

GOBIERNO DE ESPAÑA
MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA

Sustitución de Certificados en Soporte Papel



DGIAE
Ministerio de la Política Territorial y Administración Pública

DIRECCIÓN GENERAL PARA EL IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA

04/11/2011 1

GOBIERNO DE ESPAÑA
MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA

Sustitución de Certificados en Soporte Papel

Índice

1. **Protocolo de Sustitución de certificados en papel**
2. Esquemas de intercambio de datos SCSP
3. Librerías SCSPv3
4. Recubrimiento SCSP_WS



DIRECCIÓN GENERAL PARA EL IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA

04/11/2011 2

GOBIERNO DE ESPAÑA
MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA

Sustitución de Certificados en Soporte Papel

Objetivo: el derecho del ciudadano

Afecta a múltiples procedimientos y diversos certificados.

Reduce cargas administrativas

Simplificar los procedimientos

Calidad de los datos. Evita errores

Consulta on-line inmediata

Aportar documentos al final del proceso por el organismo

DIRECCIÓN GENERAL PARA EL IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA

04/11/2011 3 3

GOBIERNO DE ESPAÑA
MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA

Sustitución de Certificados en Soporte Papel

Evolución de las soluciones de Intercambio de datos

NTI Protocolos Interoperabilidad

Cliente ligero 2010

Plataforma 2009

SVDI/SVDR 2007

SCSP 2004

Especificaciones para la sustitución de certificados en papel.
 Librerías que se instalan en cada uno de los organismos.
 Comunicación bidireccional.
 Simplifica la interoperabilidad
 Facilita la integración del backoffice.
 SCSPv2

DIRECCIÓN GENERAL PARA EL IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA

04/11/2011 4

GOBIERNO DE ESPAÑA MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA

Sustitución de Certificados en Soporte Papel

Evolución de las soluciones de Intercambio de datos

NTI Protocolos Interoperabilidad

Cliente ligero 2010

Plataforma 2009

SVDI/SVDR 2007

SCSP 2004

Eliminación de aportar las fotocopias de DNI y el volante de empadronamiento. Primer Germen de la plataforma de intermediación.

DIRECCIÓN GENERAL PARA EL IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA

04/11/2011 5

GOBIERNO DE ESPAÑA MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA

Sustitución de Certificados en Soporte Papel

Evolución de las soluciones de Intercambio de datos

NTI Protocolos Interoperabilidad

Cliente ligero 2010

Plataforma 2009

SVDI/SVDR 2007

SCSP 2004

Extensión del modelo intermediación construyendo la actual plataforma de intermediación. Fomento de la integración de aplicaciones

DIRECCIÓN GENERAL PARA EL IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA

04/11/2011 6

GOBIERNO DE ESPAÑA
MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA

Sustitución de Certificados en Soporte Papel

Evolución de las soluciones de Intercambio de datos

NTI Protocolos Interoperabilidad

Cliente ligero 2010

Plataforma 2009

SVDI/SVDR 2007

SCSP 2004

Desarrollo del cliente ligero para promover la consulta de forma inmediata.
Aplicación web, intuitiva segura, auditable.
No necesita ningún desarrollo por parte del organismo.
Especificación SCSPv3

DIRECCIÓN GENERAL PARA EL IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA

04/11/2011 7

GOBIERNO DE ESPAÑA
MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA

Sustitución de Certificados en Soporte Papel

Evolución de las soluciones de Intercambio de datos

NTI Protocolos Interoperabilidad 2011

Cliente ligero 2010

Plataforma 2009

SVDI/SVDR 2007

SCSP 2004

Se amplían funcionalidades del Cliente Ligero y de las Librerías SCSPv3
Rediseño del Modelo de datos

Especificación SCSPv3 pieza fundamental de la NTI de Protocolos de Interoperabilidad

DIRECCIÓN GENERAL PARA EL IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA

04/11/2011 8

Sustitución de Certificados en Soporte Papel

Objetivo

- Especificación de un Protocolo de intercambio de datos extensible e interoperable → síncrono y asíncrono
- Desarrollo de unas librerías (J2EE y .NET) reutilizables por las AAPP que implementa el protocolo.
- Facilita el desarrollo de aplicaciones cliente o servicios de publicación de certificados, de una forma más ágil, sencilla y validada.
- Facilita la sustitución de certificados en papel por transmisiones de datos.

DIRECCIÓN GENERAL PARA EL IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA

