

## **ANEXO E INFORME TÉCNICO**

### **1 REQUISITOS TECNICOS**

La solución debe cumplir los requisitos técnicos que se desglosan en los siguientes puntos.

Por otro lado, al ser la finalidad del suministro su implantación en los sistemas informáticos municipales, deberá cumplir además los requisitos técnicos incluidos en el ANEXO PLATAFORMA TECNOLÓGICA.

#### **1.1 MÓDULO DE ELEVACIÓN Y VERIFICACIÓN DE FIRMAS**

Actualmente la plataforma de @Firma está completamente integrada dentro de la Plataforma de Firma del Ayuntamiento de Zaragoza (SEIFAZ). Sin embargo, @Firma no facilita el soporte a toda la funcionalidad requerida por el Ayuntamiento de Zaragoza (en concreto en los servicios de elevación y verificación de firmas).

Por este motivo, se plantea una solución híbrida donde se combine @Firma en unos puntos y la plataforma de la Unión Europea, SD-DSS (Digital Signature Service) en aquellos puntos que no resuelve la primera.

La integración con la plataforma @Firma es completa actualmente por lo que dicha labor no es parte del objeto del contrato.

Es objeto del contrato el suministro de un módulo de elevación y verificación de firmas electrónicas basado en la plataforma SD-DSS. Este módulo soportará los siguientes formatos de firma:

- CAdES
- XAdES
- PAdES

Además permitirá trabajar tanto con firmas sencillas como con firmas múltiples (secuencial y/o paralela) y algoritmos de firma SHA-256 y SHA-512..

El proceso de elevación permitirá, al menos, elevar firmas desde niveles -BES y -EPES a nivel -A (en su defecto -LTA).

El proceso de validación deberá necesariamente utilizar los servicios de validación de certificados y obtención de sellos de tiempo proporcionados por el Ayuntamiento de Zaragoza (integrado con los servicios de @Firma).

En el ANEXO INTERFAZ DE LOS SERVICIOS DE ELEVACIÓN Y VERIFICACIÓN DE FIRMAS se describe el interfaz que deben tener este módulo.

Este módulo podrá ser utilizado en forma de librería o como servicios web de tipo REST en formato JSON securizados mediante SSL (sólo de servidor) y autenticación de usuario/contraseña (WSS4J).

## **1.2 INTEGRACIÓN DEL COMPONENTE CLIENTE DE @FIRMA AUTOFIRMA (@FIRMAFACIL)**

Teniendo en cuenta las cada vez mayores limitaciones que se imponen a los componentes Java se hace necesario disponer de formas alternativas para poder realizar la firma de documentos.

Por este motivo, en el Ayuntamiento de Zaragoza será necesario el despliegue del componente cliente de @Firma AutoFirma (antes conocido como “@FirmaFacil”) que permite realizar una firma electrónica sin necesidad de tener disponible Java en el navegador. Este elemento en el ordenador del cliente debe colaborar con uno o varios elementos en la parte servidora.

Es objeto de este contrato el suministro de la integración de estos elementos para su posterior uso dentro de la Plataforma de Firma del Ayuntamiento.

## **1.3 INTEGRACIÓN DEL COMPONENTE CLIENTE DE @FIRMA EN MÓVIL**

La tendencia en informática supone la necesidad de tener acceso a las diferentes soluciones en movilidad. La firma no es un elemento exento de esta problemática.

Por este motivo, en el Ayuntamiento de Zaragoza será necesario el despliegue del componente cliente de @Firma conocido como “Cliente@Firma Móvil” que permite realizar una firma electrónica en dispositivos móviles (Android 4.0 y posterior, iOS 6 y posterior, Windows RT y 8 con interfaz Metro). Este elemento en el ordenador del cliente debe colaborar con uno o varios elementos en la parte servidora.

Es objeto de este contrato el suministro de la integración de estos elementos para su posterior uso dentro de la Plataforma de Firma del Ayuntamiento.

