

---

## Modelo de Datos Librerías SCSP J2EE 4.23.0

**Proyecto:** Librerías SCSP 4.23.0  
**Título:** Librerías SCSP 4.23.0  
**Revisión:** 1.20  
**Fecha:** Junio de 2020



## Ficha del documento

Fecha	Revisión	Autor	Verificado por
31/03/2014	3.4.0	Oficina Técnica	José Antonio Eusamio

## Documentos relacionados

Fecha	Revisión	Título

## Lista de distribución del documento

Fecha	Nombre
03/04/2014	Administraciones Públicas

## Control de versiones

Fecha	Revisión	Descripción del cambio
31/03/2014	1.0	Versión inicial
19/09/2014	1.1	Adaptación a las librerías 3.5.0
22/04/2015	1.2	Adaptación a las librerías 3.5.3
09/06/2015	1.3	Adaptación a las librerías 3.5.4
12/01/2016	1.4	Adaptación a las librerías 3.5.5
10/08/2016	1.5	Adaptación a las librerías 3.5.6
12/01/2017	1.6	Adaptación a las librerías 3.5.7
03/07/2017	1.7	Adaptación a las librerías 4.0.0
16/10/2017	1.8	Adaptación a las librerías 4.2.0
06/11/2017	1.9	Adaptación a las librerías 4.3.0
30/01/2018	1.10	Adaptación a las librerías 4.6.0

Fecha	Revisión	Descripción del cambio
07/05/2018	1.11	Adaptación a las librerías 4.8.0
13/07/2018	1.12	Adaptación a las librerías 4.11.1
05/11/2018	1.13	Adaptación a las librerías 4.15.0
29/03/2019	1.14	Adaptación a las librerías 4.18.0
20/05/2019	1.15	Corrección de erratas.
04/07/2019	1.16	Adaptación a las librerías 4.20.0
06/09/2019	1.17	Corrección de erratas.
20/12/2019	1.18	Adaptación a las librerías 4.21.0
23/03/2020	1.19	Adaptación a las librerías 4.22.0
18/06/2020	1.20	Adaptación a las librerías 4.23.0



**© 2020 Ministerio de Asuntos Económicos y Transformación Digital**

Reservados todos los derechos. Quedan rigurosamente prohibidas, sin el permiso escrito de los titulares del copyright, la reproducción o la transmisión total o parcial de esta obra por cualquier procedimiento mecánico o electrónico, incluyendo la reprografía y el tratamiento informático, y la distribución de ejemplares mediante alquiler o préstamos públicos.

This work is protected by copyright. All rights reserved for reproduction or copying of this document or parts thereof. This also applies to its translations. No parts of this work may, in any form whatsoever, (print, photocopy, microfilm or any other procedures), including for training purpose, be reproduced or electronically processed, duplicated or disseminated without the written permission of the copyright owner.

## Contenido

FICHA DEL DOCUMENTO .....	2
DOCUMENTOS RELACIONADOS.....	2
LISTA DE DISTRIBUCIÓN DEL DOCUMENTO .....	2
CONTROL DE VERSIONES.....	2
1    MODELO DE DATOS LIBRERÍAS SCSP .....	8
1.1    Descripción cambios incluidos en Modelo de Datos Librerías SCSP 3.2.1 .....	8
1.2    Descripción cambios incluidos en Modelo de Datos Librerías SCSP 3.2.2 .....	9
1.3    Descripción cambios incluidos en Modelo de Datos Librerías SCSP 3.3.0 .....	10
1.4    Descripción cambios incluidos en Modelo de Datos Librerías SCSP 3.3.1 .....	10
1.5    Descripción cambios incluidos en Modelo de Datos Librerías SCSP 3.4.0 .....	11
1.6    Descripción cambios incluidos en Modelo de Datos Librerías SCSP 3.5.0 .....	11
1.7    Descripción cambios incluidos en Modelo de Datos Librerías SCSP 3.5.3 .....	12
1.8    Descripción cambios incluidos en Modelo de Datos Librerías SCSP 3.5.4 .....	12
1.9    Descripción cambios incluidos en Modelo de Datos Librerías SCSP 3.5.5 .....	12
1.10    Descripción cambios incluidos en Modelo de Datos Librerías SCSP 3.5.6 .....	12
1.11    Descripción cambios incluidos en Modelo de Datos Librerías SCSP 3.5.7 .....	12
1.12    Descripción cambios incluidos en Modelo de Datos Librerías SCSP 4.0.0 .....	13
1.13    Descripción cambios incluidos en Modelo de Datos Librerías SCSP 4.2.0 .....	13
1.14    Descripción cambios incluidos en Modelo de Datos Librerías SCSP 4.3.0 .....	13
1.15    Descripción cambios incluidos en Modelo de Datos Librerías SCSP 4.4.0 .....	14
1.16    Descripción cambios incluidos en Modelo de Datos Librerías SCSP 4.5.0 .....	14
1.17    Descripción cambios incluidos en Modelo de Datos Librerías SCSP 4.6.0 .....	14
1.18    Descripción cambios incluidos en Modelo de Datos Librerías SCSP 4.7.0 .....	14
1.19    Descripción cambios incluidos en Modelo de Datos Librerías SCSP 4.8.0 .....	14

1.20	Descripción cambios incluidos en Modelo de Datos Librerías SCSP 4.11.1 .....	14
1.21	Descripción cambios incluidos en Modelo de Datos Librerías SCSP 4.15.0 .....	14
1.22	Descripción cambios incluidos en Modelo de Datos Librerías SCSP 4.18.0 .....	15
1.23	Descripción cambios incluidos en Modelo de Datos Librerías SCSP 4.20.0 .....	15
1.24	Descripción cambios incluidos en Modelo de Datos Librerías SCSP 4.21.0 .....	15
1.25	Descripción cambios incluidos en Modelo de Datos Librerías SCSP 4.22.0 .....	15
1.26	Descripción cambios incluidos en Modelo de Datos Librerías SCSP 4.23.0 .....	15
1.27	Diagrama Modelo de datos SCSP J2EE Requirente .....	16
1.28	Diagrama Modelo de datos SCSP J2EE Emisor .....	17
2	DESCRIPCIÓN TABLAS .....	18
2.1	Tablas comunes .....	18
2.1.1	CORE_SERVICIO .....	18
2.1.2	CORE_CLAVE_PRIVADA .....	23
2.1.3	CORE_CLAVE_PUBLICA .....	24
2.1.4	CORE_EMITOR_CERTIFICADO .....	24
2.1.5	CORE_MODULO .....	25
2.1.6	CORE_MODULO_CONFIGURACION .....	26
2.1.7	CORE_PARAMETRO_CONFIGURACION .....	27
2.1.8	CORE_PETICION_RESPUESTA .....	32
2.1.9	CORE_REQ_SECUENCIA_IDPETICION .....	33
2.1.10	CORE_TIPO_MENSAJE .....	34
2.1.11	CORE_TOKEN_DATA .....	35
2.1.12	CORE_TRANSMISION .....	36
2.1.13	CORE_CODIGO_ERROR .....	37
2.1.14	CORE_ESTADO_PETICION .....	38
2.1.15	CORE_CACHE_CERTIFICADOS .....	38
2.1.16	CORE_ORGANISMO_CESIONARIO .....	39
2.1.17	CORE_REQ_CESIONARIOS_SERVICIOS .....	39
2.1.18	CORE_REQ_MODULO_PDF .....	40
2.1.19	CORE_REQ_MODULO_PDF_CESIONARIO .....	40
2.2	Tablas entorno emisor .....	41
2.2.1	CORE_EM_BACKOFFICE .....	41

---

2.2.2	CORE_EM_CODIGO_ERROR_SECUN .....	41
2.2.3	CORE_EM_APLICACION.....	42
2.2.4	CORE_EM_AUTORIZACION_CA .....	42
2.2.5	CORE_EM_AUTORIZACION_CERT .....	43
2.2.6	CORE_EM_AUTORIZACION_ORGANISMO .....	43
2.2.7	CORE_EM_SECUENCIA_IDTRANS .....	44

## 1 Modelo de Datos Librerías SCSP

### 1.1 Descripción cambios incluidos en Modelo de Datos Librerías SCSP 3.2.1

Las librerías SCSP han introducido un cambio en su modelo de datos buscando facilitar el proceso de instalación y configuración. Se cambió la filosofía de configuración a través de ficheros XML y properties, para pasar a un modelo donde toda la configuración parametrizable por un administrador resida en Base de datos.

El objetivo final de este cambio, sería poder tener herramientas que automaticen el proceso de configuración y propongan al administrador una interfaz más amigable e intuitiva que la edición de ficheros.

A continuación se muestran las nuevas características del nuevo modelo de datos de SCSP 3.1.

Las características más importantes son:

- Aparece una tabla de configuración de parejas clave/valor común a toda la aplicación: `core_parametro_configuracion`.
- Se incluye la información relativa a la configuración de servicios (URLs, tipo de seguridad, etc.) que anteriormente se almacenaba en los XMLs de la aplicación.
- Se añaden dos tablas para el control de los certificados a emplear en la securización de mensajes, tanto de las claves públicas como privadas:
  - `Core_clave_publica`
  - `Core_clave_privada`
- Se añade la tabla `BackOffice` para los emisores, que asocia la clase que procesa las peticiones con cada tipo de certificado: `emisor_backoffice`
- Se añaden dos tablas para configurar los módulos que están habilitados:
  - `Core_modulo`: permite una configuración de activación global
  - `Core_modulo_configuracion`: permite una configuración por servicios

Actualmente dicha configuración se realiza a partir del fichero de configuración de Axis2.

- Se modifica la disposición de la tabla “`T_PETICION_RESPUESTA_D`”, que ahora se divide en dos tablas:
  - `Peticionesrespuestas`: Registrará la meta-data de los mensajes
  - `Tokendata`: Almacenará los propios XML intercambiados

El motivo de esta separación es aumentar el rendimiento en los procesos de consulta, evitando la carga del XML cuando será más probable el acceso para consultar exclusivamente información de meta-data.