04/11/20119

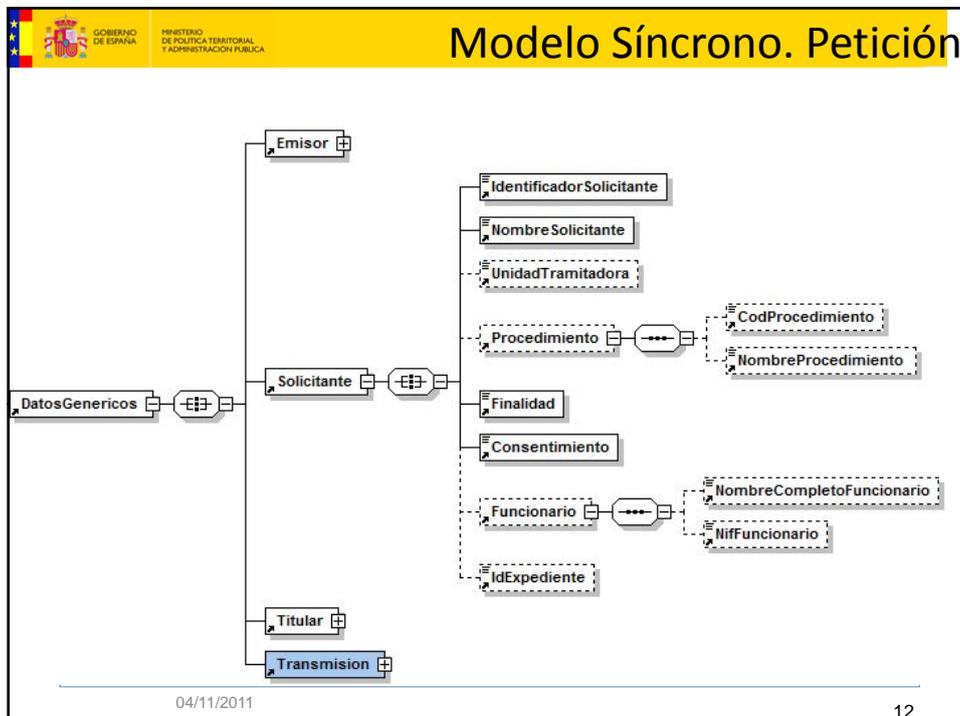
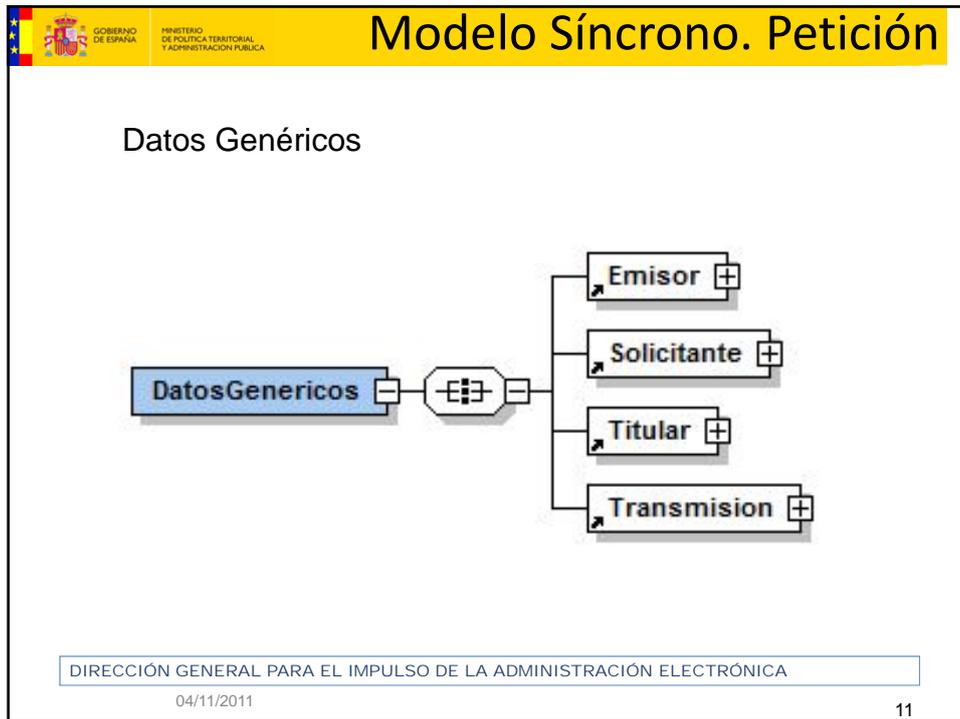
Sustitución de Certificados en Soporte Papel