## **1.4 ENTREGABLE**

El módulo a suministrar será entregado incluyendo a su vez el código fuente implementado, de forma que garantice un posible mantenimiento futuro con completa independencia del proveedor que suministre el objeto del presente contrato.

Será asimismo aportada como parte del entregable toda la documentación necesaria para su utilización, instalación en los sistemas municipales y mantenimiento futuro, con especial atención a actualizaciones por parte del Ministerio de Hacienda y Administraciones Públicas y de la Comisión Europea de las plataformas @firma y SD-DSS (Digital Signature Service) respectivamente.

## **1.5 GARANTIA**

La garantía mínima a acompañar al suministro objeto del presente contrato será de 1 año a contar a partir del momento de la entrega del mismo.

## **2 REQUISITOS DE SOLVENCIA**

La empresa licitadora deberá tener experiencia en la utilización tanto de la plataforma SD-DSS (Digital Signature Service) como de la plataforma @firma en proyectos de la Administración Pública y demostrarlo mediante un certificado emitido por la Administración Pública correspondiente.

## **3 PRESENTACION Y VALORACION DE LAS OFERTAS**

### **3.1 Contenido de las ofertas:**

Las ofertas incluirán y deberán seguir la siguiente estructura:

- Certificado de solvencia de la empresa
- Memoria técnica de la solución propuesta
- Mejoras propuestas

Deberá incluir la siguiente tabla:

|      |                                     |
|------|-------------------------------------|
| RQO1 | Precio sin IVA                      |
| RQO2 | Ampliación del tiempo de garantía   |
| RQO3 | Período de mantenimiento adaptativo |

|      |               |
|------|---------------|
| RQO4 | Otras mejoras |
|------|---------------|

### 3.2 Criterios de Valoración

Es imprescindible que la empresa cumpla con los requisitos de solvencia exigidos.

Se valorará, sobre un total de 100 puntos:

RQO1. Con 55 puntos el precio (sin IVA) de las ofertas, aplicando la fórmula

$$\text{Valor} = 55 \times (\text{oferta\_mínima} / \text{oferta\_estudio})$$

RQO2. con un 15 puntos, ampliación del período de garantía contabilizado en meses incluido en el precio de la oferta

$$\text{Valor} = 15 \times (\text{ampliación\_oferta\_estudio} / \text{ampliación\_oferta\_máxima\_garantía})$$

RQO3. Con 15 puntos, inclusión de un período de mantenimiento adaptativo frente a nuevas versiones de @firma y DSS cuantificado en meses incluido en el precio de la oferta

$$\text{Valor} = 15 \times (\text{período\_adaptativo\_oferta\_estudio} / \text{período\_oferta\_máximo\_período\_adaptativo})$$

RQO4. Con 15 puntos máximo, inclusión en el precio de la oferta de mejoras que serán valoradas de la siguiente manera:

Importancia alta: 5 puntos

Importancia media: 3 puntos

Importancia baja: 1 punto

Sin utilidad para el Ayuntamiento de Zaragoza: 0 puntos

## *ANEXO PLATAFORMA TECNOLÓGICA*

# **1 ENTORNO TECNOLÓGICO CORPORATIVO**

## **1.1 ENTORNO DE APLICACIÓN**

La infraestructura tecnológica actual de las aplicaciones

|                               |                                         |
|-------------------------------|-----------------------------------------|
| Front-end HTTP                | Oracle AS 11g Webcache                  |
| Servidor HTTP                 | Oracle AS 11g HTTP Server Apache 2      |
| Servidor de aplicaciones J2EE | Weblogic 10.3.6                         |
| Máquina virtual               | JRockit R28 compatible con JDK 1.6.0_45 |

Si es necesaria la utilización de librerías añadidas se podrán configurar librerías compartidas dentro de las instancias de servidor de aplicaciones

El entorno tecnológico en el que se basan los desarrollos en el Ayuntamiento está compuesto por EJB 3.0 y JDBC 2.0 para el acceso a bases de datos y Java Server Faces para la capa de presentación. Se valorará que la plataforma presentada disponga una tecnología similar a esta. En cualquier caso, los nuevos desarrollos que sea preciso incluir en este proyecto se realizarán con esta tecnología.