Otra ventaja sería la de poder aplicar políticas diferentes de administración de base de datos a la tabla tokendata, ya que por su naturaleza el crecimiento de la misma será varios órdenes de magnitud mayor que el del resto de las tablas.

- Se han añadido nuevas columnas en la tabla transmisiones, anteriormente T\_TRANSMISIONES\_RECIBIDAS\_D o T\_TRANSMISIONES\_EMITIDAS\_D. Dichas columnas recogerán la información perteneciente a los datos genéricos de la transmisión, de tal forma que una aplicación consumidora de esta información no se vea obligada a procesar el nodo de transmisiones.
- Para la lógica del emisor se han añadido tablas para gestionar las autorizaciones de los organismos a los servicios emitidos a través de aplicaciones. Para ello se han incluido las tablas :
  - Autorizacion\_aplicacion:  
Tabla en la que se registran las diferentes aplicaciones a las que se le va a dar acceso a los servicios, almacenando sus datos identificativos contenidos en el certificado digital empleado para firmar sus peticiones
  - Autorizacion\_organismo:  
Tabla que gestionará los organismos autorizados a emplear una aplicación a través de la cual podrán solicitar los certificados emitidos.
  - Autorizacion\_certificado:  
Tabla en la que se incluye las relaciones de autorización existentes entre la tabla de aplicaciones y de certificados
  - Autorizacion\_ca:  
Tabla que almacenará las diferentes autoridades de certificación cuyos certificados serán empleados en la securización de los mensajes.

## 1.2 Descripción cambios incluidos en Modelo de Datos Librerías SCSP 3.2.2

Las librerías SCSP han introducido los siguientes cambios en su modelo de Base de Datos.

- Se han añadido y modificado nuevos campos en la tabla CORE\_TRANSMISION
  - Se añade el campo NombreTitular
  - Se añade el campo Apellido1Titular
  - Se añade el campo Apellido2Titular
  - Se añade el campo NombreCompletoTitular
  - Se permite que el campo DocTitular sea nulo
- Se ha añadido el siguiente campo a la tabla CORE\_EMITOR\_CERTIFICADO

- Se añade el campo fechaBaja para permitir dar de baja emisores de certificados dados de alta
- Se añaden los siguientes campos en la tabla CORE\_SERVICIO
  - Se añade el campo xpathcoderror
  - Se añade el campo xpathliteralerror
  - Se añade el campo timeout
  - Se añade el campo validaFirma
- En la tabla AUTORIZACION\_ORGANISMO se elimina la foreign key a AUTORIZACION\_APLICACION
- En la tabla AUTORIZACION\_CERTIFICADO se añade una foreign key a idorganismo de la tabla AUTORIZACION\_ORGANISMO. Dicha columna pasará a formar parte de la primary key compuesta de esta tabla.
- En la tabla AUTORIZACION\_CERTIFICADO se añaden los siguientes campos
  - IDORGANISMO
  - FECHAALTA
  - FECHABAJA
- En la tabla CORE\_PARAMETRO\_CONFIGURACION se modifica lo siguiente
  - Se añade el parámetro prefijo.idtransmision
  - Se añade el parámetro versión.datamodel.scsp
  - Se elimina el parámetro validación.formatofirma

### 1.3 Descripción cambios incluidos en Modelo de Datos Librerías SCSP 3.3.0

- Se elimina la tabla CORE\_BLOQUEO

### 1.4 Descripción cambios incluidos en Modelo de Datos Librerías SCSP 3.3.1

- Se añade un parámetro para permitir validar el Cif del Emisor con el configurado en BBDD

## 1.5 Descripción cambios incluidos en Modelo de Datos Librerías SCSP 3.4.0

- En la tabla CORE\_CLAVE\_PRIVADA se añaden los siguientes campos
  - ID (Pasa a ser la Primary Key para permitir multifirma)
  - ORGANIMOS
- En la tabla CORE\_CLAVE\_PUBLICA se añade el siguiente campo
  - ID (Pasa a ser la Primary Key)
- En la tabla CORE\_SERVICIO se modifica lo siguiente
  - El campo CLAVEPRIVADA pasa a ser un INTEGER con FK a ID de CORE\_CLAVE\_PRIVADA
  - El campo CLAVEPUBLICA pasa a ser un INTEGER con FK a ID de CORE\_CLAVE\_PUBLICA
  - Se añade el campo PLANTILLAXSLT
  - Se añade la tabla ORGANISMO\_CESIONARIO que contendrá los organismos cesionarios
  - Se añade la tabla SERVICIO\_AUTORIZADO\_CESIONARIO que contendrá las autorizaciones del organismo cesionario junto a su certificado de firma

## 1.6 Descripción cambios incluidos en Modelo de Datos Librerías SCSP 3.5.0

- Se añaden las siguientes secuencias:
  - ID\_AUTORIZACION\_ORGANISMO\_SEQ
  - ID\_AUTORIZACION\_CERTIFIC\_SEQ
  - ID\_SERVICIO\_SEQUENCE
  - ID\_EMITOR\_SEQUENCE
- En la tabla CORE\_SERVICIO se añaden los campos
  - ID (Pasa a ser la Primary Key)
- En la tabla CORE\_EMITOR\_CERTIFICADO se añaden los campos
  - ID (Pasa a ser la Primary Key)
- En la tabla AUTORIZACION\_ORGANISMO se añaden los campos
  - ID (Pasa a ser la Primary Key)
- En la tabla AUTORIZACION\_CERTIFICADO se añaden los campos
  - ID (Pasa a ser la Primary Key)

- IDCERTIFICADO

- En la tabla EMISOR\_BACKOFFICE se añade como Primary Key el campo CERTIFICADO
- En la tabla CORE\_CLAVE\_PRIVADA se añaden los campos
  - INTEROPERABILIDAD
- En la tabla SERVICIO\_AUTORIZADO\_CESIONARIO se añaden los campos
  - ORGANISMO

### 1.7 Descripción cambios incluidos en Modelo de Datos Librerías SCSP 3.5.3

- NO HAY CAMBIOS EN EL MODELO DE DATOS

### 1.8 Descripción cambios incluidos en Modelo de Datos Librerías SCSP 3.5.4

- NO HAY CAMBIOS EN EL MODELO DE DATOS

### 1.9 Descripción cambios incluidos en Modelo de Datos Librerías SCSP 3.5.5

- Se establece como **NOT NULL** el campo BLOQUEADO de la tabla SERVICIO\_AUTORIZADO\_CESIONARIO
- Se establece como **NOT NULL** el campo BLOQUEADO de la tabla ORGANISMO\_CESIONARIO

### 1.10 Descripción cambios incluidos en Modelo de Datos Librerías SCSP 3.5.6

- NO HAY CAMBIOS EN EL MODELO DE DATOS

### 1.11 Descripción cambios incluidos en Modelo de Datos Librerías SCSP 3.5.7

- NO HAY CAMBIOS EN EL MODELO DE DATOS

### 1.12 Descripción cambios incluidos en Modelo de Datos Librerías SCSP 4.0.0

- Se renombran las tablas a CORE\_\*
- Se renombran las tablas específicas del emisor a CORE\_EM\_\*
- Se modifica el campo PREFIJO de la tabla CORE\_EM\_SECUENCIA\_IDTRANS
- Se modifican los campos PREFIJO PETICION y PREFIJO IDTRANSMISION de la tabla CORE\_SERVICIO
- Se modifica el campo DESCRIPCION de la tabla CORE\_EM\_CODIGO\_ERROR\_SECUN
- Se modifica el campo MENSAJE de la tabla CORE\_LOG
- Se modifica el campo LOGO de la tabla CORE\_ORGANISMO\_CESIONARIO
- Se modifica el campo DATOS de la tabla CORE\_TOKEN\_DATA
- Se modifica el campo XMLTRANSMISION de la tabla CORE\_TRANSMISION
- Se genera la tabla CORE\_REQ\_MODULO\_PDF
- Se genera la tabla CORE\_REQ\_MODULO\_PDF\_CESIONARIO

### 1.13 Descripción cambios incluidos en Modelo de Datos Librerías SCSP 4.2.0

- Se añade el campo SSLFLAG a la tabla CORE\_REQ\_CESIONARIOS\_SERVICIOS

### 1.14 Descripción cambios incluidos en Modelo de Datos Librerías SCSP 4.3.0

- Se modifica el campo DOCTITULAR y EXPEDIENTE de la tabla CORE\_TRANSMISION
- Se añaden los campos ESTADO SECUNDARIO, CODIGO UNIDAD TRAMITADORA, SEUDONIMO FUNCIONARIO a la tabla CORE\_TRANSMISION
- Se añaden los campos ERROR SECUNDARIO y ESTADO SECUNDARIO a la tabla CORE\_PETICION\_RESPUESTA
- Se añade el campo XPATH CODIGO ERROR SECUNDARIO a la tabla CORE\_SERVICIO

- Se borra la columna ORDEN de la tabla CORE\_REQ\_MODULO\_PDF\_CESIONARIO si existe la columna
- Se modifica el campo CODIGOSECUNDARIO de la tabla CORE\_EM\_CODIGO\_ERROR\_SECUN

#### 1.15 Descripción cambios incluidos en Modelo de Datos Librerías SCSP 4.4.0

- NO HAY CAMBIOS EN EL MODELO DE DATOS

#### 1.16 Descripción cambios incluidos en Modelo de Datos Librerías SCSP 4.5.0

- Se añade el campo DESCRIPCION a la tabla CORE\_EM\_APLICACION
- Se añade el campo CODIGOUNIDADTRAMITADORA a la tabla CORE\_ORGANISMO\_CESIONARIO (*Modo Requirente*)