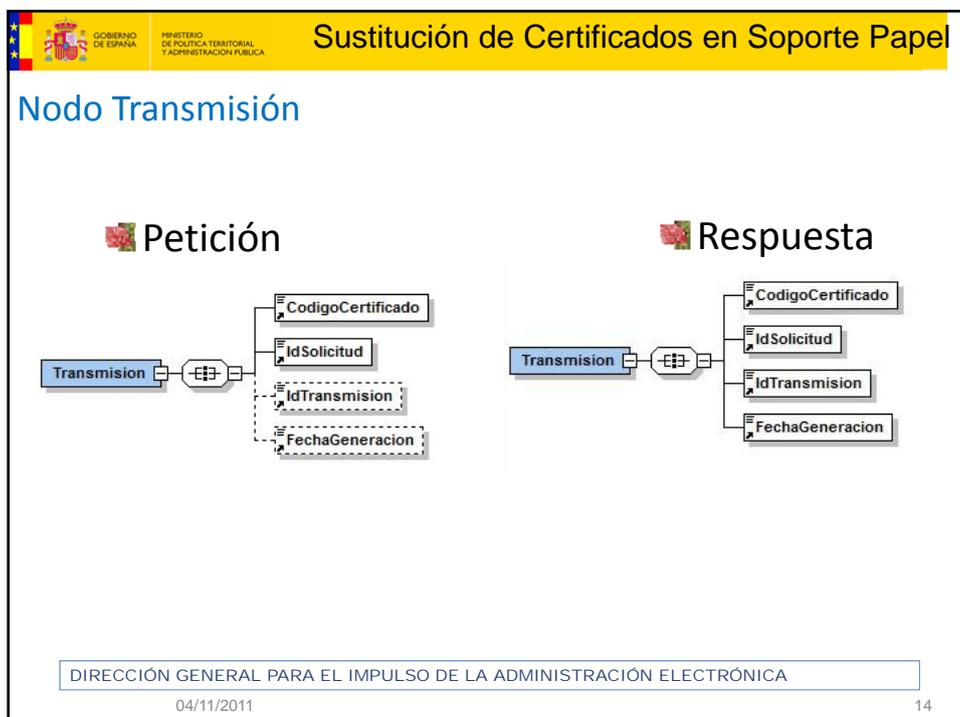
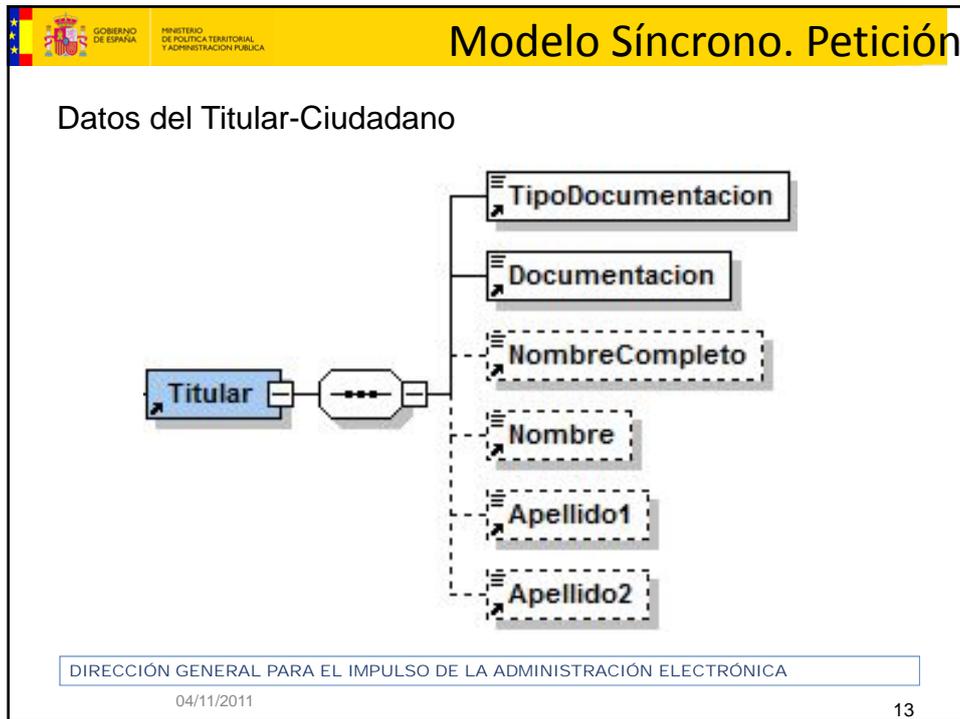
Índice

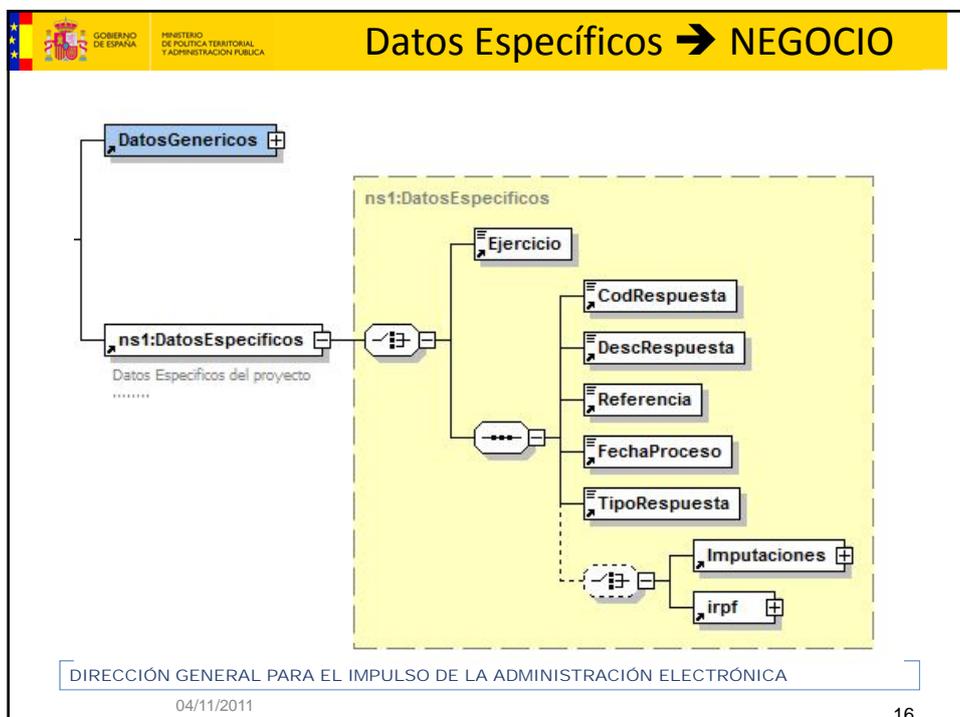
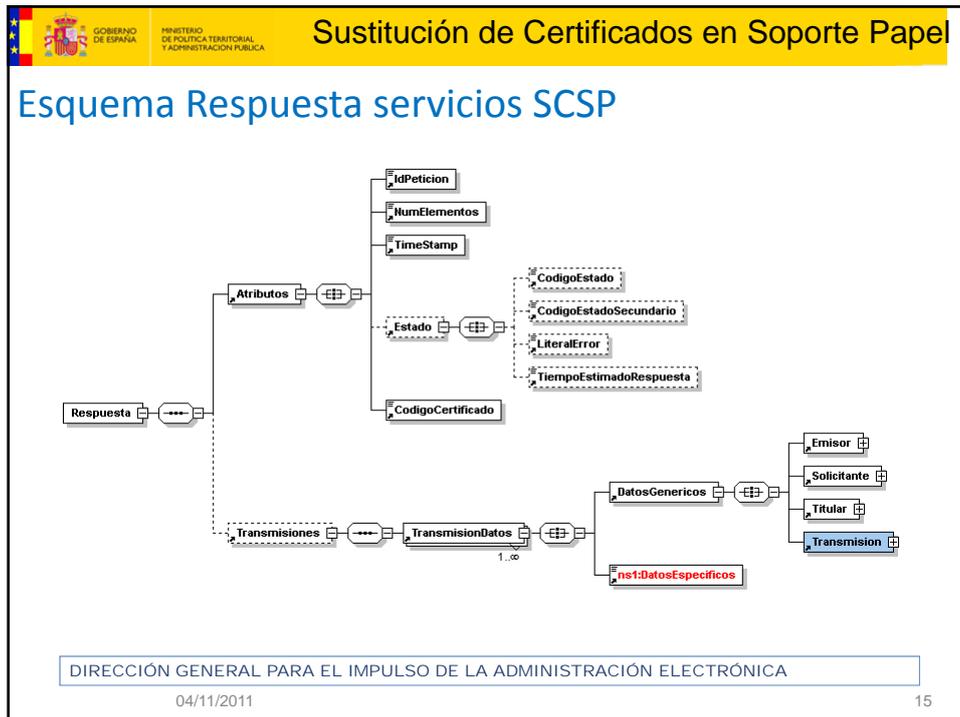
1. Protocolo de Sustitución de certificados en papel
- 2. **Esquemas de intercambio de datos SCSP**
3. Librerías SCSPv3
4. Recubrimiento SCSP_WS

