiliación y cotización a la Seguridad Social
- 20 → Autorizaciones, licencias, concesiones y homologaciones
- 21 → Ayudas, Becas y Subvenciones
- 22 → Certificados
- 23 → Contratación pública
- 24 → Convenios de Colaboración y Comunicaciones administrativas
- 25 → Gestión Económica y Patrimonial
- 26 → Declaraciones y comunicaciones de los interesados
- 27 → Inspectora
- 28 → Premios
- 29 → Prestaciones
- 30 → Registros y Censos
- 31 → Responsabilidad patrimonial y otras solicitudes de indemnización
- 32 → Revisión de Actos administrativos y Recursos
- 33 → Sugerencias, Quejas, Denuncias e Información a los ciudadanos
- 34 → Aduanero
- 35 → Plazas educativas, matrículas y otras gestiones académicas n.c.o.p.
- 36 → Plazas e inscripciones no académicas
- 99 → Resolución de incidencias (***Destinado exclusivamente para entornos de produccción***)

El campo Clase de tramite se especifica como opcional, no obstante si algún cedente requiere el envío del dato, se establecerá como obligatorio

- ✓ **Tipo de tramitación**: Indicará el tipo de tramitación que se realiza a la hora de realizar la consulta de datos.

Se definen los siguientes tipos de trámite:

- **S → Si**: Cuando se realizan peticiones sin intervención de un funcionario, es decir cuando el proceso de consulta es automático.
- **N → No**: Cuando se realizan peticiones con intervención de un funcionario, es decir cuando el proceso de consulta es automático.

El campo Tipo de tramitación se especifica como opcional, no obstante si algún cedente requiere el envío del dato, se establecerá como obligatorio

- ✓ **Funcionario**: Datos identificativos del Funcionario, será posible indicar un seudónimo de empleado público conforme al RD 668/2015 de 17 de Julio para los casos en los que sea necesario.
    - Para los casos de procesos automatizados se debe rellenar el nombre del funcionario responsable del servicio, y el NIF del responsable que realiza la consulta de datos.

Si el emisor de los datos lo permite se podría rellenar con el literal "PROCESO AUTOMATIZADO SIN INTERVENCION HUMANA"

- ✓ **Consentimiento**: Indica si se tiene consentimiento o no es necesario (consulta por ley) . El consentimiento puede ser expreso por parte del ciudadano objeto de la consulta "***Si***", No oposición por parte del ciudadano objeto de la consulta "***NoOpo***" o por Ley cuando exista una Ley que permita la consulta de datos "***Ley***"
- ✓ **Finalidad**: Indica la descripción de la finalidad de la consulta. Complementario a la información relativa al procedimiento.

