16

SUSTITUCIÓN DE CERTIFICADOS EN SOPORTE PAPEL

Francisco Villanueva Díez
Jefe de Área de Desarrollo
Ministerio de Administraciones Públicas. Dirección General de Modernización Administrativa. División de Proyectos Tecnológicos.

1. ANTECEDENTES

Desde la publicación de la Ley 30/1992, los ciudadanos tienen el derecho a no aportar documentación que ya se encuentre en poder de la Administración actuante. Esta legislación no se ha venido aplicando de forma general, bien por falta de exigencia por parte del ciudadano, o por trabas impuestas por la propia administración.

Así por ejemplo, en casi todos los procedimientos de la Administración General del Estado todavía se exige la aportación de certificados de estar al corriente de cumplimiento de obligaciones tributarias y con la Seguridad Social para participar en las licitaciones públicas.

Por otra parte, en el año 2003 entra en vigor el Real Decreto 209 que regula la utilización de medios telemáticos, para la sustitución de la aportación de certificados por los ciudadanos. Este decreto, establece el plazo máximo de un año a partir de su publicación, para que todos los organismos de la AGE, sustituyan sus certificados, bien por transmisiones de datos, bien por certificados telemáticos.

También en el año 2003, el Plan de Choque para el Impulso de la Administración Electrónica, presentado por los Ministerios de Ciencia y Tecnología y Administraciones Públicas, encomienda al MAP en su medida número 11, el desarrollo de los aspectos técnicos referentes a la arquitectura y estándares de intercambio, necesarios para posibilitar el uso generalizado de certificados telemáticos y transmisiones de datos entre departamentos de la Administración.

2. EL PROYECTO DE SUSTITUCIÓN DE CERTIFICADOS EN PAPEL

De acuerdo con esta encomienda, el Ministerio de Administraciones Públicas ha coordinado un grupo de trabajo, en el que participan también la Agencia Estatal de Administración Tributaria, la Tesorería General de la Seguridad Social, y el Ministerio de Agricultura, en el que se han elaborado unas especificaciones técnicas de un sistema informático, que permita, a cualquier organismo de la Administración General del Estado, sustituir certificados en papel con las garantías jurídicas descritas en el RD 209/2003, y facilitar la fácil implantación del sistema definido.

El proyecto se estructura en varias fases,

- **Elaboración de unas especificaciones funcionales y técnicas.** Estas especificaciones deben satisfacer los requisitos de autenticidad, confidencialidad, integridad, disponibilidad y conservación de la información impuestos por el RD 263/1996 para la utilización de técnicas electrónicas, informáticas y telemáticas en la Administración General del Estado, y utilizar algunas de las dos técnicas posibles de sustitución enumeradas por el Real Decreto; el certificado telemático o la transmisión de datos.
- **Construcción de un piloto** operativo entre los miembros del grupo de trabajo, que sirva para demostrar la utilidad y viabilidad del sistema. El piloto debe implementar la funcionalidad mínima descrita en las especificaciones, manteniendo la validez jurídica de los certificados en papel sustituidos por su mediación.
- **Desarrollo de unas librerías de código,** para su distribución entre aquellos organismos de la AGE que quieran utilizar el servicio. Las librerías se construirán en las dos tecnologías de programación mas extendidas en la Administración General del Estado, J2EE y .NET, para facilitar la integración del máximo número de entidades.

- **Comunicación y distribución de resultados.** Uno de los puntos mas importantes para el éxito del servicio, es el conocimiento que del mismo tengan el resto de organismos de la Administración del Estado, para que de forma paulatina se extienda su utilización.
  Esta misma ponencia es un ejemplo del esfuerzo que quiere hacer el MAP, para llegar a todas las unidades interesadas de la AGE.

3. REQUISITOS

A la hora de elaborar las especificaciones, se han estudiado las condiciones que tiene que cumplir un servicio telemático para sustituir con validez jurídica un certificado en papel, y que vienen descritas en el RD 263/1996, (redacción del RD 209/2003).