La parametrización de las aplicaciones se realizará mediante ficheros de propiedades, por ejemplo las rutas de acceso a los logs o url de servicios Web utilizados.

## **1.2 ENTORNO DE BASE DE DATOS**

El entorno de base de datos corporativo se basa en el SGBD Oracle

|                             |                                        |
|-----------------------------|----------------------------------------|
| Base de datos de producción | Oracle Real Application Cluster 11g R2 |
| Base de datos de desarrollo | Oracle Database Server 11g R2          |

La base de datos está en proceso de migración a Oracle 12c

El acceso a recursos de base de datos debe utilizar data-sources del servidor de aplicaciones.

Puede utilizar JDBC 10.1.0.2, 10.2.0.4 o superior.

Se deberá intentar, en la medida de lo posible la utilización de estándares SQL para el tratamiento de los datos, sin utilizar paquetes específicos añadidos.

Otros recursos a utilizar como capas de persistencia, etc, deberán ser consensuados con los técnicos municipales.

Los esquemas y usuarios de BBDD deberán utilizarse sólo para almacenamiento de información y procedimientos. En la medida de lo posible se utilizará un esquema de BBDD para gestionar los

objetos de la aplicación. No se utilizarán los usuarios de BBDD como mecanismo de gestión de usuarios finales.

Deberá realizarse una estimación del espacio necesario en la BBDD así como el crecimiento anual.

### **1.3 ENTORNO DE FICHEROS**

- Las aplicaciones podrán utilizar recursos del sistema de ficheros.
- Las rutas utilizadas deberán estar convenientemente parametrizadas.
- Se deberá especificar la naturaleza y dimensionamiento de los ficheros alojados, así como el crecimiento anual previsto.

### **1.4 ENTORNO DOCUMENTAL**

El Ayuntamiento dispone del sistema de Gestión documental Alfresco Enterprise 4.1.2 o superior. En caso de ser necesario se podría establecer un espacio para alojar documentos de la aplicación.

El acceso a los recursos de Alfresco deberá realizarse según los métodos proporcionados por el equipo de Desarrollo del ayuntamiento.

Si los documentos deben estar contemplados en el ciclo de vida de los documentos corporativos deberá aplicarse el esquema de metadatos del Ayuntamiento.

Deberá realizarse una estimación del volumen y número de documentos a almacenar así como el crecimiento anual.

### **1.5 OTROS REQUISITOS DE SOFTWARE**

Para la publicación de servicios en el portal corporativo los desarrollos deben ser integrados con el Gestor de Peticiones del Cliente.

Si son necesarias licencias adicionales a la propia plataforma, se especificará con detalle, aportando su cuantía en euros y su inclusión o no en la oferta.

#### ***RECURSOS DE RED***

El acceso a recursos de red : servicios RMI, otros servidores, deberá realizarse mediante nombres DNS proporcionados por los técnicos municipales, evitando el uso de direcciones IP.

#### ***PARAMETRIZACIÓN***

De manera general deberá evitarse la utilización de referencias explícitas a nivel de código utilizando parametrización a nivel de ficheros de propiedades.

La parametrización de las aplicaciones se realizará mediante ficheros de propiedades, por ejemplo las rutas de acceso a los logs o url de servicios Web utilizados. A estos ficheros de propiedades se accederá mediante rutas de classpath (como recurso del

ClassLoader) evitando así una dependencia en el propio código de rutas absolutas del propio servidor.