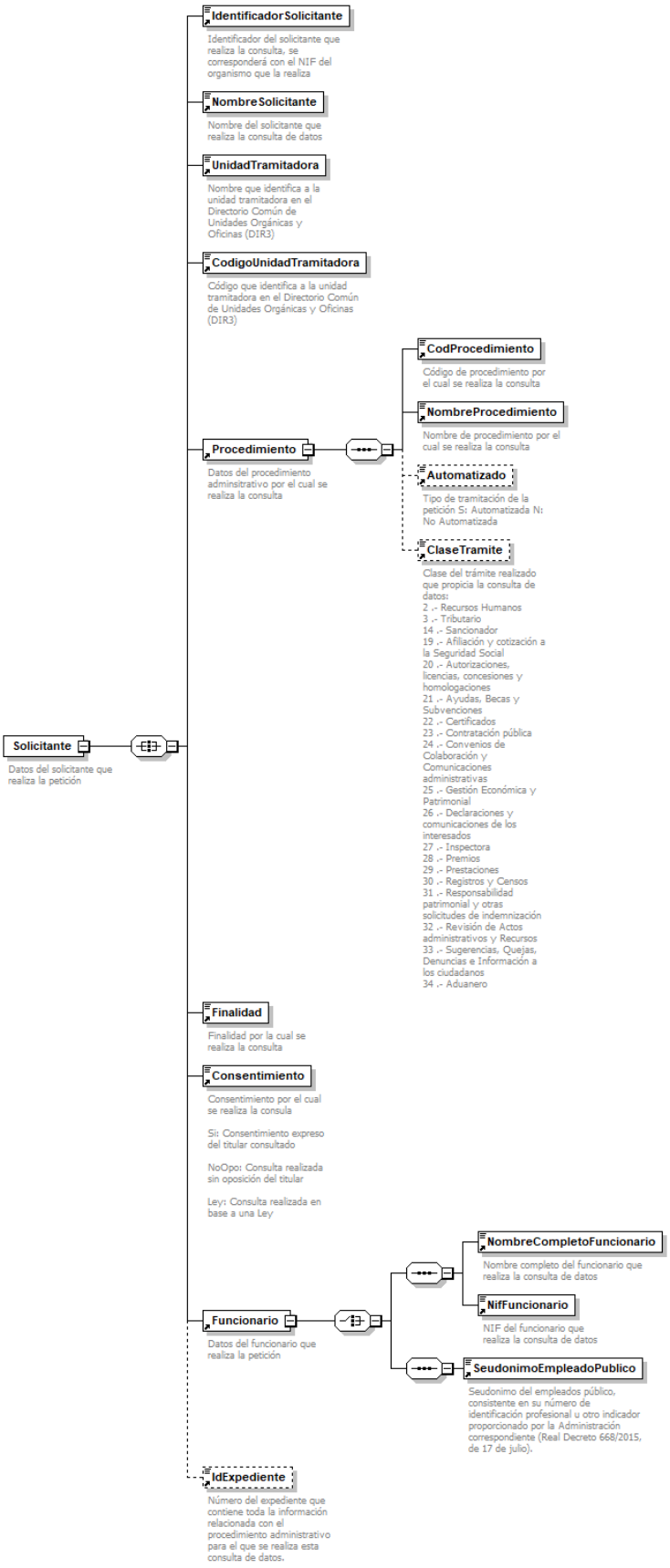


Imagen 3.- Diagrama de petición SCSPv3.3 - Solicitante

4.1.2 Titular

La identificación del titular estará formada por los siguientes campos en la parte genérica:

- ✓ **TipoDocumentacion**: Tipo de documentación identificativa (Los valores aceptados a fecha 7-03-2017 son DNI, NIE, CIF, NIF, Pasaporte, NumeroIdentificacion, Otros, CSV) 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 el tipo de documentación requerida por cada servicio emisor.
- ✓ **Documentacion**: 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, como se indica en la tabla referente a formatos de los mensajes.
- ✓ **NombreCompleto**: 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.