De acuerdo al artículo 4, hay que "asegurar la autenticidad, confidencialidad, integridad, disponibilidad y conservación de la información". El legislador añade aquí con gran criterio, que "dichas 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 y a los riesgos a los que estén expuestos".

En el artículo 13, se detalla entidades informáticas se puede sustituir un certificado en papel; un **certificado telemático** o una **transmisión de datos.** Los artículos 14 y 15 definen en que consisten cada una de estas dos entidades. A continuación se enumeran las características principales de cada una de ellas, y las posibilidades y dificultades que conlleva su implementación sobre un sistema informático.

El **certificado telemático,** debe ir **firmado** por la autoridad competente para expedirlo.

Además, el contenido, o sea, los datos objeto de certificación, **deberán poder ser impresos en papel,** donde aparecerá también un código de verificación (huella), que permita contrastar su autenticidad accediendo por medios telemáticos a los archivos del organo emisor.

Esta condición es claramente incongruente con el hecho de que estamos hablando de un certificado en formato electrónico, y que ya contiene una firma reconocida que cumple con la ley 59/2003 de firma electrónica, lo que hace completamente innecesario acceder al organismo emisor para verificar los datos.

El certificado telemático se puede expedir **a instancias del interesado** (persona a la que se refieren los datos), **o a instancias del órgano requirente,** (órgano que necesita el certificado para la tramitación de algún procedimiento). En este último caso, los funcionarios de estos órganos deberán estar habilitados para ello, y esta habilitación anotada en el Registro Central de Personal, pudiendo ser consultada por los órganos competentes.

Desde el punto de vista de un sistema que expida automáticamente certificados telemáticos para su transmisión entre organismos, como el que se propone definir en el proyecto, esta definición tiene dos **dificultades** principales:

- **La firma por autoridad competente.** Los certificados en papel que se pretende sustituir en el marco de la Administración General del Estado, van todos firmados por personas físicas, que ostentan la titularidad de la unidad u órgano responsable de su expedición.
  Es difícil persuadir a estas personas a que cedan sus certificados X509 personales (de la FNMT o DNI electrónico en un futuro, por ejemplo), para que las máquinas de los organismos emisores generen de forma automática las certificaciones requeridas.

En otro caso, la firma de la autoridad requeriría varios días de retraso, además de generar una notable carga de trabajo. Hay que tener en cuenta además, que el certificado X509 de la autoridad aporta validez legal a todos los documentos firmados, de acuerdo a la ley 59/2003 de Firma electrónica, lo que impide que el titular del mismo firme de forma mecánica cualquier fichero sin revisarlo con anterioridad.

- **La habilitación de los funcionarios.** El RD establece que los funcionarios que solicitan a otro organismo certificaciones relativas a ciudadanos o empresas, deben estar habilitados para ello, pero no dice quien tiene capacidad para realizar esta habilitación, (el subsecretario, el jefe de la unidad, el titular del organismo).
  Además, esta habilitación debe de poder ser consultada por los órganos emisores, con lo cual hay que articular un sistema de acceso al Registro Central de Personal integrado en el sistema de sustitución de certificados en papel.

La **transmisión de datos** por su parte, **no necesita ir firmada.** Siempre se expide a instancias de un órgano requirente, y de su petición y recepción se ha de dejar constancia en el expediente del procedimiento para el que pidió. (Mediante un oficio por ejemplo).

El no repudio en las transmisiones se comprueba habilitando mecanismos para que **los órganos de fiscalización y control** de la AGE, como interventores y abogados del estado, **puedan acceder a los datos transmitidos** a efectos de verificar el origen y la autenticidad de los datos.

Desde el punto de vista de un sistema informático, una transmisión de datos es una consulta directa, por parte de un organismo tramitador, a los datos que posee el organismo emisor. No tiene materialización, ni duración en el tiempo.