#### 1.17 Descripción cambios incluidos en Modelo de Datos Librerías SCSP 4.6.0

- Se añade el campo CODIGOUNIDADTRAMITADORA a la tabla CORE\_ORGANISMO\_CESIONARIO (*Modo Emisor*)

#### 1.18 Descripción cambios incluidos en Modelo de Datos Librerías SCSP 4.7.0

- NO HAY CAMBIOS EN EL MODELO DE DATOS

#### 1.19 Descripción cambios incluidos en Modelo de Datos Librerías SCSP 4.8.0

- Se añade el campo FECHAALTA a la tabla CORE\_EMITOR\_CERTIFICADO

#### 1.20 Descripción cambios incluidos en Modelo de Datos Librerías SCSP 4.11.1

- NO HAY CAMBIOS EN EL MODELO DE DATOS

#### 1.21 Descripción cambios incluidos en Modelo de Datos Librerías SCSP 4.15.0

- NO HAY CAMBIOS EN EL MODELO DE DATOS

## 1.22 Descripción cambios incluidos en Modelo de Datos Librerías SCSP 4.18.0

- Se modifica el tamaño del campo Estado correspondiente a la tabla CORE\_TRANSMISION

## 1.23 Descripción cambios incluidos en Modelo de Datos Librerías SCSP 4.20.0

- NO HAY CAMBIOS EN EL MODELO DE DATOS

## 1.24 Descripción cambios incluidos en Modelo de Datos Librerías SCSP 4.21.0

- NO HAY CAMBIOS EN EL MODELO DE DATOS

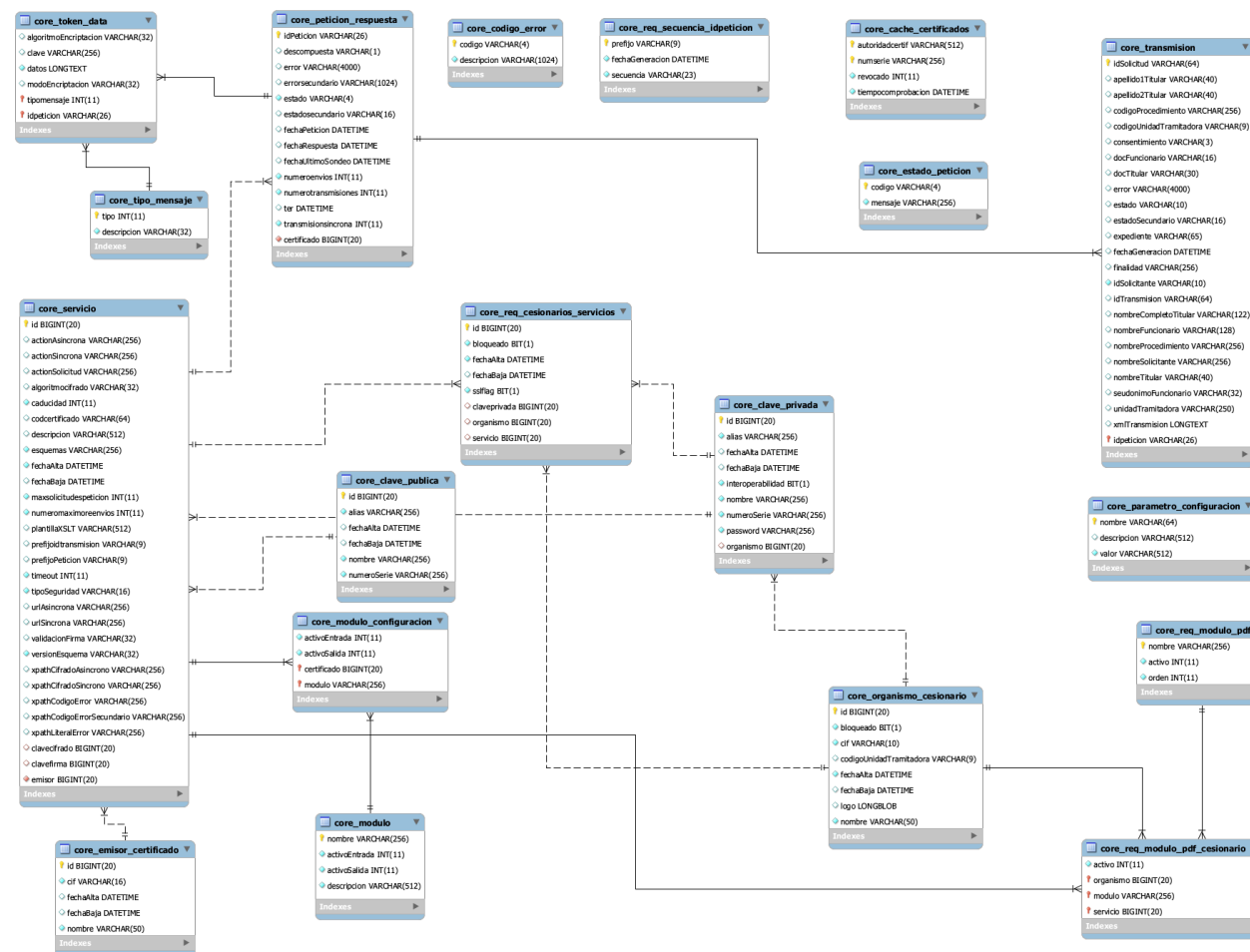
## 1.25 Descripción cambios incluidos en Modelo de Datos Librerías SCSP 4.22.0

- NO HAY CAMBIOS EN EL MODELO DE DATOS

## 1.26 Descripción cambios incluidos en Modelo de Datos Librerías SCSP 4.23.0

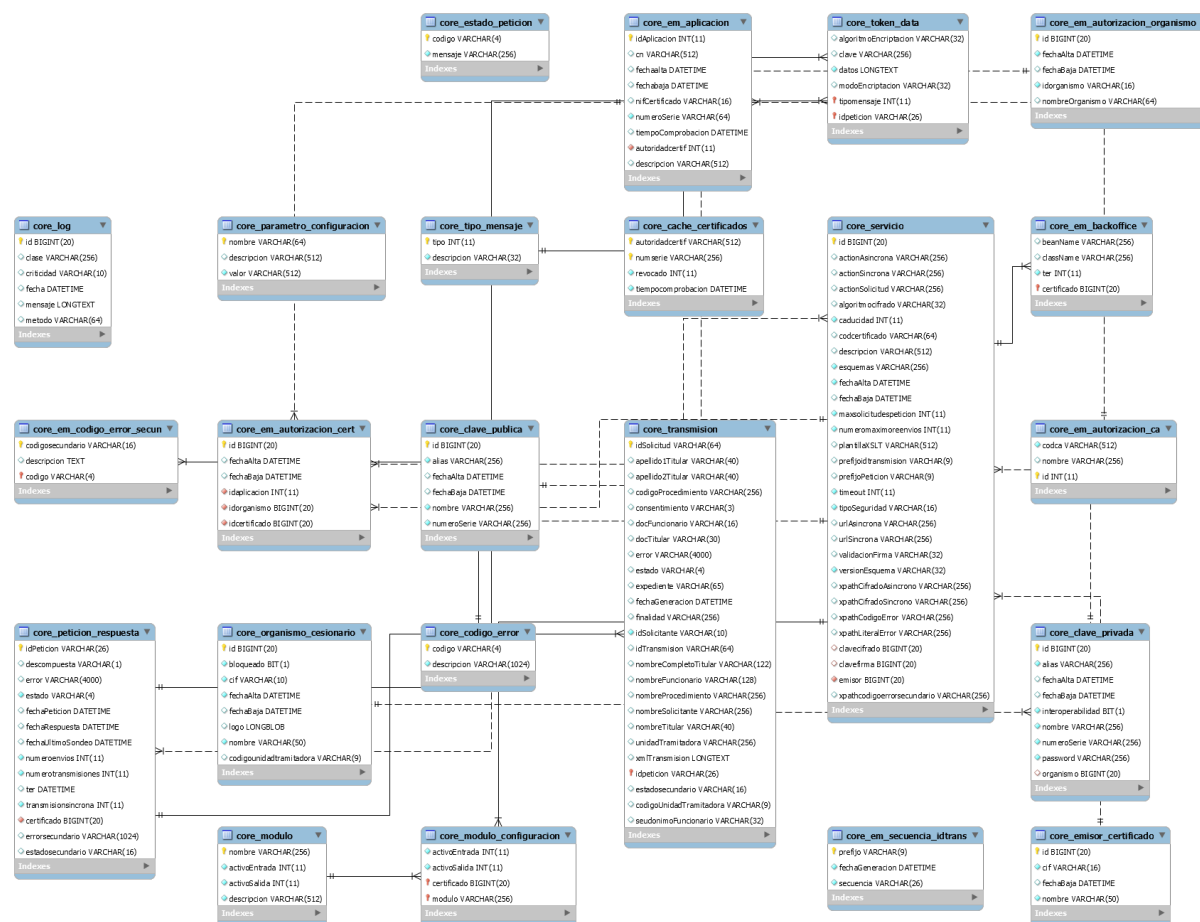
- NO HAY CAMBIOS EN EL MODELO DE DATOS

## 1.27 Diagrama Modelo de datos SCSP J2EE Requirente





## 1.28 Diagrama Modelo de datos SCSP J2EE Emisor



## 2 Descripción Tablas

### 2.1 Tablas comunes

#### 2.1.1 CORE\_SERVICIO

Esta tabla registrará cada uno de los certificados SCSP que van a ser utilizados por el sistema. En el caso del requirente corresponderán a los servicios que este vaya a consumir, mientras que en el caso del emisor corresponderán con los servicios que este vaya a ofrecer a otros organismos.