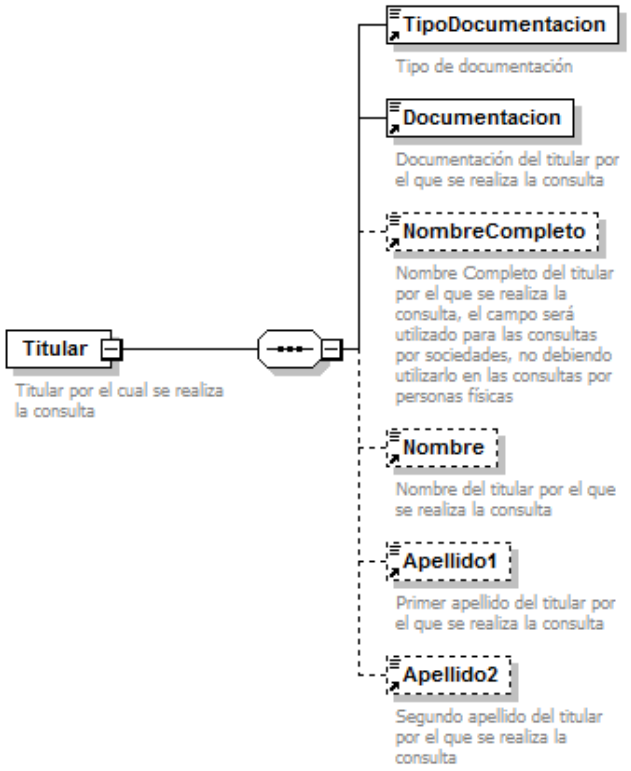


Imagen 4.- Diagrama de petición SCSPv3.3 – Titular

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

En el caso en el que se quiera prestar servicio permitiendo identificar al titular por otros elementos unívocos distintos de la documentación (y otros atributos necesarios) podría hacerse siendo responsabilidad del emisor ofrecer el servicio, así como la validación de que los datos indicados para la identificación sean únicos. (Apellidos, fecha de nacimiento, lugar de nacimiento, etc...)

En caso de ser necesario, los datos de documentación, o Nombre, Apellidos[1|2] pueden ser opcionales u obligatorios según el emisor requiera.

4.1.3 Transmisión

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

- ✓ **CodigoCertificado**: 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.
- ✓ **IdTransmision**: 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.

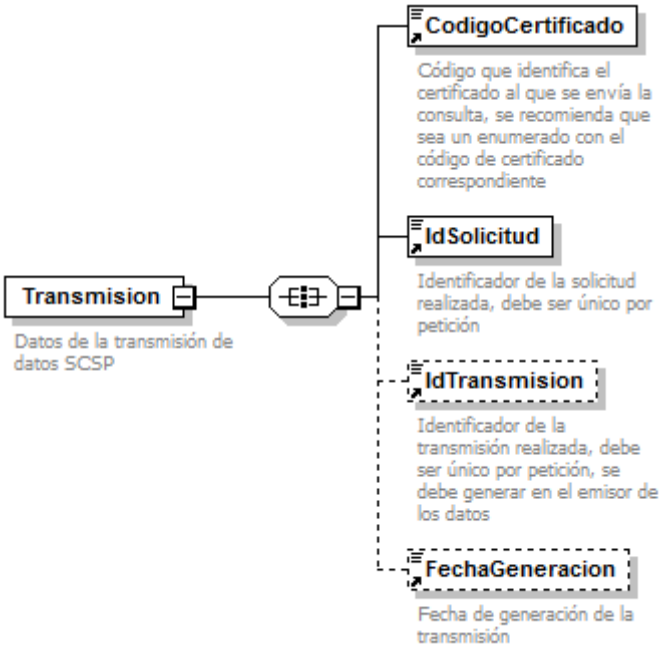


Imagen 5.- Diagrama de petición SCSPv3.3 – Transmisión

Se deberá ofrecer un mecanismo a los órganos de fiscalización y control para la validación de la transmisión efectuada para un NIF concreto.

4.2 Mensaje de respuesta SCSPv3.3

A continuación se recoge el esquema de respuesta SCSPv3.3.

Como se aprecia en la *Imagen 6.- Diagrama de respuesta SCSPv3.3*. "Mensaje de Respuesta SCSPv3.3", la respuesta estará formada por dos ramas de información, la rama definida como ***Atributos***, y la de ***Transmisiones***.