La condición impuesta por el artículo 15.5 del RD 263/1996, "acceder a los datos transmitidos a efectos de verificar el origen y la autenticidad de los datos", obliga por un lado, a **almacenar todas las transmisiones emitidas** por un organismo, y por otro, a **definir un sistema de localización y acceso a posteriori** de esas transmisiones.

Otro de los requisitos que se han considerado en el proyecto, ha sido la **homogeneización de los formatos,** tanto en lo relativo a las peticiones de emisión de certificados como en las respuestas, de forma que dichos formatos,

- No estén condicionados por las infraestructuras o tecnologías de emisor y requirente.
- No tengan dependencias del tipo de información a obtener o trasmitir.
- Sean los suficientemente amplios o presenten extensiones que garanticen que no sea necesaria su modificación ante nuevos tipos de certificados.

Por último, se ha impuesto como condición del sistema, que la especificación obtenida sea fácilmente extensible para la incorporación al mismo de otras administraciones públicas, como las Comunidades Autónomas y las Entidades Locales.

4. RESULTADOS

Teniendo en cuenta estas alternativas, certificado telemático o transmisión de datos, y las distintas características de cada una, el sistema definido ha optado por **utilizar las transmisiones de datos como medio estándar de sustitución de los certificados en papel.** Las condiciones impuestas a las transmisiones se consideran mas asequibles y fáciles de reflejar sobre un sistema informático que las relativas a los certificados telemáticos.

El formato elegido para las solicitudes y las transmisiones es el **XML.** Se ha definido un documento con dos partes; la primera, **Datos Genéricos,** donde se transmite información común a todos los certificados en papel que se sustituyen, como la relativa al organismo solicitante, al organismo emisor, al interesado al que se refieren los datos, y la relativa a la propia transmisión.

En la segunda parte de **Datos Específicos,** cada organismo define los campos que transmite en función del tipo de certificado en papel que se está sustituyendo. Estos datos específicos también deberán estar en formato XML, pero es obligación de cada organismo emisor publicar el esquema XSD que indica la estructura del mismo.

La tecnología empleada para realizar las peticiones y enviar las respuestas con las transmisiones es **Servicios Web.** Este es un estándar soportado por la mayoría de las infraestructuras tecnológicas del mercado, y fácilmente interoperable entre distintas plataformas.

El **protocolo** utilizado para la comunicación es **SOAP sobre HTTP(s),** siguiendo el **modelo de documento XML.**

El acceso a los servicios Web publicados por los organismos emisores es **directo** por parte de los organismos requirentes. Existirá un directorio UDDI, disponible en el MAP, donde cada organismo emisor publicará aquellos servicios Web que vaya haciendo accesibles para transmitir datos que sustituyan certificados en papel. Los organismos requirentes que necesiten dichos datos, consultarán el directorio para conocer la estructura y dirección donde está disponible el servicio. A continuación accederán directamente al organismo certificador para solicitar y recabar la información.

La **infraestructura de comunicaciones** sobre la que se apoya todo el servicio de sustitución de certificados en papel es la **Intranet Administrativa.**

Para asegurar la **autenticidad,** entendida como identificación de los organismos que acceden y la veracidad de la información transmitida, se utilizan certificados X509V3 clase 2, de servidor SSL, emitidos por la Fábrica Nacional de Moneda y Timbre u otras autoridades de certificación reconocidas por la Administración General del Estado.