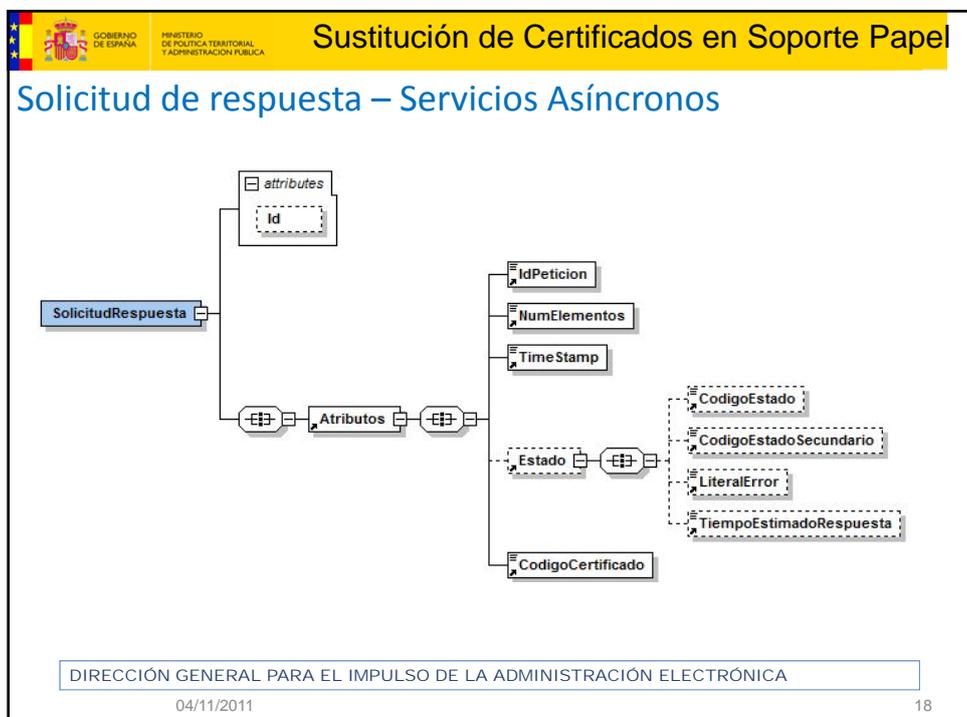
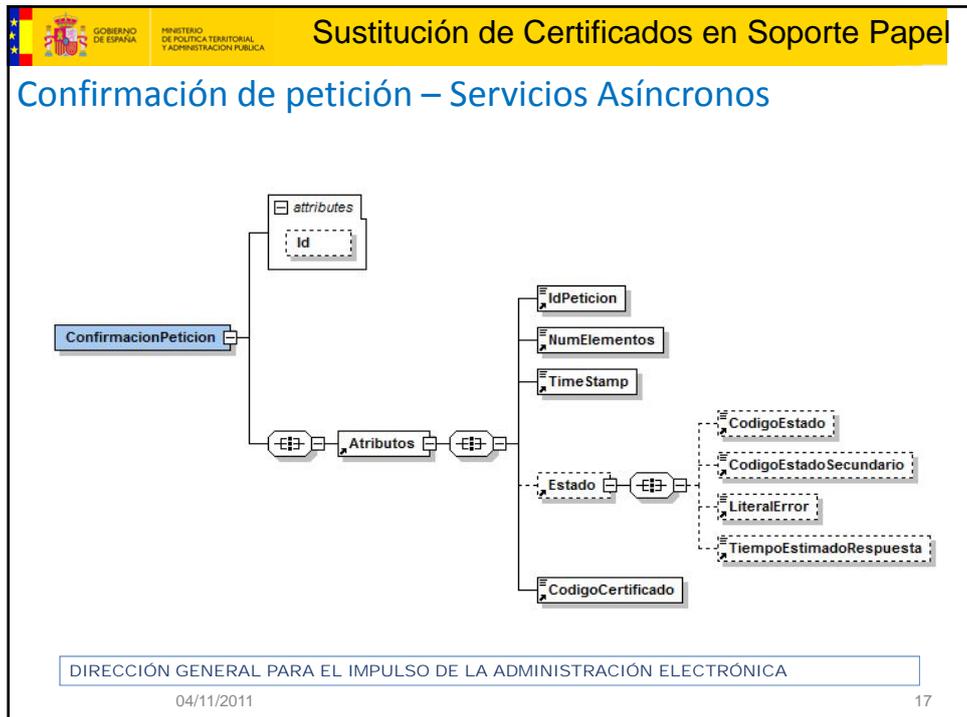
DIRECCIÓN GENERAL PARA EL IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA