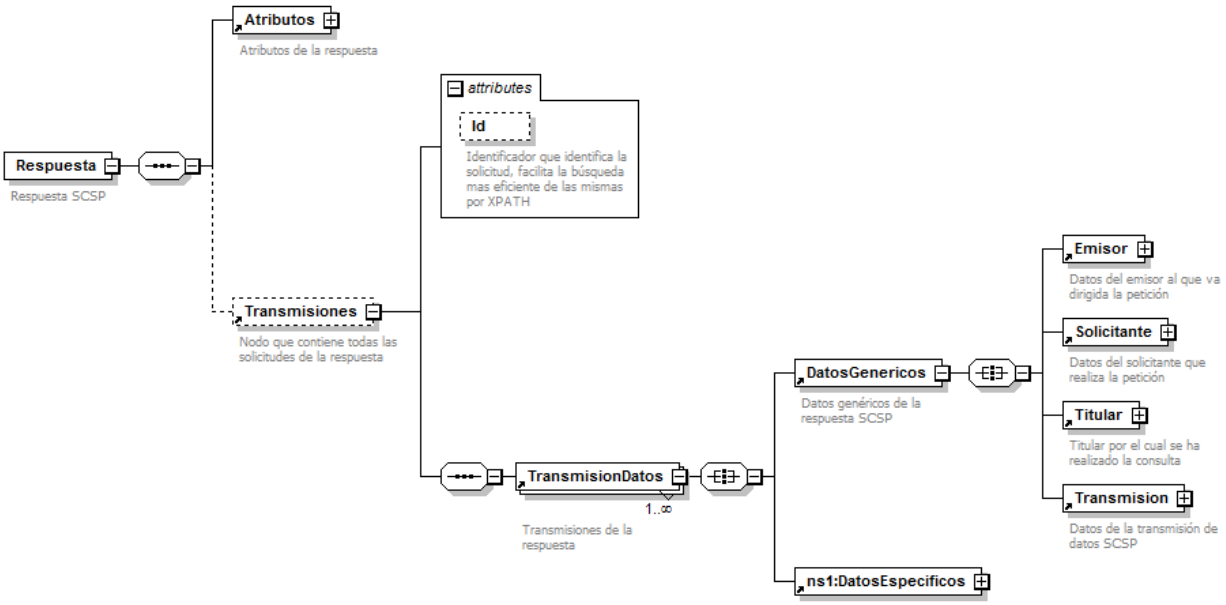


Imagen 6.- Diagrama de respuesta SCSPv3.3

La rama ***Atributos***, contiene los datos de control relativos a toda la respuesta.
La rama **Transmisiones** contiene las Transmisiones de Datos (Nodo TransmisionDatos) 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**: Se refiere al organismo que proporciona la información
- ✓ **Solicitante**: Se refiere al Organismo que proporciona la información
- ✓ **Titular**: Se refiere al "administrado" sobre quien se recaba Información
- ✓ **Transmisión**: Se refiere a la transmisión concreta realizada

La estructura de ***DatosEspecíficos*** en la respuesta contendrá los parámetros específicos de cada servicio, y será definida por el emisor.
Salvo que se produzca un error, los datos relativos la parte genérica el emisor podrá responder con los enviados por el requirente.
En caso de que los datos que se envían en la petición no fueran informados, y cuando existan en el emisor y sean relevantes para el servicio, se deben rellenar adecuadamente por el Emisor.

Este comportamiento permitirá validar la calidad de las respuestas.

4.2.1 Emisor

Véase el apartado *4.1.1 Emisor*

4.2.2 Solicitante

Véase el apartado *4.1.1 Solicitante*

4.2.3 Titular

Véase el apartado *4.1.2 Titular*

4.2.4 Transmisión

Véase el apartado *4.1.3 Transmisión*

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

- ✓ **CodigoCertificado**: 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.
- ✓ **IdTransmision**: 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.
- ✓ **FechaGeneracion**: Indica la fecha en la que se generó la transmisión de datos.

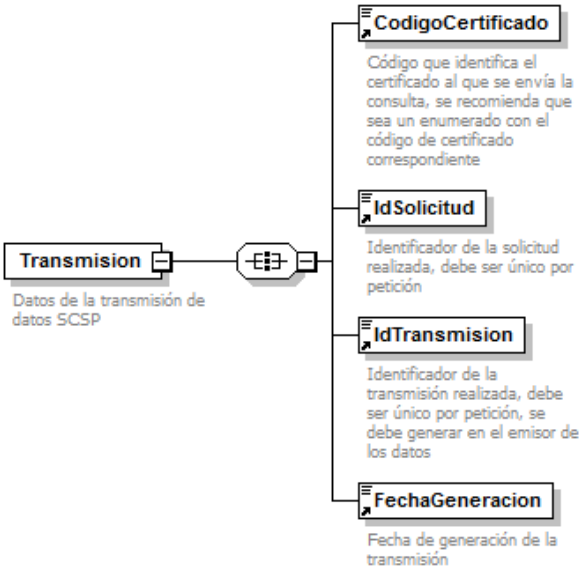


Imagen 7.- Diagrama de respuesta SCSPv3.3 - Transmisión

Se deberá ofrecer un mecanismo a los órganos de fiscalización y control para la validación de la transmisión efectuada para un NIF concreto.