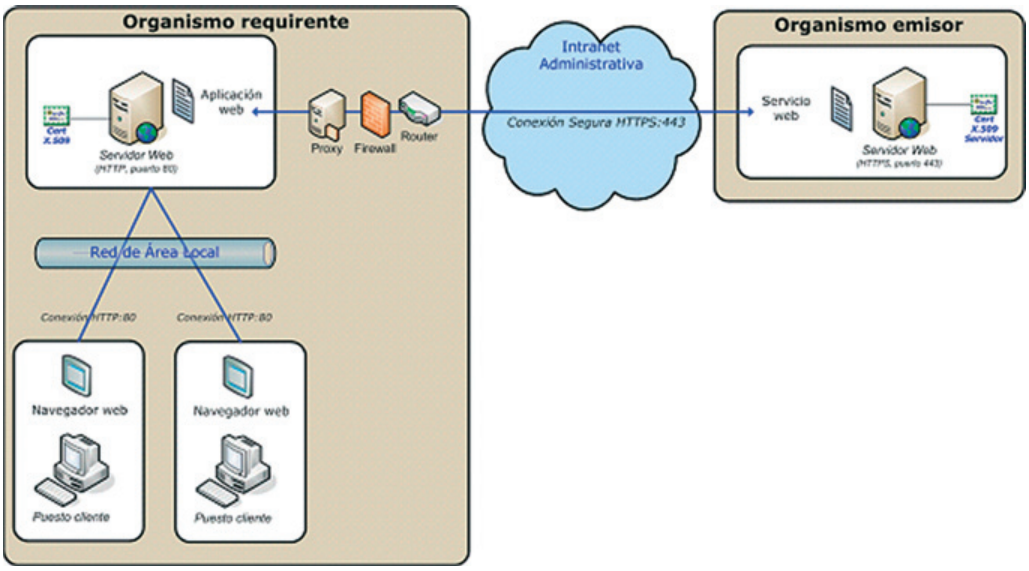

Figura 1. Arquitectura de identificación de servidores

Los organismos solicitantes y emisores que participan en el sistema necesitan tener un servidor Web identificado mediante uno de estos certificados X509V3. A la hora de establecerse la comunicación entre el requirente y el emisor, este último comprueba que el solicitante tiene uno de estos certificados, verifica su identidad como perteneciente a la Administración General del Estado y valida que tiene permiso para acceder a la información solicitada accediendo a una **base de datos de autorizaciones,** distribuida en cada organismo emisor, que asigna, para cada tipo de transmisión de datos publicada, permisos de acceso a los organismos que utilizan el servicio.

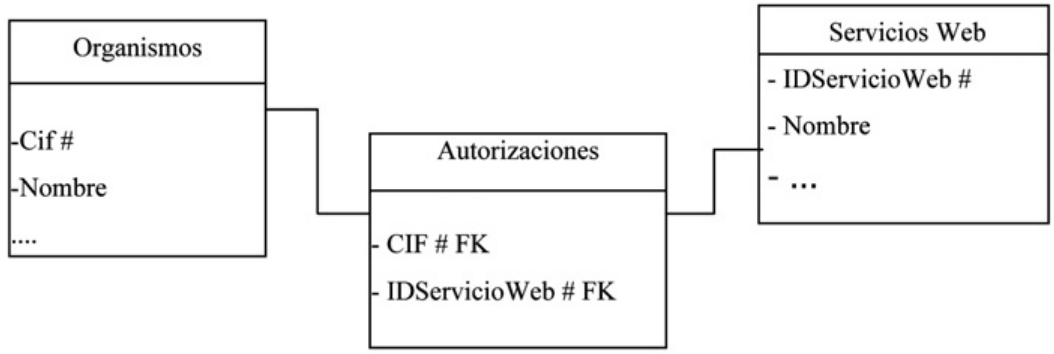

Figura 2. Base de datos de autorizaciones

El control de accesos al sistema de consultas de los organismos requirentes es responsabilidad de cada uno de ellos..

Para asegurar la **confidencialidad,** y también para la transmisión del certificado X509V3 entre ambos organismos se utiliza el protocolo SSL, exigiendo identificación a ambos extremos.

La **integridad** de los datos se garantiza de dos maneras. Por una parte, y de acuerdo al artículo 15.5 del Real Decreto 263, en el organismo emisor se deja constancia de todas las transmisiones emitidas, y existe un mecanismo para acceder a dichas transmisiones a posteriori. Además, aunque la legislación no lo exige para las transmisiones de datos, tanto las peticiones como las respuestas emitidas en el sistema **van firmadas.** Esta firma se utiliza tanto para comprobar la integridad de los datos, como para extraer la información de identificación relativa a los certificados X509V3 de ambos extremos.