04/11/201110









GOBIERNO DE ESPAÑA
MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA

Sustitución de Certificados en Soporte Papel

Índice

1. Protocolo de Sustitución de certificados en papel
2. Esquemas de intercambio de datos SCSP
3. **Librerías SCSPv3**
4. Recubrimiento SCSP_WS



DIRECCIÓN GENERAL PARA EL IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA

04/11/2011 19

GOBIERNO DE ESPAÑA
MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA

Sustitución de Certificados en Soporte Papel

Funciones de las librerías SCSP

- Soporta Requirentes y emisores
- Funcionalidades Comunes:
 - ✚ Composición de mensajes SCSPvX (v2/v3 según el certificado requerido)
 - ✚ Firma de mensajes SCSP (XMLDsig o WS-Security)
 - ✚ Cifrado de mensajes SCSP (si procede)
 - ✚ Almacenamiento histórico de mensajes y transmisiones
 - ✚ Envío de la petición al Endpoint de cada servicio
 - ✚ Recepción de mensajes SCSP y validación de los mismos
 - ☞ Validación de esquemas XSD
 - ☞ Validación de la firma digital y del certificado con el que se firmó
 - ☞ Descifrado de mensajes SCSP si procede (Por ejemplo respuestas AEAT y TGSS)
- Funcionalidad del Emisor
 - ✚ Autorización y Autentificación de Organismos Requirentes/Cesionarios
 - ✚ Comunicación con el BackOffice

DIRECCIÓN GENERAL PARA EL IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA

04/11/2011 20

Sustitución de Certificados en Soporte Papel

Arquitectura de las librerías SCSP

La aplicación cliente del organismo requirente, utiliza el ClienteUnico (clase de acceso a cualquier servicio Web SCSP) para comunicarse con el servicio Web concreto que le permite obtener un determinado tipo de certificado.

Interfaz ClienteUnico

- String idPetición = getIdPetición(codcertificado);
- Respuesta respuesta = realizaPeticiónSincrona(petición);
- ConfirmaciónPetición confirmación = realizaPeticiónAsincrona(petición);
- Respuesta respuesta = realizaSolicitudRespuesta(solicitud, cif);

DIRECCIÓN GENERAL PARA EL IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA

04/11/2011 21

Sustitución de Certificados en Soporte Papel

Funcionamiento en modo síncrono

Peticiones con una única solicitud para un titular.

La respuesta del servicio web será en línea, sobre la misma conexión https establecida entre el requirente y el emisor

DIRECCIÓN GENERAL PARA EL IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA

04/11/2011 22

Sustitución de Certificados en Soporte Papel

Funcionamiento de las librerías en modo síncrono

<ol style="list-style-type: none"> 1. Recibe un objeto Petición de “Aplicación de Peticiones” 2. Obtener datos del certificado 3. Generar id petición (si no se ha indicado) 4. Generar mensaje XML de petición 5. Validar esquema XSD 6. Cifrar el mensaje XML de petición (si procede) 7. Firmar el mensaje XML de petición 8. Registrar el XML de petición en BBDD 9. Enviar XML de petición 	<ol style="list-style-type: none"> 1. Recibir un mensaje XML de petición 2. Validar esquema del mensaje 3. Autorizar organismo y validar certificado de firma 4. Validar firma del mensaje 5. Enviar solicitud al backoffice 6. El backoffice tramita la solicitud y devuelve un objeto respuesta con la respuesta generada 7. Generar XML de respuesta 8. Cifrar la respuesta XML (si procede) 9. Firmar la respuesta XML 10. Registrar en base de datos la respuesta 11. Enviar la respuesta al requirente
---	--