PK	Nombre	Tipo	Not Null	Único	Comentarios
TRUE	ID (PK)	INT	TRUE	TRUE	Id que identifica el registro
FALSE	CODCERTIFICADO	VARCHAR (64)	TRUE	TRUE	Código del certificado que lo identifica unívocamente en las comunicaciones SCSP.
FALSE	DESCRIPCION	VARCHAR (512)	TRUE	FALSE	Literal descriptivo del servicio a solicitar utilizando el código de certificado.
FALSE	EMISOR (FK)	INT	TRUE	FALSE	Nombre del emisor del certificado.
FALSE	FECHAALTA	DATETIME	TRUE	FALSE	Timestamp con la fecha en la cual el certificado se dió de alta en el sistema y por lo tanto a partir de la cual se podrán emitir peticiones al mismo.
FALSE	FECHABAJA	DATETIME	FALSE	FALSE	Timestamp con la fecha en la cual el certificado se dio de baja en el sistema y por tanto a partir de la cual no se podrán emitir peticiones al mismo.
FALSE	CADUCIDAD	INTEGER	TRUE	FALSE	Número de días que deberán sumarse a la fecha de respuesta de una petición, para calcular la fecha a partir de la cual se podrá considerar que la respuesta está caducada y se devolverá el error scsp correspondiente para indicar que la respuesta ha perdido su valor.
FALSE	URLSINCRONA	VARCHAR (256)	FALSE	FALSE	Endpoint de acceso al servicio de tipo síncrono
FALSE	URLASINCRONA	VARCHAR (256)	FALSE	FALSE	Endpoint de acceso al servicio de tipo asíncrono del certificado
FALSE	ACTIONSINCRONA	VARCHAR (256)	FALSE	FALSE	Valor del Soap:Action de la petición síncrona utilizado por el servidor WS en el caso de que sea necesario.

PK	Nombre	Tipo	Not Null	Único	Comentarios
FALSE	ACTIONASINCRONA	VARCHAR (256)	FALSE	FALSE	Valor del Soap:Action de la petición asíncrona utilizado por el servidor WS en el caso de que sea necesario.
FALSE	ACTIONSOLICITUD	VARCHAR (256)	FALSE	FALSE	Valor del Soap:Action de la solicitud asíncrona de respuesta utilizado por el servidor WS en el caso de que sea necesario.
FALSE	VERSIONESQUEMA	VARCHAR (32)	TRUE	FALSE	Indica la versión de esquema utilizado en los mensajes SCSP.  Puede tomar los valores V2 y V3.
FALSE	TIPOSEGURIDAD	VARCHAR (16)	TRUE	FALSE	Indica el tipo de firma a utilizar en los mensajes.  Puede tomar los valores  XMLSignature y WS-Security.
FALSE	CLAVEFIRMA (FK)	INTEGER	FALSE	FALSE	Id que identifica unívocamente, en el almacén de claves configurado, la clave privada con la que se firmarán los mensajes.
FALSE	CLAVECIFRADO (FK)	INTEGER	FALSE	FALSE	Id que identifica unívocamente, en el almacén de claves configurado, el certificado de clave pública con el que se cifrarían los mensajes enviados, en caso de que sean necesario el uso de cifrado.
FALSE	XPATHCIFRADOSINCRONO	VARCHAR (256)	FALSE	FALSE	En el caso de las comunicaciones síncronas, se trata del literal que identifica el nodo del mensaje XML a cifrar en caso de que los mensajes intercambiados deban viajar cifrados. Se corresponde con una expresión xpath que permite localizar al nodo en el mensaje XML.  Tendrá el siguiente formato  //*[local-name()='NODO_A_CIFRAR']  donde 'NODO_A_CIFRAR' es el local name del nodo que se desea cifrar.  Ej://*[local-name()='DatosEspecificos']
FALSE	XPATHCIFRADOASINCRONO	VARCHAR (256)	FALSE	FALSE	En el caso de las comunicaciones asíncronas, se trata del literal que identifica el nodo del mensaje

PK	Nombre	Tipo	Not Null	Único	Comentarios
					<p>XML a cifrar en caso de que los mensajes intercambiados deban viajar cifrados. Se corresponde con una expresión xpath que permite localizar al nodo en el mensaje XML.</p> <p>Tendrá el siguiente formato</p> <pre>//*[local-name()='NODO_A_CIFRAR']</pre> <p>donde 'NODO_A_CIFRAR' es el local name del nodo que se desea cifrar.</p> <p>Ej: <code>//*[local-name()='DatosEspecificos']</code></p>
FALSE	ALGORITMOCIFRADO	VARCHAR (32)	FALSE	FALSE	<p>Literal que identifica el algoritmo utilizado para el cifrado de los mensajes SCSP.</p> <p>Debe poseer un valor reconocido por las librerías de Rampart:</p> <ul style="list-style-type: none"> <li>- Basic128Rsa15: En caso de que el cifrado sea con AES128</li> <li>- TripleDesRsa15: En caso de que el cifrado sea con con TripleDes</li> <li>- Basic256Rsa15: En caso de que el cifrado sea con AES256</li> </ul>
FALSE	PREFIJOPETICION	VARCHAR (9)	FALSE	FALSE	<p>Literal con una longitud máxima de 8 caracteres y mínima de 3, el cual será utilizado para la construcción de los identificadores de petición, anteponiéndose a un valor secuencial. Mediante este literal pueden personalizarse los identificadores de petición haciéndolos más descriptivos.</p>
FALSE	ESQUEMAS	VARCHAR (256)	FALSE	FALSE	<p>Ruta que indica el directorio donde se encuentran los esquemas (*.xsd) con el que se validará el XML de los diferentes mensajes intercambiados. Esta ruta podrá tomar un valor relativo haciendo referencia al classpath de la aplicación o un path absoluto.</p>
FALSE	NUMEROMAXIMOREENVIOS	INTEGER	TRUE	FALSE	<p>Valor que indica en el caso del requirente, el número máximo de solicitudes de respuesta que</p>

PK	Nombre	Tipo	Not Null	Único	Comentarios
					<p>pueden realizarse sobre una petición asíncrona.</p> <p>En el caso del emisor, hace referencia al número máximo de veces que devolverá una respuesta para las solicitudes de respuesta que se hagan sobre una misma petición.</p>
FALSE	MAXSOLICITUDESPETICION	INTEGER	TRUE	FALSE	Número máximo de solicitudes de transmisión que se van a permitir por petición asíncrona.
FALSE	PREFIJOIDTRANSMISION	VARCHAR (9)	FALSE	FALSE	Semilla empleada por el emisor para generar los identificadores de transmisión de las respuestas. Será un valor alfanumérico con un mínimo de 3 caracteres y un máximo de 8.
FALSE	XPATHCODIGOERROR	VARCHAR (8)	FALSE	FALSE	<p>Se corresponde con una expresión xpath que permite localizar al nodo estipulado para contener el código de estado de la transmisión dentro de los datos específicos.</p> <p>Tendrá el siguiente formato</p> <p><code>//*[local-name()='NODO_DE_ESTADO]</code></p> <p>donde 'NODO_DE_ESTADO' es el local name del nodo que se desea cifrar.</p> <p>Su valor se buscará siempre bajo el nodo &lt;DatosEspecificos&gt;</p>
FALSE	XPATHCODIGOERRORSECUNDARIO	VARCHAR (256)	FALSE	FALSE	<p>Se corresponde con una expresión xpath que permite localizar al nodo estipulado para contener el código de estado secundario de la transmisión dentro de los datos específicos.</p> <p>Tendrá el siguiente formato</p> <p><code>//*[local-name()='NODO_DE_ESTADO]</code></p> <p>donde 'NODO_DE_ESTADO' es el local name del nodo que se desea cifrar.</p> <p>Su valor se buscará siempre bajo el nodo &lt;DatosEspecificos&gt;</p>

PK	Nombre	Tipo	Not Null	Único	Comentarios
FALSE	XPATHLITERALERROR	VARCHAR (256)	FALSE	FALSE	<p>Se corresponde con una expresión xpath que permite localizar al nodo estipulado para contener el mensaje descriptivo del estado de la transmisión dentro de los datos específicos.</p> <p><b>Tendrá el siguiente formato</b></p> <p><b>//*[local-name()='NODO_ERROR_LITERAL']</b></p> <p><b>donde 'NODO_ERROR_LITERAL' es el local name del nodo que se desea cifrar.</b></p> <p><b>Su valor se buscará siempre bajo el nodo &lt;DatosEspecificos&gt;</b></p>
FALSE	TIMEOUT	INTEGER	TRUE	FALSE	<p>Tiempo medido en segundos que se considerará como timeout en las comunicaciones realizadas entre los requirentes y emisores. Por defecto tendrá el valor 60.</p>
FALSE	VALIDACIONFIRMA	VARCHAR (32)	FALSE	FALSE	<p>Columna que contendrá el tipo de validación de firma para el caso del emisor (en el caso del requirente, esta columna no tendrá uso). Sus posibles valores son:</p> <ul style="list-style-type: none"> <li>- Permisivo: El emisor acepta mensajes firmados en un estándar XMLSignature o Ws-Security con independencia de su configuración.</li> <li>- Estricto: El emisor solo permite mensajes firmados en el estándar configurado.</li> </ul>
FALSE	PLANTILLAXSLT	VARCHAR (215)	FALSE	FALSE	<p>Ruta a la plantilla XSLT de transformación del XML de respuesta a PDF. Esta ruta podrá tomar un valor relativo haciendo referencia al classpath de la aplicación o un path absoluto.</p>

### 2.1.2 CORE\_CLAVE\_PRIVADA

Esta tabla almacenará los datos de configuración necesarios para acceder a las claves privadas disponibles en el almacén de claves configurado.