La firma se transmite en la cabecera SOAP del mensaje, utilizando la codificación XMLdSig, como se ve en el documento XML de ejemplo.

En cuanto a la **disponibilidad** de los servicios, la responsabilidad de la misma recae sobre cada organismo emisor, y sobre los sistemas de respaldo de la propia Intranet Administrativa.

El catálogo UDDI publicado por el MAP, es el único elemento centralizado del sistema, y estará configurado en alta disponibilidad, existiendo además la posibilidad de distribuir réplicas del mismo en otros puntos de la red, si se detecta que actúa como cuello de botella.

Para la **conservación de la información,** cada organismo emisor deberá almacenar las transmisiones emitidas un mínimo de 6 años. Se propone un sistema y esquema de almacenamiento común a todos los organismos emisores, (incluido en las librerías).

5. ARQUITECTURA

Se han definido dos modelos de explotación del sistema, un modelo **síncrono** y otro **asíncrono.**

En el modelo síncrono, sólo se admiten peticiones de consultas unitarias, esto es, solo se puede recabar información de un único tipo de certificado, relativa a un único titular.

La respuesta del servicio web debe ser en línea, sobre la misma conexión https establecida entre el requeriente y el emisor.

En el modelo asíncrono, se admiten peticiones múltiples y respuestas asíncronas, o modo batch.

Las peticiones múltiples están pensadas para procedimientos tipo campaña, como por ejemplo un periodo abierto para solicitar subvenciones, en que el organismo tramitador se encuentra con que necesita en un breve periodo de tiempo, información relativa a muchos interesados. La petición contendrá por tanto muchas solicitudes, aunque en el sistema se ha determinado que todas ellas deben referirse a un único tipo de certificado.

También se ha establecido, en ambos modelos, que cada tipo de certificado en papel que se pretende sustituir debe dar lugar a un servicio web distinto. Esto es, cada servicio web sustituirá un único tipo de certificado en papel.

En la figura siguiente puede verse el esquema de la arquitectura para el modelo asíncrono. Por mantener la sencillez del modelo, el protocolo de comunicaciones utilizado sigue siendo https, y el sistema para recoger las peticiones realizadas se basa en un sondeo periódico por parte del requirente, a un servicio Web de recogida de respuestas, en función de un parámetro "Tiempo Estimado de Respuesta", que se conoce cuando se realiza la petición original.

Este servicio Web de recogida de respuestas sí es único para cada organismo emisor, y en él se recogen las peticiones relativas a cualquier tipo de certificación en papel sustituida.