04/11/2011 23

Sustitución de Certificados en Soporte Papel

Funcionamiento de las librerías en modo síncrono

<ol style="list-style-type: none"> 1. Verificar firma del mensaje XML de respuesta 2. Descifrar la respuesta (si procede) 3. Validar esquema XSD de la respuesta 4. Registrar la respuesta recibida en BBDD 5. <i>Procesar las transmisiones de datos recibidas</i> 6. Devolver a la “Aplicación de Peticiones” un objeto Respuesta. 	
---	--

DIRECCIÓN GENERAL PARA EL IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA

04/11/2011 24

Sustitución de Certificados en Soporte Papel

Funcionamiento de las librerías en modo asíncrono

- Peticiones con múltiples solicitudes (1 .. 1000) para múltiples titulares, pero sobre un mismo certificado
- La respuesta no será en línea
- Depende el Organismo Emisor (Según disponibilidad y/o Naturaleza de los datos que podrían no estar disponibles online)
- Facilidad de adaptación a la tramitación de los organismos (Lotes)

DIRECCIÓN GENERAL PARA EL IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA

04/11/201125

Sustitución de Certificados en Soporte Papel

Funcionamiento de las librerías en modo asíncrono

<ol style="list-style-type: none"> 1. Recibir un objeto petición de "Aplicación de Peticiones" 2. Obtener datos del certificado 3. Generar id petición 4. Generar mensaje XML de petición con las <u>múltiples solicitudes</u> 5. Validar esquema XSD del mensaje, cifrarlo (si procede), firmarlo y registrarlo en BBDD 6. Enviar XML de petición 	<ol style="list-style-type: none"> 1. Recibir un mensaje XML de petición 2. Validar esquema del mensaje 3. Autorizar organismo y validar certificado de firma 4. Validar firma del mensaje 5. Enviar solicitud al backoffice y este le devuelve un objeto ConfirmacionPetición 6. Generar el mensaje XML de confirmación de petición, firmarlo y registrarlo en BBDD 7. Enviar confirmación de petición
--	--

DIRECCIÓN GENERAL PARA EL IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA

04/11/201126

Sustitución de Certificados en Soporte Papel

Funcionamiento de las librerías en modo asíncrono

The diagram illustrates the asynchronous process flow. On the left, an 'Aplicación de Peticiones' (Application of Requests) is connected to a 'ClienteUnico' (Single Client) box, which is linked to a 'Librería Requiriente' (Requesting Library). This library connects to the 'Intratet Administrativa' (Administrative Intranet). On the right, the 'Intratet Administrativa' connects to a 'WS Cert' (Certificate Web Service), which is linked to a 'Librería Emisor' (Issuing Library). The 'Librería Emisor' is connected to a 'Backoffice' system.

1. Recibir confirmación de la petición
2. Validar el esquema XSD del mensaje
3. Validar firma del mensaje y almacenar el mensaje en BBDD
4. Actualizar el TER y el Estado de la petición
5. **Devuelve a "Aplicación de Peticiones" un objeto ConfirmacionPeticon**

DIRECCIÓN GENERAL PARA EL IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA

04/11/201127

Sustitución de Certificados en Soporte Papel

Funcionamiento en modo asíncrono

Modulo de polling de las librerías

The diagram shows the internal structure of the 'Librerías SCSP' (SCSP Libraries) polling module. A 'Temporizador' (Timer) is connected to a 'Módulo de Polling' (Polling Module). The 'Módulo de Polling' is connected to a 'Módulo de Tratamiento XML' (XML Processing Module). Below the XML module is a database labeled 'Peticones Respuestas' (Requests Responses). The 'Módulo de Tratamiento XML' is connected to a 'Servicio Web' (Web Service). The 'Módulo de Tratamiento XML' sends an 'XML Solicitud' (XML Request) to the 'Servicio Web' and receives a 'Respuesta' (Response) back.

1. Se activa el temporizador y, este activa el módulo de polling
2. Recuperar peticiones pendientes con TER vencido
3. Enviar solicitud de respuesta

DIRECCIÓN GENERAL PARA EL IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA

04/11/201128

Sustitución de Certificados en Soporte Papel

Funcionamiento en modo asíncrono

<ol style="list-style-type: none"> 1. Consulta el estado de la petición y el TER 2. Si estado PENDIENTE y el TER ha vencido <ol style="list-style-type: none"> 1. generar mensaje XML de solicitudRespuesta 2. Validar esquema XSD del mensaje, cifrarlo (si procede), firmarlo y registrarlo en BBDD 3. Enviar XML de solicitud de respuesta 	<ol style="list-style-type: none"> 1. Recibir un mensaje XML de solicitud de respuesta 2. Validar esquema del mensaje 3. Autorizar organismo y validar certificado de firma 4. Validar firma del mensaje 5. Consultar el estado de la petición y el TER 6. Enviar al backoffice la solicitud de respuesta si estado PENDIENTE y vencido el TER 7. Recuperar fichero de respuesta o Recuperar nuevo TER 8. Generar mensaje XML de respuesta 9. Cifrar respuesta (si procede) 10. Firmar la respuesta 11. Enviar respuesta
--	--

04/11/201129

Sustitución de Certificados en Soporte Papel

Funcionamiento en modo asíncrono

<ol style="list-style-type: none"> 1. Recibir XML de respuesta 2. Verificar firma del mensaje 3. Descifrar respuesta (si procede) 4. Validar esquema XSD del mensaje 5. Almacenar el mensaje de respuesta en BBDD 6. Procesar las transmisiones de datos recibidas 7. Devuelve un objeto Respuesta a "Aplicación de Peticiones" 	
---	--