Las claves privadas aquí configuradas serán las que se utilicen para la firma de los mensajes emitidos. Cada clave privada va a asociada a un organismo

PK	Nombre	Tipo	Not Null	Único	Comentarios
TRUE	ID (PK)	INT	TRUE	TRUE	Id que identifica de manera unívoca, dentro del almacén de claves que haya sido configurado en la core_parametro_configuracion bajo el 'keystoreFile' a la clave privada
FALSE	ALIAS	VARCHAR (256)	TRUE	FALSE	Alias que identifica el certificado, dentro del almacén de claves que haya sido configurado en la core_parametro_configuracion bajo el 'keystoreFile' a la clave privada.
FALSE	NOMBRE	VARCHAR (256)	TRUE	FALSE	Nombre descriptivo de la clave privada.
FALSE	PASSWORD	VARCHAR (256)	TRUE	FALSE	Password de la clave privada necesaria para hacer uso de la misma.
FALSE	NUMEROSERIE	VARCHAR (256)	TRUE	FALSE	Numero de serie de la clave privada
FALSE	ORGANISMO (FK)	INT	TRUE	FALSE	Organismo al que pertenece el certificado.
FALSE	FECHAALTA	DATETIME	TRUE	FALSE	Fecha de alta del certificado.
FALSE	FECHABAJA	DATETIME	FALSE	FALSE	Fecha de baja del certificado.
FALSE	INTEROPERABILIDAD	INT	FALSE	FALSE	Indica si una clave de firma puede ser utilizada por mas de un organismo.

### 2.1.3 CORE\_CLAVE\_PUBLICA

Esta tabla almacenará los datos de configuración necesarios para acceder a las claves públicas disponibles en el almacén de claves configurado.

Las claves públicas aquí configuradas serán las utilizadas para el cifrado de los mensajes emitidos.

PK	Nombre	Tipo	Not Null	Único	Comentarios
TRUE	ID (PK)	INT	TRUE	TRUE	Id que identifica de manera unívoca, dentro del almacén de claves que haya sido configurado en la tabla core_parametro_configuracion bajo el nombre 'keystoreFile', a la clave pública.
FALSE	ALIAS	VARCHAR (256)	TRUE	FALSE	Alias que identifica el certificado, dentro del almacén de claves que haya sido configurado en la tabla core_parametro_configuracion bajo el nombre 'keystoreFile', a la clave pública.
FALSE	NOMBRE	VARCHAR (256)	TRUE	FALSE	Nombre descriptivo de la clave pública.
FALSE	NUMEROSERIE	VARCHAR (256)	TRUE	TRUE	Numero de serie de la clave publica.
FALSE	FECHAALTA	DATETIME	TRUE	FALSE	Fecha de alta del certificado.
FALSE	FECHABAJA	DATETIME	FALSE	FALSE	Fecha de baja del certificado.

### 2.1.4 CORE\_EMITOR\_CERTIFICADO

Esta tabla almacenará los diferentes emisores de servicio configurados.

PK	Nombre	Tipo	Not Null	Único	Comentarios
TRUE	ID (PK)	INT	TRUE	TRUE	Id que identifica el registro
TRUE	NOMBRE	VARCHAR (50)	TRUE	TRUE	Nombre descriptivo del organismo emisor de servicios.
TRUE	CIF	VARCHAR (16)	TRUE	TRUE	CIF identificativo del organismo emisor de servicios.
FALSE	FECHAALTA	DATETIME	TRUE	FALSE	Fecha de alta del emisor de certificados.
FALSE	FECHABAJA	DATETIME	FALSE	FALSE	Fecha de baja del emisor de certificados.



## 2.1.5 CORE\_MODULO

Tabla que almacena la configuración de activación o desactivación de los módulos, a nivel global, que componen el ciclo de ejecución de las librerías SCSP.

Los módulos que existieran en esta tabla serán los siguientes:

- **AlmacenarBaseDatos:** Almacena en BBDD todos los mensajes XML intercambiados.
- **AlmacenarFichero:** Almacena en fichero todos los mensajes XML intercambiados.
- **AlmacenarFicheroPlain:** Si alguno de los mensajes intercambiados llega cifrado, este módulo se encarga de almacenarlo en claro en fichero.
- **ValidarCertificado:** Este módulo se encarga de la validación de los certificados con los que se firman los mensajes XML intercambiados.
- **ValidarEsquema:** Este módulo se encarga de la validación de la estructura de los mensajes XML intercambiados.

PK	Nombre	Tipo	Not Null	Único	Comentarios
TRUE	NOMBRE (PK)	VARCHAR (256)	TRUE	TRUE	Nombre del módulo
FALSE	DESCRIPCION	VARCHAR (512)	FALSE	FALSE	Nombre del módulo
FALSE	ACTIVOENTRADA	INTEGER	TRUE	FALSE	Valor que indica si el módulo esta activo o no en la emisión de mensajes. Puede tomar valor 1 (Activo) ó 0 (Inactivo)
FALSE	ACTIVOSALIDA	INTEGER	TRUE	FALSE	Valor que indica si el módulo esta activo en la recepción de mensajes. Puede tomar valor 1 (Activo) ó 0 (Inactivo)

### 2.1.6 CORE\_MODULO\_CONFIGURACION

Tabla que permite tener una configuración de los módulos, distinta a la global (tabla core\_modulo) para un servicio en concreto

De manera que se podría tener por ejemplo, activa la Validación de esquemas tanto en el envío de mensajes como en la recepción de los mismos de manera global y, tenerla desactiva en la emisión de servicios para por ejemplo, el servicio de consulta de datos de identidad.

PK	Nombre	Tipo	Not Null	Único	Comentarios
TRUE	MODULO (PK-FK)	VARCHAR (256)	TRUE	FALSE	Nombre del módulo a configurar
FALSE	CERTIFICADO (PK FK)	INT	TRUE	FALSE	Código del certificado solicitado
FALSE	ACTIVOENTRADA	INTEGER	TRUE	FALSE	Valor que indica si el módulo está activo en la emisión de mensajes. Puede tomar valor 1 (Activo) ó 0 (Inactivo)
FALSE	ACTIVOSALIDA	INTEGER	TRUE	FALSE	Valor que indica si el módulo está activo en la recepción de mensajes. Puede tomar valor 1 (Activo) ó 0 (Inactivo)

### 2.1.7 CORE\_PARAMETRO\_CONFIGURACION

Tabla que almacena aquellos parámetros de configuración que son globales a todos los servicios que se configuren.

PK	Nombre	Tipo	Not Null	Único	Comentarios
TRUE	NOMBRE (PK)	VARCHAR (64)	TRUE	TRUE	Nombre identificativo del parámetro.
FALSE	VALOR	VARCHAR (512)	TRUE	FALSE	Valor del parámetro.
FALSE	DESCRIPCION	VARCHAR (512)	FALSE	FALSE	Literal descriptivo de la utilidad del parámetro.

Los parámetros que contendrá esta tabla son los siguientes:

PARAMETRO	VALOR	DESCRIPCIÓN
<b>afirma.enabled</b>	<b>TRUE/FALSE</b>	<p>Este campo nos indica si la comunicación con @firma para la validación de certificados se encuentra activa o no.</p> <ul style="list-style-type: none"> <li>Si el valor es <i>TRUE</i>, estará activa y deberán estar rellenos los siguientes campos de esta tabla: <ul style="list-style-type: none"> <li><b>afirma.url</b></li> <li><b>afirma.idAplicacion</b></li> <li><b>afirma.modoValidacion</b></li> <li><b>afirma.autenticacion.aliasSignerCert</b></li> </ul> y el campo <b>custom.cert.validation.class</b> de esta tabla deberá tener como valor 'none'.</li> <li>Si el valor es <i>FALSE</i> la validación no se realizará mediante @firma sino mediante una clase propia que implemente la validación de certificados. En este caso se deberá rellenar el siguiente campo de esta tabla: <ul style="list-style-type: none"> <li><b>custom.cert.validation.class</b></li> </ul> y los siguientes campos de esta tabla deberán tener como valor 'none' <ul style="list-style-type: none"> <li><b>afirma.url</b></li> <li><b>afirma.idAplicacion</b></li> <li><b>afirma.modoValidacion</b></li> <li><b>afirma.autenticacion.aliasSignerCert</b></li> </ul> </li> </ul> <p>Para más información sobre como implementar la clase propia para validación de certificados véase "Manual para</p>

PARAMETRO	VALOR	DESCRIPCIÓN
<i>Desarrolladores sobre Librerías J2EE SCSP.docx, en el punto Implementación propia de validación de certificados".</i>		
<b>afirma.autenticacion.aliasSignerCert</b>	Cadena de caracteres	<p>El valor de este campo será el alias del certificado con el que se firmarán las peticiones de validación de certificados que se envíen a @firma.</p> <p><b>Este alias de certificado deberá existir en el almacén de claves configurado en la tabla 'core_parametro_configuracion' bajo el nombre 'keystoreFile'.</b></p>
<b>afirma.idAplicacion</b>	Cadena de caracteres	<p>Identificador de aplicación proporcionado por @firma con el fin de identificar a la aplicación que envía peticiones a sus servicios.</p> <p><b>Debe ser un identificador de aplicación con autenticación mediante certificado.</b></p>
<b>afirma.modoValidacion</b>	1/2	<p>Indica el modo de validación de los certificados.</p> <p><b>Valores posibles:</b></p> <ul style="list-style-type: none"> <li>1: Con este modo de validación se comprueba la caducidad, integridad, confianza y estado de revocación del certificado.</li> <li>2: Con este modo de validación se realizan las comprobaciones del modo 1 y además se valida la cadena de confianza al completo.</li> </ul>
<b>afirma.url</b>	Cadena de caracteres formato URL	<p>Este valor es la url de donde se encuentra el servicio de validación de certificados de @firma.</p> <p><b>PRE</b> <a href="https://des-afirma.redsara.es/afirmaws/services/ValidarCertificado">https://des-afirma.redsara.es/afirmaws/services/ValidarCertificado</a></p> <p><b>PRO</b> <a href="https://afirma.redsara.es/afirmaws/services/ValidarCertificado">https://afirma.redsara.es/afirmaws/services/ValidarCertificado</a></p>
<b>almacenamiento.ficheros</b>	Cadena de caracteres formato de Path.	<p>Directorio donde se van a almacenar los ficheros de las distintas mensajes SCSP que se intercambien.</p> <p><b>Debe ser un path absoluto.</b></p>
<b>almacenamiento.transmisiones</b>	0/1	<p>Este parámetro indica si en el campo 'xmltransmision' de la tabla 'core_transmision' se almacenará el XML correspondiente a cada una de las transmisiones de datos que se realicen (xml del nodo TransmisionDatos).</p> <p><b>Valores posibles</b></p> <p>1: Se almacenan los XML de las transmisiones.</p>