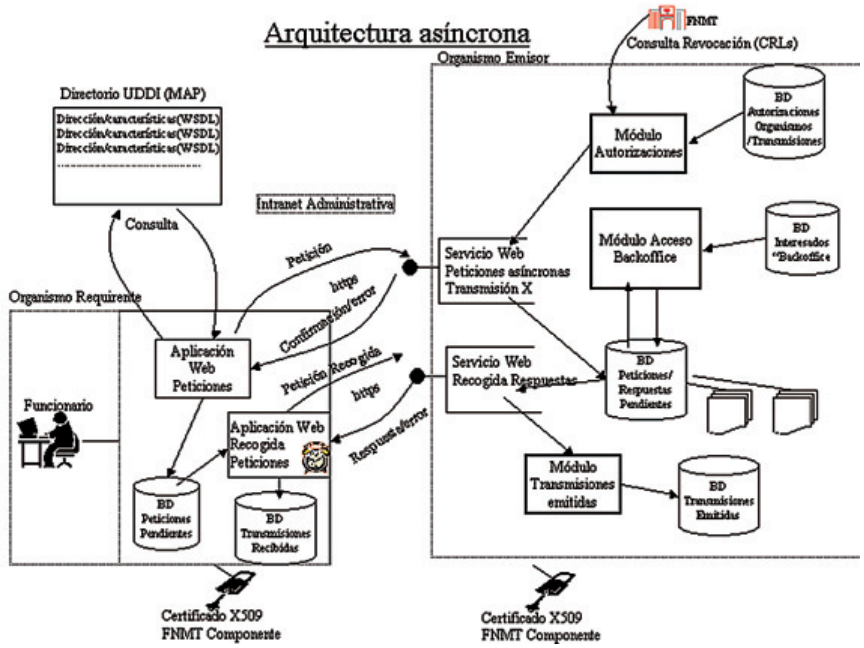

Figura 3. Arquitectura asíncrona

Tanto en el modelo síncrono como en el asíncrono, existe un módulo de acceso al backoffice, que es el encargado de leer la solicitud y recabar los datos del interesado que obran en poder del organismo. Como se ve en el punto dedicado a las librerías, estos módulos son dependientes de cada organismo, y no serán objeto de desarrollo común.

En cuanto al organismo requirente, el proyecto de sustitución de certificados en papel, no entra a definir cual es el sistema del organismo tramitador a través del cual se gestiona el procedimiento. Éste puede haberse iniciado a partir de una instancia presentada en papel en ventanilla, en la cual se autoriza al organismo requirente a recabar los datos necesarios para la tramitación, o bien puede haberse iniciado debido a la recepción de los datos de un formulario situado en el registro telemático del Ministerio. A su vez el trámite puede estarse gestionando en papel o mediante un sistema tramitador automático integrado con flujos de trabajo. Lo que proporciona el servicio de sustitución de certificados son los conectores apropiados para montar las solicitudes, y recoger y visualizar las respuestas.

6. FORMATOS XML

A continuación, se muestra un ejemplo de documento XML para una respuesta que contiene una única transmisión.

```
<?xml version="1.0"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
    <soap:Header>
            <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
            <!-- firma digital -->
            <SignedInfo>
                <CanonicalizationMethod
                Algorithm= "http://www.w3.org/TR/2000/CR-xml-c14n-
                20001026"/>
                    <SignatureMethod
                    Algorithm="http://www.w3.org/2000/09/xmldsig#-sha1"/>
                    <Reference URI="#Body">
                        <DigestMethod
                        Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                        <DigestValue>+DS8235nx6t9WLwqUWZSBGGMhxI=
                        </DigestValue>
                    </Reference>
            </SignedInfo>
            <SignatureValue>gGBeFkCYBNvfr1s8/Jjoyu0wbtUBuDyb0M7h9BMS9DTvNNNou
            jJibE4sRphbQV9LvqXW1 .....
            </SignatureValue>
            <KeyInfo>
                <X509Data>
                    <X509SubjectName>CN=nombreOrganismo</X509SubjectName>
                    <X509Certificate>
                    MIIB8DCCAVkCBDnQPmQwDQYJKoZIhvcNAQEEBQAwPzELMAkG81UEBhMCS
                    lAxDDAKBgNVBAoTTTEMMAoGA1UECxMDVFJMMRQwEgYDVQQDEwtUQU1VUk
                    EgS2VudDAeFw0wMDA5MjYwNjEyNTJaMDEyMjUwNjEyNTJaMD8xCzAJBgN
                    VBAYTAkpQMQwwCgYDVQQKEwNJQk0xDDAKBgNVBAsTA1RS...
                    </X509Certificate>
                </X509Data>
            </KeyInfo>
        </Signature>
        <IdPeticion/>
        <NumElementos/>
        <TimeStamp/>
        <Estado>
            <codigoEstado/>
            <literalError/>
            <TiempoEstimadoRespuesta/>
        </Estado>
    </soap:Header>
    <soap:Body>
        <!-- cuerpo del mensaje -->
        <!-- aqui va la solicitud o la transmision en cuenstion -->
        <TransmisionDatos>
            <DatosGenericos>
                <Emisor>
                    <NifEmisor/>
                    <NombreEmisor/>
                </Emisor>
                <Solicitante>
                    <NifSolicitante/>
                    <NombreSolicitante/>
                    <Finalidad/>
                    <Consentimiento/>
                </Solicitante>
                <Titular>
                    <TipoDocumentacion/>
                    <Documentacion/>
                    <NombreCompleto/>
                    <Nombre/>
                    <Apellido1/>
                    <Apellido2/>
                </Titular>
                <Transmision>
                    <CodigoCertificado/>
                    <IdSolicitud/>
                    <IdTransmision/>
                    <FechaEmision/>

                </Transmision>
            </DatosGenericos>
            <DatosEspecificos>
            <!-- Aqui cada organismo meteria los datos propios de sus
            certificados en formato XML -->
            <!-- Para el caso de la AEAT seria -->
                <Codigo_IDENT>
                <!-- Identificacion del interesado -->
                </Codigo_IDENT>
                <Codigo_Cert>
                <!-- Sentido del certificado -->
                </Codigo_Cert>
                <Codigo_Negativo>
                <!-- Motivo del certificado negativo -->
                </Codigo_Negativo>
                <Datos_Propios>
                </Datos_Propios>
                <Referencia>
                <!-- Identificador interno del certificado -->
                </Referencia>
            </DatosEspecificos>
        </TransmisionDatos>
    </soap:Body>
</soap:Envelope>
```