4.3 Mensaje de confirmación de petición SCSPv3.3

A continuación se recoge el mensaje de confirmación de petición SCSPv3.3.

Se usará 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.

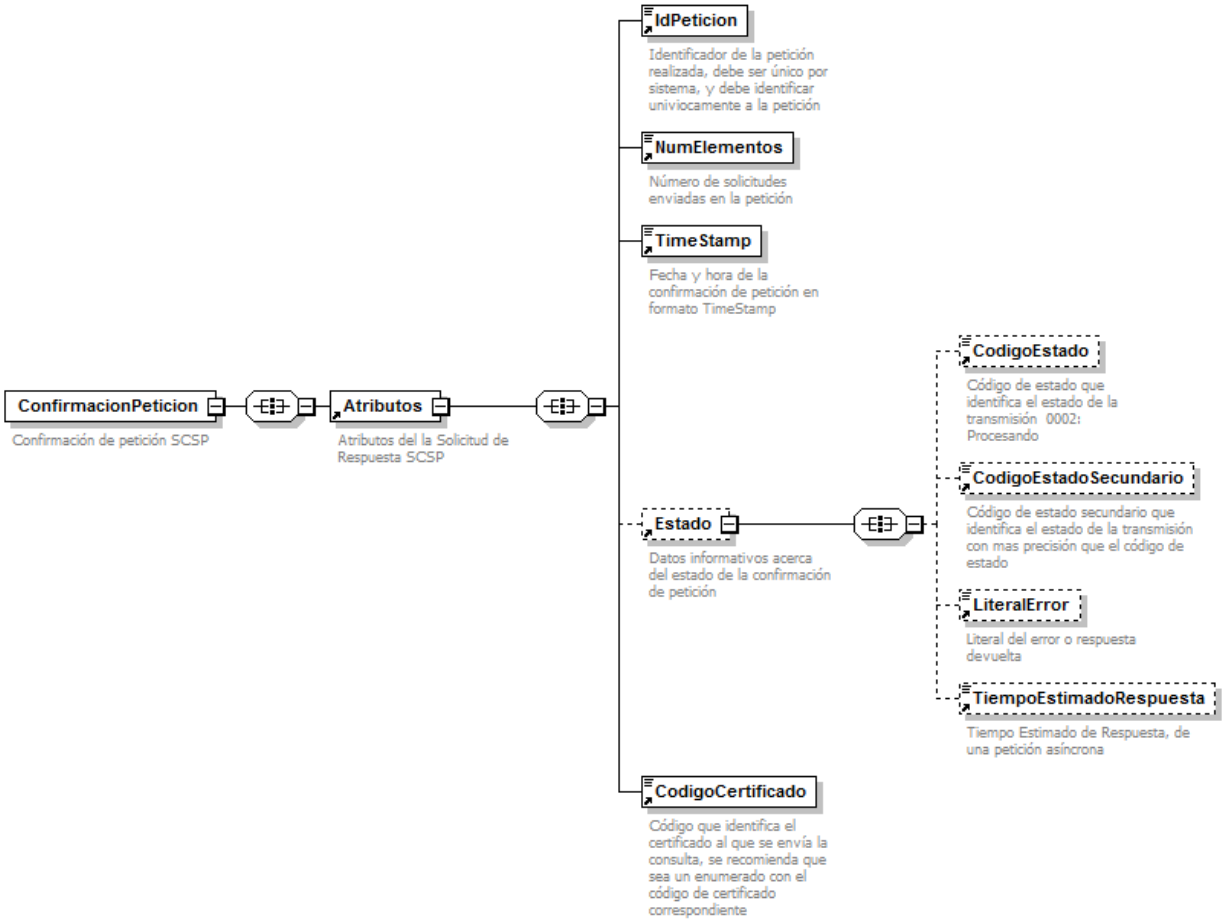


Imagen 8.- Diagrama de confirmación de petición SCSPv3.3

Como se aprecia en la *Imagen 8.- Diagrama de confirmación de petición SCSPv3.3*. la respuesta estará formada por una ramas de información, la rama definida como ***Atributos***.
Los atributos son los relativos a la petición recibida:

- ✓ **IdPeticion**: 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 respuesta y con el número de solicitudes y transmisiones a intercambiar.
- ✓ **TimeStamp**: Marca de tiempo en la que se ha realizado la confirmación de petición. El formato especificado viene definido en el documento de especificaciones técnicas SCSPv3.3.
- ✓ **Estado**: Bloque con la información de control. Si no se ha producido ningún error su valor será "**0002**" **EN PROCESO**. Si se ha producido un error, indicará el error correspondiente.
- ✓ **CodigoCertificado**: Se refiere al Certificado de datos al que sustituye la transmisión.

4.4 Mensaje de solicitud de respuesta SCSPv3.3

A continuación se recoge el mensaje de solicitud de respuesta SCSPv3.3.

Se usará 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.



Imagen 9.- Diagrama de solicitud de respuesta SCSPv3.3

Como se aprecia en la *Imagen 9.- Diagrama de solicitud de respuesta SCSPv3.3*, la Solicitud de respuesta estará formada por una rama de información ***Atributos***.
Los atributos son los relativos a la petición enviada:

- ✓ **IdPeticion**: 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. El formato especificado viene definido en el documento de especificaciones técnicas SCSPv3.3.
- ✓ **Solicitante**: Bloque con la información del solicitante que ha enviado la solicitud de respuesta. Esta información deberá ser la misma del solicitante que realizó la petición asíncrona.