PARAMETRO	VALOR	DESCRIPCIÓN
		0: No se almacenan los XML de las transmisiones.
<b>cif.solicitante</b>	Cadena de caracteres alfanumérico	Cadena de caracteres de tipo alfanumérico que contiene el CIF del organismo Emisor.
<b>custom.cert.validation.class</b>	Nombre completo de una clase JAVA	<p>Este parámetro se deberá rellenar cuando la validación de certificados se quiera realizar con una clase propia.</p> <p><b>El formato que deberá tener es el siguiente</b></p> <p><b>&lt;paquete&gt;.&lt;nombre_de_la_clase&gt;</b>,</p> <p>Además para que la validación se haga con la clase aquí indicada, se deberá poner parámetro afirma.enabled de esta tabla a <b>FALSE</b>.</p> <p><b>Ej: es.map.validacion.ClaseValidacion</b></p> <p>Para más información sobre como implementar la clase propia para validación de certificados véase “Manual para Desarrolladores sobre Librerías J2EE SCSP.docx, en el punto Implementación propia de validación de certificados”.</p>
<b>keystoreFile</b>	Cadena de caracteres con formato de Path	<p>Este parámetro contiene la ruta en la que se encuentra el keystore donde se almacenan los certificados que se emplearan para la firma de las peticiones y, los certificados de cifrado en caso de que fuera necesario que las peticiones se enviasen cifradas.</p> <p>Deberá cumplir el siguiente formato:</p> <ul style="list-style-type: none"> <li>• <u>Si el keystore es un fichero externo a la aplicación (no está contenido en el .war o .jar):</u></li> </ul> <p><b>file:/c:\directorio_keystore\nombre_almacen.jks</b></p> <p>- <u>Si el keystore es un fichero interno a la aplicación:</u></p> <p><b>classpath:/nombre_almacen.jks</b></p> <p>donde nombre_almacen será el nombre que tenga el almacen de claves.</p>
<b>keystorePass</b>	Cadena de caracteres	Password del keystore.
<b>keystoreType</b>	JKS	<p>Cadena de caracteres con el tipo de keystore que estamos utilizando.</p> <p><b>Valores posibles</b></p> <p><b>JKS</b></p>
<b>nivelTraza</b>	DEBUG ERROR,INFO	Cadena de caracteres con el nivel de traza.

PARAMETRO	VALOR	DESCRIPCIÓN
<p><b>WARN_FATAL</b></p> <p>Los valores posibles, de más a menos nivel de traza, son : DEBUG, ERROR, INFO, WARN o FATAL</p>		
nombre.solicitante	Cadena caracteres	de Es una cadena de caracteres que contiene el nombre del Emisor:  Ej: MPTAP
pathLogs	Cadena caracteres	de Contiene el path completo del fichero de log de la aplicación.
prefijo.idpeticion	Cadena caracteres	de Contiene el prefijo a utilizar en la generación de los identificadores de petición.  Deberá estar constituido por un mínimo de 3 caracteres y un máximo de 8.
polling.enabled	TRUE/FALSE	Valor que indica si se encuentra activo o no el proceso de polling.  Los valores posibles son: <ul style="list-style-type: none"> <li>TRUE: El polling está activo</li> <li>FALSE: el polling no está activo.</li> </ul> En caso de querer activar el polling se deberá configurar también los parámetros de esta tabla:  task.polling.intervalo task.polling.espera
task.polling.intervalo	Valor numérico	Valor numérico que indica cada cuanto tiempo se ejecuta el proceso de polling. Se indica en minutos.  Aunque el polling no este activo este campo deberá existir y, se deberá rellenar con algun valor numérico (por ejemplo 0).
task.polling.espera	Valor numérico	Valor numérico que indica el tiempo a esperar desde que se inicia la aplicación, para que el polling se ejecute por primera vez. Se indica en milisegundos.  Aunque el polling no este activo este campo deberá existir y, se deberá rellenar con algun valor numérico (por ejemplo 0).
task.polling.size	Valor numérico	Número de peticiones máximo a ser tratadas por ciclo de polling
tipoid	Short/long	Indica la longitud del identificador de petición para los servicios SCSPv3.  Los valores posible son:

PARAMETRO	VALOR	DESCRIPCIÓN
		<ul style="list-style-type: none"> <li>• short → 16 bytes</li> <li>• long → 29 bytes</li> </ul> <p>Se recomienda el uso de <i>long</i>.</p>
periodo.validacion.certificados	Valor numérico	Parametro de la cache de certificados, que permite indicar el número de horas durante las que se considerará válida la respuesta de @Firma considerando válido un certificado y durante el cual no habrá que ir a validar el certificado.
prefijo.idtransmision	Cadena de caracteres	<p>Contiene el prefijo a utilizar en la generación de los identificadores de transmisión por el emisor.</p> <p><b>Deberá estar constituido por un mínimo de 3 caracteres y un máximo de 8.</b></p>
logDinamico.enabled	TRUE/FALSE	Parámetro que permite que la configuración de los logs se pueda hacer dinámicamente a través de la configuración de base de datos o bien que la configuración la coja del fichero log4j.properties, si el valor que toma es FALSE, en caso contrario, es decir, si tomase un valor diferente a TRUE o FALSE, se cargará la configuración del fichero log4j.properties.
imagen.logo	Nombre de la imagen	Indica la imagen a mostrar en los justificantes PDF debe de incluirse en la ruta /images del archivo scsp-core-3.2.x.jar
version.datamodel.scsp	Versión del modelo de datos.	Versión del modelo de datos.
validate.nif.emisor.enabled	TRUE/FALSE	<p>Permite validar el Cif del Emisor de la petición con el configurado en BBDD</p> <p>Los valores posibles son:</p> <ul style="list-style-type: none"> <li>• TRUE: La validación está activa</li> <li>• FALSE: la validación no está activa.</li> </ul> <p>Por defecto si no se configura el valor será FALSE</p>

### 2.1.8 CORE\_PETICION\_RESPUESTA

Esta tabla registrará todas las peticiones y respuestas intercambiadas entre los requirentes y los emisores de servicios.

PK	Nombre	Tipo	Not Null	Único	Comentarios
TRUE	IDPETICION (PK)	VARCHAR (26)	TRUE	TRUE	Identificador unívoco de la petición de servicio.
FALSE	CERTIFICADO (FK)	INT	TRUE	FALSE	Código del certificado que se solicita en la petición
FALSE	ESTADO	VARCHAR (4)	TRUE	FALSE	Código identificativo del estado de la petición.  Tomará sus valores de las tablas core_estado_peticion y core_codigo_error
FALSE	ESTADOSECUNDARIO	VARCHAR (16)	FALSE	FALSE	Código identificativo del estado secundario de la petición.
FALSE	FECHAPETICION	DATETIME	TRUE	FALSE	Timestamp que indica la fecha en la que se generó la petición.
FALSE	FECHARESPUESTA	DATETIME	FALSE	FALSE	Timestamp que indica la fecha en la cual se recibió/envió la respuesta a la petición.
FALSE	TER	DATETIME	FALSE	FALSE	Timestamp que indica la fecha a partir de la cual una petición de tipo asíncrono podrá solicitar una respuesta definitiva al servicio.
FALSE	ERROR	VARCHAR (4000)	FALSE	FALSE	Mensaje descriptivo del error, si lo hubiera, en la solicitud del servicio.
FALSE	ERRORSECUNDARIO	VARCHAR (1024)	FALSE	FALSE	Mensaje descriptivo del error secundario, si lo hubiera, en la solicitud del servicio.
FALSE	NUMEROTRASMISIONES	INTEGER	TRUE	FALSE	Número de Solicitudes de Transmisión que se enviaron en la petición.
FALSE	NUMEROENVIOS	INTEGER	TRUE	FALSE	Valor que indica el número de solicitudes de respuesta que se han enviado para una petición asíncrona.
FALSE	TRANSMISIONSINCRONA	INTEGER	FALSE	FALSE	Valor binario que indica si la petición fue solicitada a un servicio de tipo síncrono o asíncrono.  Podrá tomar los valores: <ul style="list-style-type: none"> <li>0: La comunicación fue de tipo asíncrono,</li> </ul>



PK	Nombre	Tipo	Not Null	Único	Comentarios
					<ul style="list-style-type: none"> <li>1: La comunicación fue de tipo síncrono</li> </ul>
FALSE	FECHAULTIMOSONDEO	DATETIME	FALSE	FALSE	Timestamp que indica la fecha del último reenvío de una petición de tipo asíncrono.
FALSE	DESCOMPUESTA	VARCHAR (1)	FALSE	FALSE	<p>Caracter que indica el estado del procesamiento de las transmisiones de la respuesta recibida. Podrá tomar los siguientes valores:</p> <ul style="list-style-type: none"> <li>'S': Se ha procesado correctamente la respuesta, obtenido todas las transmisiones en ella incluidas y quedado registradas en la tabla core_transmision.</li> <li>'N': No han sido procesadas las transmisiones de la respuesta.</li> <li>'E': La respuesta terminó correctamente (estado 0003), pero se ha producido un error al procesar sus trasmisiones.</li> </ul>

### 2.1.9 CORE\_REQ\_SECUENCIA\_IDPETICION

Tabla que almacena las semillas (secuenciales) utilizadas para la generación de los identificadores de petición. Existirá un secuencial asociado a cada prefijo configurado y, en caso de no configurarse ningún prefijo se usará como tal el/los número/s de serie del/los certificado/s configurados para la firma.