## **GESTIÓN DE ERRORES**

### **Mensajes de error al usuario**

La aplicación deberá controlar adecuadamente los errores producidos y mostrar mensajes claros al usuario, distinguiendo claramente los errores lógicos o de funcionalidad de los errores de plataforma. Para facilitar la gestión de incidencias.

### **Registro de LOG**

Los logs de la aplicación deberán almacenarse en un fichero adecuadamente identificado, evitando al máximo posible el standard output

Deberán estar claramente identificados los tipos de errores. Deberán ser suficientemente claros y escuetos.

Los logs almacenados deberán respetar en todo momento la normativa de protección de Datos de Caracter personal.

La plataforma de log podrá ser log4java.

## **1.6 ENTORNO CLIENTE**

La aplicación deberá ser compatible con el puesto de trabajo corporativo, la tipología del puesto de trabajo del Ayuntamiento de Zaragoza es:

| Sistema operativo  | Navegador             | Maquina Virtual JAVA (cliente) |
|--------------------|-----------------------|--------------------------------|
| Windows XP Sp3     | Mozilla Firefox 32.03 | 1.7.0_40                       |
| Ubuntu 12_04.2 LTS | Mozilla Firefox 32.03 | 1.7.0_40                       |

## **1.7 REQUISITOS DE SEGURIDAD Y LOPD**

Si el módulo desarrollado realiza un tratamiento de datos personales, deberá tener en cuenta la normativa pertinente en el tratamiento de los datos.

Deberá implementar las medidas correspondientes (control de accesos, trazabilidad de los accesos, control de cambios, etc.) al tratamiento de los datos según la categorización de los mismos.

## 2 REQUERIMIENTOS INFORMACIÓN TÉCNICA

**El equipo de desarrollo deberá suministrar la documentación técnica suficiente para describir la infraestructura técnica asociada al proyecto.**

A la hora de describir la infraestructura de la aplicación, se deben definir los requisitos desde el nivel de base de datos a los del cliente final que realice las consultas.

- esquema general del sistema : módulos principales
- comunicaciones : protocolos de comunicación (http, https, etc)
- entorno de servidor de aplicaciones
  - dimensionamiento de la aplicación (requisitos de memoria, o espacio en disco si conviene)
  - datasources necesarios, espacio en disco si conviene
- entorno de base de datos : estructura de esquemas y dimensionamiento
- entorno de ficheros: requisitos de alojamiento en el sistema de ficheros de los servidores, dimensionamiento y necesidades de publicación
- entorno documental (si necesario): estructura y dimensionamiento
- requerimientos de seguridad de la aplicación
- requerimientos de otros módulos (servicios Web)
- necesidades de integración con :
  - plataforma SSO, plataforma de firma
  - gestión de usuarios corporativa

Es importante enviar información de dimensionamiento de la aplicación:  
número de usuarios concurrentes

- espacio necesario en BBDD y número de objetos
- espacio necesario en filesystem y número de ficheros
- espacio necesario en Alfresco y número de ficheros

Se deberá proveer de un manual de instalación y configuración de la aplicación.

Se deberán especificar los mecanismos de soporte y resolución de incidencias de la aplicación.

Se consensuará con los técnicos corporativas la definición y utilización de los recursos de los BBDD , ficheros y documentales.

## ANEXO INTERFAZ DE LOS SERVICIOS DE ELEVACIÓN Y VERIFICACIÓN DE FIRMAS

El servicio de elevación de firmas debe tener el siguiente interfaz:

```
static public ResultadoVerificacionDocumento elevacionFirma  
    (ParametrosVerificacion params);
```

Y el servicio de elevación de verificación debe tener el siguiente interfaz:

```
static public ResultadoVerificacionDocumento verificacionFirma  
    (ParametrosVerificacion params);
```

Para la validación de los certificados se utilizará el siguiente servicio ya existente en el Ayuntamiento:

```
static public ResultadoValidacionEInfoCert validacionCertificado  
    (ParametrosValidarCertificado params);
```

A continuación se detallan los objetos parámetro y resultado.