- ✓ **Estado**: Bloque con la información de control. En este mensaje debe No debe ir informado.
- ✓ **CodigoCertificado**: Se refiere al Certificado de datos al que sustituye la transmisión.

4.5 Datos específicos

Si bien no es un mensaje concreto sino un componente general que puede ser incluido tanto en el mensaje de petición (***siempre que sea necesario***) como en el de respuesta, se analizan las características generales que deben cumplir los datos específicos, así como las recomendaciones al respecto para una mejor implementación.

- ✓ Los datos específicos se definirán bajo un único namespace, tanto si se incluyen en la petición, en la respuesta o en ambos casos.
- ✓ En caso de implementarse en un único fichero y ser requerido tanto en la petición como en la respuesta se optará por una estructura de tipo "switch" para indicar que en cada caso solo pueden venir los datos de entrada o la respuesta.
- ✓ Si los parámetros de entrada se quieren devolver en la respuesta, la parte de respuesta debería quedar como opcional y validarse por parte del emisor que cuando se reciba en la entrada debe ignorarse o generarse el error correspondiente.
- ✓ Se recomienda incluir un indicador de Negocio del estado del tratamiento de cada solicitud/transmisión conteniendo los datos específicos de cada negocio.
    - o En relación al tratamiento asíncrono este indicador permitirá devolver el estado de cada petición incluso en el caso de que produzca un fallo en el tratamiento.
    - o En caso de no incluirse, en el procesamiento asíncrono implicará que si falla una de las solicitudes/transmisiones, deberá fallar toda la petición/transmisión de datos, generando un SOAP Fault.

Una recomendación aproximada de datos específicos es como la siguiente, esta recomendación se especifica técnicamente en el documento de especificación técnica SCSPv3.3.