PK	Nombre	Tipo	Not Null	Único	Comentarios
TRUE	PREFIJO (PK)	VARCHAR (9)	TRUE	TRUE	<p>Prefijo utilizado para la construcción de los identificadores.</p> <p>Dicho valor podrá ser:</p> <ul style="list-style-type: none"> <li>El prefijo especificado para cada servicio configurado en la tabla 'core_servicio',</li> <li>El prefijo especificado de manera</li> </ul>

					global en la tabla 'core_parametro_configuracion' o ante la no existencia de ninguno de estos,  Los 8 primeros dígitos del número de serie del certificado con el que se firmarán los mensajes SCSP.
FALSE	SECUENCIA	VARCHAR (23)	TRUE	FALSE	Valor secuencial que será concatenado al prefijo para generar los identificadores de petición..
FALSE	FECHAGENERACION	DATETIME	TRUE	FALSE	Fecha en la que se registró el secuencial

### 2.1.10 CORE\_TIPO\_MENSAJE

Tabla maestra que almacena los diferentes tipos de mensajes que pueden ser intercambiados a lo largo de un ciclo de comunicación SCSP. Estos valores serán:

- Peticion
- Respuesta
- SolicitudRespuesta
- ConfirmaciónPeticion
- Fault

PK	Nombre	Tipo	Not Null	Único	Comentarios
TRUE	TIPO (PK)	INTEGER	TRUE	TRUE	Tipo identificativo del mensaje  Los valores posibles son:  0: Peticion  1: Respuesta  2: ConfirmacionPeticion  3: SolicitudRespuesta  4: Fault
FALSE	DESCRIPCION	VARCHAR (32)	TRUE	FALSE	Literal descriptivo del tipo de mensaje

### 2.1.11 CORE\_TOKEN\_DATA

Esta tabla almacenará el contenido de los mensajes intercambiados en un proceso de comunicación SCSP.

PK	Nombre	Tipo	Not Null	Único	Comentarios
TRUE	IDPETICION (PK - FK)	VARCHAR (26)	TRUE	FALSE	Identificador de la petición a la cual está asociado el XML.
TRUE	TIPOMENSAJE (PK - FK)	INTEGER	TRUE	FALSE	Tipo de mensaje almacenado, podrá ser :  0: Peticion  1: Respuesta  2: ConfirmacionPeticion  3: SolicitudRespuesta  4: Fault
FALSE	DATOS	TEXT	TRUE	FALSE	Bytes del mensaje almacenado.
FALSE	CLAVE	VARCHAR (256)	FALSE	FALSE	Clave simétrica utilizada para el cifrado de los datos.
FALSE	MODOENCRIPCIÓN	VARCHAR (32)	FALSE	FALSE	Modo de encriptación utilizado para el proceso de cifrado. Por defecto será TransportKey.
FALSE	ALGORITMOENCRIPCIÓN	VARCHAR (32)	FALSE	FALSE	Algoritmo empleado en la encriptación del mensaje. Podrá tomar los siguientes valores:  - AES128  - AES256  - DESDe

## 2.1.12 CORE\_ TRANSMISION

Esta tabla almacenará la información específica de cada transmisión de datos que haya sido incluida en la respuesta de un servicio SCSP.

PK	Nombre	Tipo	Not Null	Único	Comentarios
TRUE	IDSOLICITUD (PK)	VARCHAR (64)	TRUE	FALSE	Identificador de la solicitud de transmisión dentro de las N posibles incluidas en una petición
TRUE	IDPETICION (PK – FK - IDX)	VARCHAR (26)	TRUE	FALSE	Identificador de la petición en la que se incluyó la solicitud de transmisión.
FALSE	IDTRANSMISION	VARCHAR (64)	FALSE	FALSE	Identificador de la transmisión que responde a la petición de servicio de la Solicitud de Transmisión identificada con idSolicitud.
FALSE	IDSOLICITANTE	VARCHAR (10)	TRUE	FALSE	CIF de organismo requirente.
FALSE	NOMBRESOLICITANTE	VARCHAR (256)	FALSE	FALSE	Nombre del organismo requirente.
FALSE	DOCTITULAR	VARCHAR (30)	FALSE	FALSE	Documento identificativo del titular sobre el cual se está realizando la petición de servicio.
FALSE	NOMBRETITULAR	VARCHAR (40)	FALSE	FALSE	Nombre del titular por el que se ha realizado la petición de servicio.
FALSE	APELLIDO1TITULAR	VARCHAR (40)	FALSE	FALSE	Primer apellido del titular por el que se ha realizado la petición de servicio.
FALSE	APELLIDO2TITULAR	VARCHAR (40)	FALSE	FALSE	Segundo apellido del titular por el que se ha realizado la petición de servicio.
FALSE	NOMBRECOMPLETOTITULAR	VARCHAR (122)	FALSE	FALSE	Nombre completo del titular por el que se ha realizado la petición de servicio.
FALSE	DOCFUNCIONARIO	VARCHAR (16)	FALSE	FALSE	Documento identificativo del funcionario que generó la solicitud de transmisión
FALSE	NOMBREFUNCIONARIO	VARCHAR (128)	FALSE	FALSE	Nombre del Funcionario que generó la solicitud de transmisión.
FALSE	SEUDONIMOFUNCIONARIO	VARCHAR (32)	FALSE	FALSE	Seudónimo del Funcionario que generó la solicitud de transmisión.
FALSE	FECHAGENERACION	DATETIME	FALSE	FALSE	Fecha en la que se generó la transmisión
FALSE	UNIDADTRAMITADORA	VARCHAR (256)	FALSE	FALSE	Unidad Tramitadora asociada a la solicitud de transmisión.
FALSE	CODIGOUNIDADTRAMITADORA	VARCHAR (9)	FALSE	FALSE	Código de Unidad Tramitadora asociada a la solicitud de transmisión.
FALSE	CODIGOPROCEDIMIENTO	VARCHAR (256)	FALSE	FALSE	Código del procedimiento en base al cual se puede solicitar el servicio

PK	Nombre	Tipo	Not Null	Único	Comentarios
FALSE	NOMBREPROCEDIMIENTO	VARCHAR (256)	FALSE	FALSE	Nombre del procedimiento en base al cual se puede solicitar el servicio
FALSE	EXPEDIENTE	VARCHAR (65)	FALSE	FALSE	Expediente asociado a la solicitud de transmisión.
FALSE	FINALIDAD	VARCHAR (256)	FALSE	FALSE	Finalidad por la cual se emitió la solicitud de transmisión
FALSE	CONSENTIMIENTO	VARCHAR (3)	FALSE	FALSE	Tipo de consentimiento asociado a la transmisión. Deberá tomar uno de los dos posibles valores:  - Si  -Ley
FALSE	ESTADO	VARCHAR (10)	FALSE	FALSE	Estado concreto en el que se encuentra la transmisión.
FALSE	ESTADOSECUNDARIO	VARCHAR (16)	FALSE	FALSE	Estado secundario concreto en el que se encuentra la transmisión.
FALSE	ERROR	TEXT	FALSE	FALSE	Descripción del posible error encontrado al solicitar la transmisión de servicio.
FALSE	XMLTRANSMISION	TEXT	FALSE	FALSE	XML de la transmisión de datos. Se almacenará si en la tabla "core_parametro_configuracion" el parámetro "almacenamiento.transmisiones" se puso a 1.

### 2.1.13 CORE\_CODIGO\_ERROR

Tabla que registrará los posibles errores genéricos que toda comunicación SCSP puede generar.

PK	Nombre	Tipo	Not Null	Único	Comentarios
TRUE	CODIGO (PK)	VARCHAR (4)	TRUE	TRUE	Código identificativo del error.
FALSE	DESCRIPCION	VARCHAR (1024)	TRUE	FALSE	Literal descriptivo del error

### 2.1.14 CORE\_ESTADO\_PETICION

Tabla que almacena los posibles estados en los que se puede encontrar una petición SCSP. Sus posibles valores serán:

- 0001 - Pendiente
- 0002 - En proceso
- 0003 – Tramitada
- 0004 – En proceso Polling

PK	Nombre	Tipo	Not Null	Único	Comentarios
TRUE	CODIGO (PK)	VARCHAR (4)	TRUE	TRUE	Código identificativo del estado.
FALSE	MENSAJE	VARCHAR (256)	TRUE	FALSE	Literal descriptivo del estado

### 2.1.15 CORE\_CACHE\_CERTIFICADOS

En esta tabla se almacenan, cada vez que se valida un certificado contra @firma, el numero de serie y la CA del certificado, la fecha en la que se realizó la validación y una indicación de si el certificado estaba revocado o no.

La siguiente vez que se recibe un mensaje firmado con el mismo certificado, no será necesario validarlo contra @firma si desde que se realizó la comprobación no han pasado el numero de horas definido en el parámetro “**periodo.validacion.certificados**” de la tabla “core\_parametro\_configuracion” que indica el periodo durante el que se considerará válida la respuesta de @firma.

El objetivo es evitar el numero de veces que se va a @firma para validar certificados.

PK	Nombre	Tipo	Not Null	Único	Comentarios
TRUE	NUMSERIE (PK)	VARCHAR (256)	TRUE	FALSE	Número de serie del certificado.
TRUE	AUTORIDADCERTIF (PK)	VARCHAR (512)	TRUE	FALSE	Autoridad certificadora que emitió el certificado.
FALSE	TIEMPOCOMPROBACION	DATETIME	TRUE	FALSE	Fecha en la que se realizó el proceso de validación del certificado por última vez.
FALSE	REVOCADO	INTEGER	TRUE	FALSE	Valor booleano ('1' o '0') que indicará: <ul style="list-style-type: none"> <li>• '1': si el proceso de validación revocó el certificado.</li> <li>• '0': si el proceso de validación aceptó el certificado.</li> </ul>

### 2.1.16 CORE\_ORGANISMO\_CESIONARIO

En esta tabla se almacenan los organismo cesionarios dados de alta en las librerías.