04/11/201130

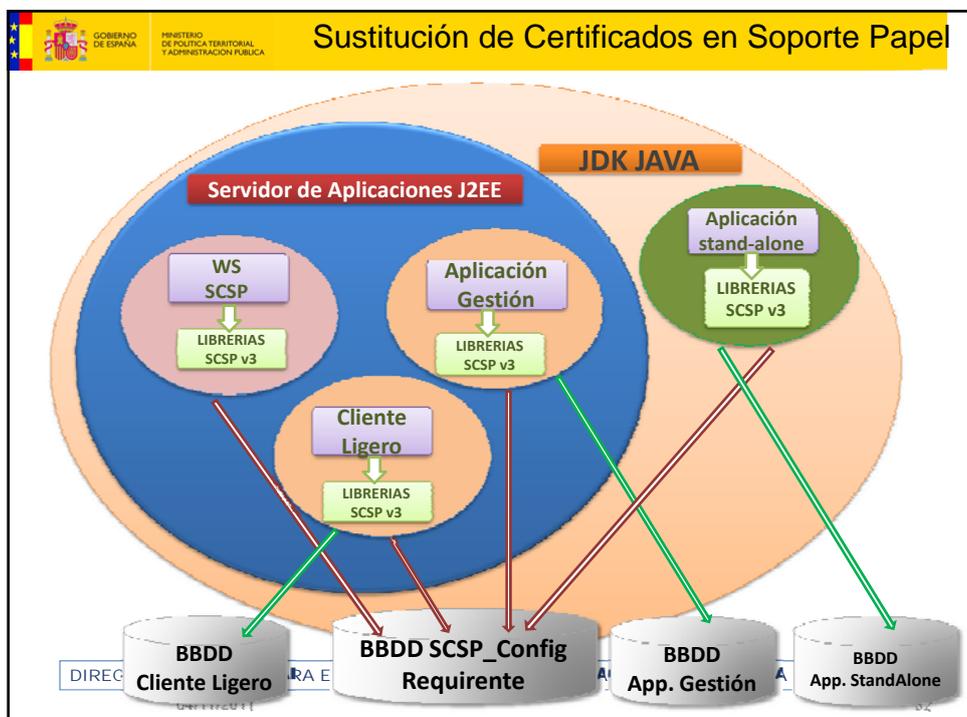
Sustitución de Certificados en Soporte Papel

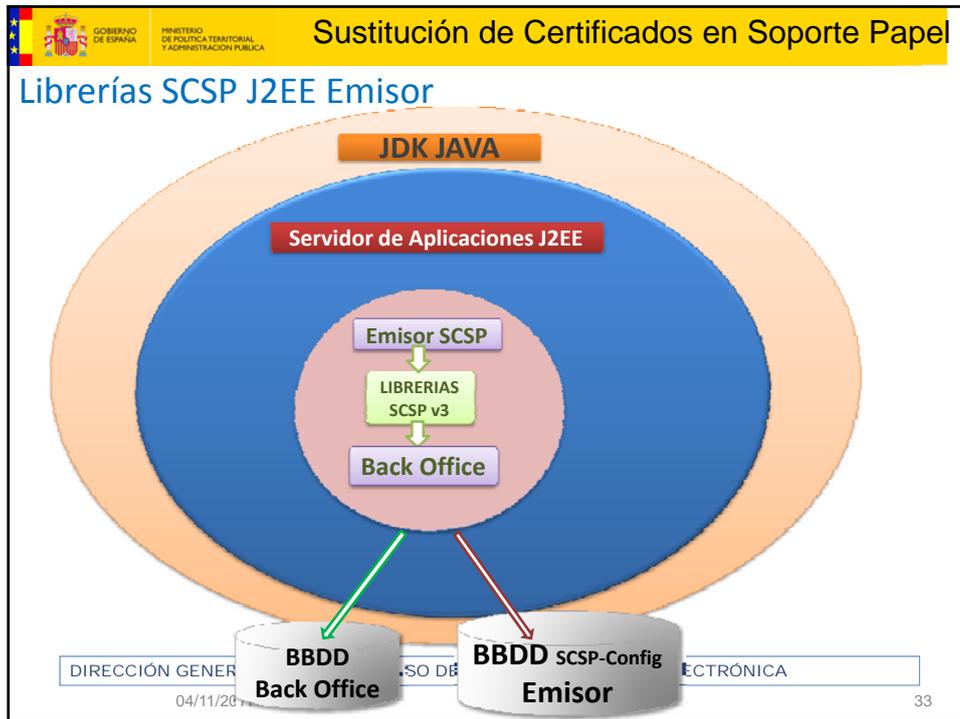
¿Pasos para usar las librerías SCSP J2EE?