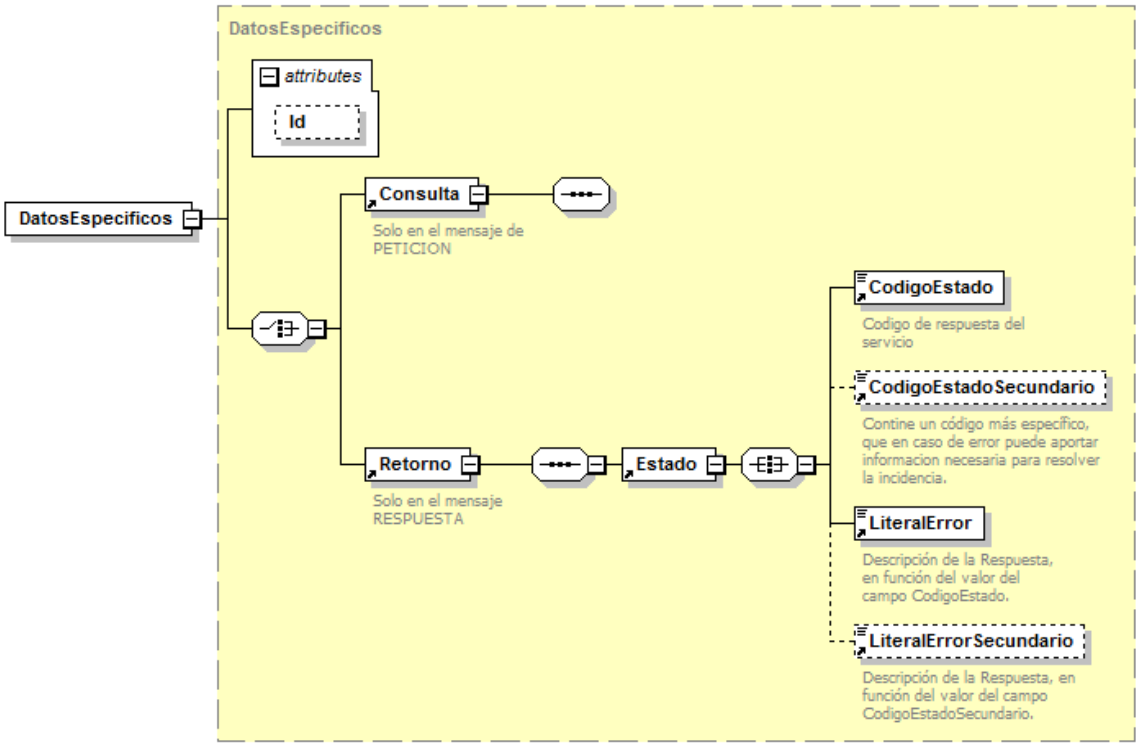


Imagen 10.- Diagrama de datos específicos SCSPv3.3

5. GESTIÓN DE ERRORES

Se entenderá que no se ha producido un error cuando no ha fallado ningún sistema, mecanismo de comunicación o similar, aunque la operación solicitada (Consulta de datos, Actualización de datos) no se haya podido realizar. Es decir cuando es una casuística contemplada en el Negocio. En estos casos, "***casuística de Negocio***", la respuesta generada seguirá las especificaciones generales del modelo de intercambio de información SCSP, especificado en los mensajes de respuesta.

Se devolverá un mensaje SOAP Fault cuando el error detectado pertenezca a alguno de los siguientes tipos:

- ✓ Error de conexión a la sistemas externos (@Firma, CICS, Servidores Externos, etc).
- ✓ Error en la validación de esquemas (o petición recibida sin firma).
- ✓ Error por validación de la Firma digital, o problemas en la autorización y autenticación.
  - No estar firmado alguno de los mensajes, petición, respuesta, confirmación de petición o solicitud de respuesta.
  - Certificado caducado, revocado o no válido.
  - Firma inválida
  - …
- ✓ Error del Sistema Interno en el tratamiento de la petición.
- ✓ Error de conexión a la BBDD.
- ✓ Errores indefinidos

Los mensajes SOAP Fault no se firmarán. En caso de devolverse firmados, no se realizará una validación de la firma/certificado del mismo

En el resto de casos, no contemplados en la lista anterior, se entenderá que la petición se ha podido tramitar y se devolverá un mensaje de Respuesta especificando en las etiquetas correspondientes el código y el texto del error o estado correspondiente (una vez mapeado) al considerarse una respuesta contemplada por el negocio.