PK	Nombre	Tipo	Not Null	Único	Comentarios
TRUE	ID (PK)	INT	TRUE	TRUE	Id del organismo cesionario
FALSE	NOMBRE	VARCHAR (50)	TRUE	FALSE	Nombre del organismo cesionario
FALSE	CIF	VARCHAR (10)	TRUE	FALSE	CIF del organismo cesionario
FALSE	CODIGOUNIDADTRAMITADORA	VARCHAR (9)	FALSE	FALSE	Código DIR3 del organismo cesionario
FALSE	FECHAALTA	DATETIME	TRUE	FALSE	Fecha de alta del organismo cesionario
FALSE	FECHABAJA	DATETIME	FALSE	FALSE	Fecha de baja del organismo cesionario
FALSE	BLOQUEADO	INT	TRUE	FALSE	Indica si el organismo cesionario estará o no bloqueado
FALSE	LOGO	CLOB	FALSE	FALSE	Logo en formato binario del organismo cesionario

### 2.1.17 CORE\_REQ\_CESIONARIOS\_SERVICIOS

En esta tabla se almacenan las autorizaciones de los organismo cesionarios dados de alta en las librerías.

PK	Nombre	Tipo	Not Null	Único	Comentarios
TRUE	ID (PK)	INT	TRUE	TRUE	Id de la autorización
FALSE	SERVICIO (FK)	INT	TRUE	FALSE	Servicio para el que se autorizará al Organismo Cesionario
FALSE	CLAVEPRIVADA (FK)	INT (20)	TRUE	FALSE	Clave privada para la que se autorizará al Organismo Cesionario
FALSE	FECHAALTA	DATETIME	TRUE	FALSE	Fecha de alta de la autorización
FALSE	FECHABAJA	DATETIME	FALSE	FALSE	Fecha de baja de la autorización
FALSE	BLOQUEADO	INT	TRUE	FALSE	Indica si la autorización estará o no bloqueada
FALSE	ORGANISMO	INT	FALSE	FALSE	Indica el organismo al que pertenece la autorización.
FALSE	SSLFLAG	INT	TRUE	FALSE	Indica si para este servicio y organismo se utilizará el certificado específico al conectarse vía SSL

### 2.1.18 CORE\_REQ\_MODULO\_PDF

En esta tabla se almacenan los módulos para la configuración de los PDF de una forma general.

PK	Nombre	Tipo	Not Null	Único	Comentarios
TRUE	NOMBRE (PK)	VARCHAR (256)	TRUE	TRUE	Nombre del módulo
FALSE	ACTIVO	INT	TRUE	FALSE	Indica si está activo el módulo
FALSE	ORDEN	INT	TRUE	FALSE	Indica el orden de ejecución del módulo

### 2.1.19 CORE\_REQ\_MODULO\_PDF\_CESIONARIO

En esta tabla se almacenan los módulos para la configuración de los PDF por organismo cesionario.

PK	Nombre	Tipo	Not Null	Único	Comentarios
FALSE	ACTIVO	INT	TRUE	FALSE	Indica si está activo el módulo
FALSE	ORGANISMO (FK)	INT	TRUE	FALSE	Organismo al que aplicará la configuración
FALSE	MODULO (FK)	VARCHAR (256)	TRUE	FALSE	Nombre del módulo
FALSE	SERVICIO (FK)	INT	TRUE	FALSE	Servicio al que aplicará la configuración



## 2.2 Tablas entorno emisor

### 2.2.1 CORE\_EM\_BACKOFFICE

Tabla en la que se configura el módulo de backoffice del emisor que enlaza las comunicaciones SCSP con la logica de negocio especifica de cada organismo.

PK	Nombre	Tipo	Not Null	Único	Comentarios
TRUE	CERTIFICADO (PK - FK)	INT	TRUE	TRUE	Código del certificado gestionado por el backoffice
FALSE	BEANNAME	VARCHAR (256)	FALSE	FALSE	Identificador del bean del contexto de Spring que contiene la clase que ofrece la puerta de entrada al backoffice
FALSE	CLASSNAME	VARCHAR (256)	FALSE	FALSE	Nombre completo de la clase que ofrece la puerta de entrada al backoffice.
FALSE	TER	INTEGER	TRUE	FALSE	Número de horas que harán esperar a un requirente para la generación de una respuesta definitiva ante una petición asíncrona.

### 2.2.2 CORE\_EM\_CODIGO\_ERROR\_SECUN

Tabla de errores que permitirá almacenar aquellos mensajes de excepción gestionados por cada lógica de negocio específica de cada emisor, y que estará asociado a un error genérico de SCSP.

PK	Nombre	Tipo	Not Null	Único	Comentarios
TRUE	CODIGO (PK)	VARCHAR (4)	TRUE	FALSE	Código de error SCSP al que esta asociado el error secundario.
TRUE	CODIGOSECUNDARIO (PK - FK)	VARCHAR (16)	TRUE	FALSE	Código identificativo del error específico secundario.
FALSE	DESCRIPCION	TEXT	TRUE	FALSE	Literal descriptivo del mensaje de error secundario.

### 2.2.3 CORE\_EM\_APLICACION

En esta tabla se registran las aplicaciones de los organismos autorizadas a realizar consultas a los servicios ofrecidos por este.

La identificación de una aplicación, se realiza mediante el numero de serie del certificado y la autoridad de certificación que lo emite.

PK	Nombre	Tipo	Not Null	Único	Comentarios
TRUE	IDAPLICACION (PK)	INTEGER	TRUE	TRUE	Identificador de la aplicación. Se va a generar automáticamente.
FALSE	NIFCERTIFICADO	VARCHAR (16)	FALSE	FALSE	Nif del certificado con el que la aplicación firmara las peticiones
FALSE	NUMEROSERIE	VARCHAR (64)	TRUE	FALSE	Numero de serie del certificado con el que la aplicación firmara las peticiones
FALSE	CN	VARCHAR (512)	TRUE	FALSE	Common Name del certificado con el que la aplicación firmara las peticiones.
FALSE	TIEMPOCOMPROBACION	DATETIME	FALSE	FALSE	Fecha en que la aplicación realizo el ultimo acceso al servicio del emisor.
FALSE	AUTORIDADCERTIF (FK)	VARCHAR (512)	FALSE	FALSE	Autoridad de certificación del certificado
FALSE	FECHAALTA	DATETIME	FALSE	FALSE	Fecha en la que se da de alta la aplicación.
FALSE	FECHABAJA	DATETIME	FALSE	FALSE	Fecha a partir de la cual la aplicación no va a poder acceder a ningún servicio.
FALSE	DESCRIPCION	VARCHAR (512)	FALSE	FALSE	Descripción del certificado dado de alta

### 2.2.4 CORE\_EM\_AUTORIZACION\_CA

Contiene información relativa a distintas autoridades de certificación.

PK	Nombre	Tipo	Not Null	Único	Comentarios
TRUE	CODCA (PK)	VARCHAR (512)	TRUE		Codigo de la autoridad de certificación (Ej: FNMT)
FALSE	NOMBRE	VARCHAR (256)	FALSE		Nombre de la autoridad de certificación (Ej: Fabrica Nacional de Moneda y Timbre)

### 2.2.5 CORE\_EM\_AUTORIZACION\_CERT

Contiene la información relativa a las autorizaciones de los distintas aplicaciones para acceder a los servicios ofrecidos por el emisor.

PK	Nombre	Tipo	Not Null	Único	Comentarios
TRUE	ID (PK)	INTEGER	TRUE	TRUE	Id que identifica el registro
FALSE	IDAPLICACION	INTEGER	TRUE	FALSE	Identificador de la aplicación autorizada
FALSE	IDCERTIFICADO	INTEGER	TRUE	FALSE	Identificador del certificado autorizado
FALSE	IDORGANISMO	VARCHAR (16)	TRUE	FALSE	Identificador del organismo solicitante
FALSE	FECHAALTA	TIMESTAMP	TRUE	FALSE	Fecha de alta de la autorización
FALSE	FECHABAJA	TIMESTAMP	FALSE	FALSE	Fecha de baja de la autorización

### 2.2.6 CORE\_EM\_AUTORIZACION\_ORGANISMO

Organismos que están dados de alta en el emisor y que van a poder consultar los servicios ofrecidos por este a través de alguna de las aplicaciones que tienen autorización para consultar los servicios.

PK	Nombre	Tipo	Not Null	Único	Comentarios
TRUE	ID (PK)	INTEGER	TRUE	TRUE	Id que identifica el registro
FALSE	IDORGANISMO	VARCHAR (16)	TRUE	FALSE	Identificador del organismo
FALSE	NOMBREORGANISMO	VARCHAR (64)	FALSE	FALSE	Nombre descriptivo del organismo requirente de servicios
FALSE	FECHAALTA	DATETIME	TRUE	FALSE	Fecha en la que se da de alta el organismo
FALSE	FECHABAJA	DATETIME	FALSE	FALSE	Fecha a partir de la cual el organismo no va a poder enviar peticiones.

### 2.2.7 CORE\_EM\_SECUENCIA\_IDTRANS

Tabla utilizada para la generación de los valores de los nodos IdTransmisión en los emisores, en caso de que estos identificadores no sean generados por el backoffice.

PK	Nombre	Tipo	Not Null	Único	Comentarios
TRUE	PREFIJO (PK)	VARCHAR (9)	TRUE	TRUE	Prefijo de IdTransmisiones al que estará asociada la secuencia.
FALSE	SECUENCIA	VARCHAR (26)	TRUE	FALSE	Valor actual de la secuencia alfanumérica asociada al prefijo.
FALSE	FECHAGENERACION	DATETIME	TRUE	FALSE	Última fecha en la que se ha generado un valor de secuencia.