Existen los correspondientes esquemas XSD para validar estos documentos. Resaltar únicamente que para el campo de "Datos Específicos", la creación y publicación de dicho esquema corresponde a cada organismo emisor.

7. LIBRERÍAS

El MAP ha iniciado la contratación de unas librerías de código, en tecnología J2EE y .NET, que cubran los módulos del requirente y emisor, que son iguales para cualquier organismo que quiera utilizar el servicio.

En el organismo emisor, estos módulos son; módulo de autorizaciones, módulo de transmisiones emitidas, servicio Web de Peticiones, Servicio Web de Recogida de Respuestas, y las bases de datos de transmisiones emitidas y autorizaciones. También habrá un módulo, (que no aparece en la arquitectura), con funciones genéricas de tratamiento de XML, como validaciones, generación de firmas, etc.

En lo relativo a las bases de datos, lo que se distribuirán serán los scripts de creación de las mismas sobre bases de datos relacionales.

Los requisitos impuestos para las librerías, es que puedan funcionar, en el caso del modelo Java, sobre servidores Linux, con Tomcat como servidor de aplicaciones, conectados vía JDBC a servidores relacionales.

En el caso de la arquitectura Microsoft, se pide que funcione sobre Windows 2000, con el servidor Internet Information Server, conectándose vía ODBC a servidores relacionales.

Para los clientes, se desarrollará la aplicación de recogida de peticiones, con su lógica de temporización, la base de datos de peticiones pendientes, los clientes de los servicios Web, (stubs), que realizan la petición y la recogida, y el módulo de tratamiento de XML que valida la información enviada y recibida, firma, etc.

Está previsto que las librerías estén listas para su distribución a mediados de enero de 2005. El MAP tiene previsto contratar un equipo de distribución y mantenimiento de estas librerías, de forma que los organismos que lo soliciten tengan todas las facilidades posibles para adherirse al sistema.

8. CONCLUSIONES

El Ministerio de Administraciones Públicas tiene un gran interés y compromiso por implantar un sistema de sustitución de certificados en soporte papel, que elimine definitivamente los requerimientos a los ciudadanos a aportar documentación que ya obra en poder de la propia Administración.

El MAP quiere extender en un futuro este servicio a otras administraciones públicas, de forma que se convierta en el estándar de transmisión de información relativa a los ciudadanos.

Cualquier órgano de la Administración que quiera incorporarse y empezar a utilizar este servicio una vez puesto en producción, contará con el apoyo del MAP para definir, instalar y configurar sus sistemas de información para acceder y publicar servicios web, con objeto de sustituir certificados en papel por transmisiones de datos.