- Obtener el asistente gráfico de configuración de las librerías disponible para Windows y Linux
- Ejecutar el asistente, que le guiará paso a paso durante todo el proceso de configuración de las librerías tanto para Requirente como para Emisor.
 - ✚ Servidores de aplicación: Tomcat, Jboss, WebLogic
 - ✚ Servidores de BBDD: MySQL, Oracle, SQL Server, PostgreSQL
- **Requirente**
 - ✚ Tras finalizar el proceso de configuración el wizard permitirá seleccionar que producto SCSP obtener
 - .rar con los jars de las librerías SCSP (recursosSCSP.rar)
 - .war recubrimiento WS SCSP (scsp_ws.war)
 - .war Cliente Ligero SCSP (ClienteLigero.war)
- **Emisor**
 - ✚ .war con los servicios web correspondientes a los servicios web SCSP a publicar

DIRECCIÓN GENERAL PARA EL IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA

04/11/2011 31





Sustitución de Certificados en Soporte Papel

Índice

1. Protocolo de Sustitución de certificados en papel
2. Esquemas de intercambio de datos SCSP
3. Librerías SCSPv3
4. Recubrimiento SCSP_WS

DIRECCIÓN GENERAL PARA EL IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA

04/11/2011

34

Sustitución de Certificados en Soporte Papel

Recubrimiento SCSP_WS

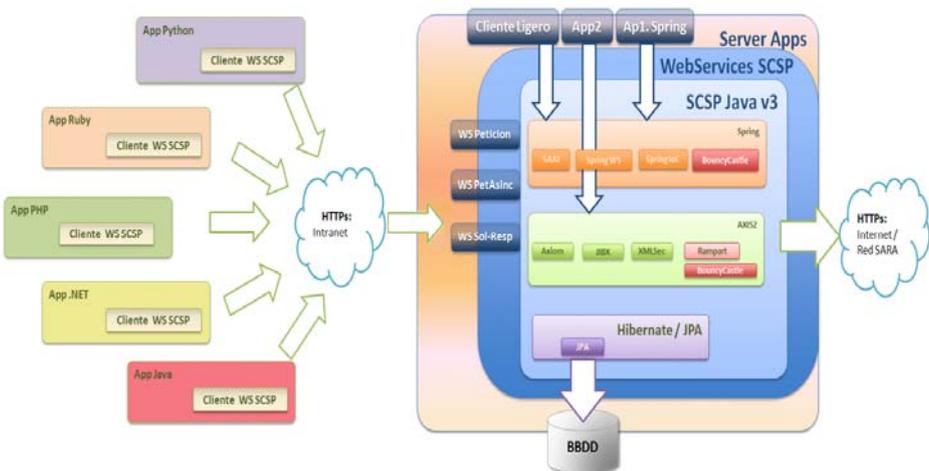
-  Aplicación web que hace uso de las librerías SCSPv3 y ofrece la funcionalidad de estas a través de servicios web.
-  Cualquier tipo de aplicación que funcione como Requirente (cliente) pueda usar las librerías SCSP para consultar datos independientemente de la tecnología subyacente.

DIRECCIÓN GENERAL PARA EL IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA

04/11/201135

Sustitución de Certificados en Soporte Papel

Uso del recubrimiento SCSP_WS por distintas aplicaciones



The diagram illustrates the architecture for using SCSP_WS. On the left, several client applications (App Python, App Ruby, App PHP, App .NET, App Java) are shown, each containing a 'Cliente WS SCSP' component. These clients connect via 'HTTP: Intranet' to a central server stack. The server stack is composed of several layers: 'Server Apps' (Cliente Ligero, AppZ, Ap1.Spring), 'WebServices SCSP' (SCSP Java v3), and a database layer (BBDD). The SCSP Java v3 layer includes components like WS Petición, WS PetAsinc, WS Sol-Resp, and Spring. The database layer includes Hibernate/JPA. The server stack also connects via 'HTTP: Internet/Red SARA' to external services.

DIRECCIÓN GENERAL PARA EL IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA

04/11/201136

Sustitución de Certificados en Soporte Papel

Esquemas de petición recubrimiento WS SCSP

- Simplificación del esquema de petición de los servicios SCSP
- El nodo Atributos sólo contendrá *CodigoCertificado*
- El nodo DatosGenericos no contendrá los nodos Emisor ni Transmision → generados por las librerías.

DIRECCIÓN GENERAL PARA EL IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA

04/11/201137

Sustitución de Certificados en Soporte Papel

Ventajas de usar el recubrimiento SCSP_WS

- Simplificación del funcionamiento de SCSP
 - ✚ Firma/Cifrado
 - ✚ Validación de Esquemas
 - ✚ Registro de Peticiones
- Detecta automáticamente las versiones configuradas de los servicios (versión SCSP, Firma, Cifrado)
- Compatible con cualquier tipo de tecnología
 - PHP
 - PYTHON
 - RUBY
- Fácil y sencillo de usar

DIRECCIÓN GENERAL PARA EL IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA

04/11/201138

Sustitución de Certificados en Soporte Papel

Uso del recubrimiento SCSP_WS por una aplicación

- A modo de prueba, existe un recubrimiento instalado en la siguiente URL con acceso a todos los entornos de Preproducción que simulan los servicios recogidos en el Catalogo de servicios
<https://10.253.114.137/scsp-ws/ws>
- El contenido del WSDL se puede obtener en la URL:
<https://10.253.114.137/scsp-ws/service.wsdl>
- Se ofrecen 3 operaciones tal y como se describe en el WSDL del servicio.
 - + Petición Síncrona → peticiónSincrona
 - + Petición Asíncrona → peticiónAsincrona
 - + Solicitud de respuesta → solicitudRespuesta

DIRECCIÓN GENERAL PARA EL IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA

04/11/2011 39