Este apartado se desarrolla en profundidad en el documento de especificación técnica de SCSPv3.3.

6. ANEXO I: WSDL Y XSD (FORMATOS Y ESQUEMAS)

Este apartado se desarrolla en profundidad en el documento de especificación técnica de SCSPv3.3

7. ANEXO II: DEFINICIONES RELEVANTES

- **CAID:** Centro de Atención a Integradores y Desarrolladores de la Agencia Estatal de Administración Digital de la Plataforma de Intermediación.
- **Cedente**: Organismo que proporciona datos y responsable de los mismos según la LOPD. Ofrecerá los datos a través de un Emisor SCSP.
- **Cesionario**: Organismo que Solicita los datos en virtud de un procedimiento o trámite. Consumirá los datos/transmisiones a través de un requirente.
- **Emisor**: Organismo que proporciona el servicio SCSP para la transmisión de datos.
- **Nodo de Interoperabilidad: (Según el RD4/2010)** Organismo que presta servicios de interconexión técnica, organizativa y jurídica entre sistemas de información para un conjunto de Administraciones Públicas bajo las condiciones que éstas fijen. Podrá ser en este caso tanto requirente como emisor de datos.
- **Plataforma de Intermediación**: Sistema que facilita la interoperabilidad entre Organismos Cesionarios y Cedentes de datos cumpliendo las especificaciones de Sustitución de Certificados en Soporte Papel.
- **Procedimiento administrativo**: proceso mediante el cual un órgano administrativo adopta decisiones sobre las pretensiones formuladas por la ciudadanía o sobre las prestaciones y servicios cuya satisfacción o tutela tiene encomendadas. Estará regulado por una Norma que implicará la necesidad de conocer o consultar los datos requeridos y que es exigida como requisito para otorgar en el acceso dicha consulta de datos.
- **Requirente**: Organismo que consume el servicio SCSP para la solicitud y transmisión de datos.
- **Servicio público**: cualquier actividad realizada por la Administración Pública dirigida a la ciudadanía para satisfacer sus necesidades, derechos u obligaciones.
  Un servicio puede estar asociado con uno o varios procedimientos administrativos o, por el contrario, no tener relación alguna.
- **Solicitud de Consentimiento:** La solicitud de consentimiento para consultar datos de carácter personal debe ser acorde a lo recogido en la LOPD y normativa vinculante al intercambio de datos entre Administraciones. (Ley 39/2015 Art 28.2). El derecho se ejercitará de forma específica e individualizada para cada procedimiento concreto, sin que el ejercicio del derecho ante un órgano u organismo implique un consentimiento general referido a todos los procedimientos que aquel tramite en relación con el interesado.
- **Trámite o fase:** actividad o grupo de actividades relacionadas entre sí que tienen por objeto cumplir una misma función concreta dentro de cada una de las fases del procedimiento. El trámite está constituido por un conjunto de actuaciones dentro de un procedimiento, con sustantividad propia, por lo que genera efectos jurídico-procesales.
- **Unidad de Auditorías: (Responsable de Auditoría)** Será la unidad encargada de la realización de las tareas de Auditorías, tanto en el Organismo Cedente como en el Cesionario.
- **Unidad Responsable de Autorización**: Unidad de gestión perteneciente al Organismo **Cesionario** que autoriza en el Organismo **Cesionario** la consulta de datos para el procedimiento o trámite en virtud del cual se solicita la información a las distintas Unidades Tramitadoras.
  La unidad Responsable de Autorización podrá aplicar el control centralizado o distribuido
- **Unidad Tramitadora**: Unidad de gestión perteneciente al Organismo **Cesionario** que tramita el procedimiento o trámite en virtud del cual se solicita la información.