

MEMORIA DESCRIPTIVA

1. DESCRIPCION ENTORNO ACTUAL

El Ayuntamiento cuenta con una aplicación de Registro Electrónico que permite la entrega telemática de entradas por parte de cualquier persona física o jurídica que así lo requiera y también presentación presencial con captura y digitalización de entradas por parte del personal municipal.

Esta funcionalidad está desarrollada en entorno J2EE y es ejecutada sobre una máquina virtual Java versión 1.6.0._45 y servidores J2EE Weblogic versión 10.3.6. La funcionalidad requerida deberá ser compatible en la parte servidor con estas características tecnológicas.

Por otro lado se cuenta con los servicios de firma corporativa incluyendo elevación de firma digital, servicios de sellado de tiempo y validación de certificados. La funcionalidad requerida en el presente contrato se integrará con estos servicios en aquellos casos en que se necesite.

2. DESCRIPCION DE SERVICIOS REQUERIDOS

Se promueve mediante este contrato la prestación de servicios para desarrollar la funcionalidad que permita la entrega telemática de entradas cifradas criptológicamente y por otro lado la captura digital de firma manuscrita de ciudadano.

2.1 Funcionalidad de cifrado de entradas administrativas

El objetivo principal de esta funcionalidad es posibilitar presentación de entradas **cifradas criptológicamente** por vía telemática y su descifrado posterior cuando sea requerido por el personal municipal autorizado para tal efecto. Esta funcionalidad será genérica y utilizable en cualquier procedimiento administrativo dentro de la herramienta municipal de gestión de expedientes.

Las tareas criptográficas se realizarán con una infraestructura de clave pública basada en cifrado y descifrado con claves asimétricas. Para ello el presentador de una entrada cifrará con clave pública el documento a presentar que será posteriormente firmado electrónicamente en presentación. El descifrado se realizará con la correspondiente clave privada. Solo hay una correspondencia entre clave pública y privada .

Para prestar la funcionalidad de cifrado/descifrado que es la objeto de este contrato, las claves se generarán con algoritmos criptográficos seguros que aseguren un alto grado de aleatoriedad. El par de claves privada/pública será único. La funcionalidad será capaz de autogenerar pares de claves X509 y también de gestionar pares proporcionados por un

tercero.

Se incluirán los siguientes servicios en la funcionalidad requerida:

- Generación y almacenamiento de pares de claves pública/privada.
- Inicialización con parámetros configurables por parte del servidor en forma de librería Java.
- Librería con función de cifrado en navegador a partir de los parámetros configurados.
- Funciones de descifrado en forma de librería Java para uso por parte del servidor.
- Auditorías de las acciones solicitadas tanto en cifrado como en descifrado para garantizar la trazabilidad de todas las operaciones.

Para el cifrado se utilizará una tecnología alternativa a Java applets y que esté disponible en la mayoría de los navegadores utilizados en el mercados y en una amplia variedad de sus versiones. Esta operativa se realizará de la manera más transparente posible de cara al usuario de la aplicación.

Se incluirá con la entrega de la funcionalidad la documentación técnica explicativa necesaria para posteriores trabajos por parte del Ayuntamiento de Zaragoza así como el código fuente de los trabajos desarrollados siguiendo los formatos e indicaciones técnicas marcados por el Ayuntamiento a tal efecto.

2.2 Funcionalidad de Firma Digital Manuscrita

Para mejorar la eficiencia del Registro Administrativo del Ayuntamiento de Zaragoza se promueve la contratación de funcionalidad orientada a la captura de firma manuscrita de ciudadano en formato digital y almacenamiento de la misma junto a sus evidencias biométricas. La solución planteada debe adoptar criterios de escalabilidad y ser extensible a cualquier punto de atención ciudadana susceptible de recoger firma de ciudadano.

Los servicios requeridos deberán tener la capacidad de ser prestados en numerosos puntos de atención ciudadana del Ayuntamiento de Zaragoza (entre 30 y 50) si bien el piloto inicial se plantea como atención en 2 puntos.

Actualmente se requiere la presencia del ciudadano y la existencia de un documento papel a firmar que posteriormente se digitaliza. Se desea posibilitar la firma del ciudadano sobre un un dispositivo digital (tipo tableta) para simplificar la tramitación al ciudadano y disminuir en la medida de lo posible el uso del papel.

El proceso de entrada en registro con firma manuscrita se realizará de la siguiente manera:

- 1) El funcionario de la oficina de atención en materia de registro, verificará la identidad del ciudadano solicitando que presente el documento acreditativo según la legislación vigente.
- 2) A continuación registrará la solicitud, incluyendo todos los documentos anexados.
- 3) La solicitud se presentará al usuario en formato digital para su firma en un dispositivo digital. El ciudadano validará sus datos de identidad, la relación de documentos incluidos y la fecha. Realizará el grafo de firma sobre la tableta.
- 4) El funcionario validará la solicitud mediante la realización de una firma electrónica

sobre el documento.

Es por ello que la funcionalidad a suministrar deberá incluir:

Funcionalidad servidor de firma manuscrita a ejecutar en servidor J2EE

Este servidor aceptará peticiones de “inclusión” de firma manuscrita recibiendo para ello un documento solicitud en formato PDF/A y unas coordenadas de posicionamiento para la inserción de la imagen de la firma manuscrita. Se tendrá la posibilidad de requerir varias firmas para la misma solicitud.

Las solicitudes deberán ser autenticadas.

Como resultado se obtendrá un documento en formato PDF/A que incluya tanto la solicitud como la imagen de firma para su posterior firmado electrónico por parte del funcionario público. Además se almacenarán en el servidor de firma manuscrita todas las evidencias biométricas firmadas electrónicamente así como trazabilidad de las peticiones cursadas.

La comunicación de esos resultados al servidor solicitante se podrá realizar de forma síncrona o asíncrona, a elección.

Como servicios añadidos al proceso de firma se posibilitará la gestión y recuperación de firmas previamente realizadas y almacenadas en el servidor de firmas.

Se mantendrán todas las auditorías que garanticen la trazabilidad completa de las acciones realizadas con el servidor de firma manuscrita.

Se incluirá una interfaz (preferiblemente REST) para la invocación de sus servicios desde el resto de elementos actuantes en el proceso de firma.

Funcionalidad encapsulada en aplicación para gestión de la firma en tabletas

Los dispositivos digitales de firma serán dispositivos dedicados y específicos (no genéricos) y la funcionalidad a ejecutar se realizará en el equipo del funcionario con conectividad directa al dispositivo mediante USB. La alimentación de la tableta dedicada se realizará preferentemente a través de este interfaz.

La funcionalidad a implementar en el equipo cliente deberá ser ejecutada sobre una máquina virtual Java versión 1.7.40. Esta funcionalidad así como los controladores de los dispositivos de firma dedicada deberán poder ser ejecutados tanto en Windows XP SP3 como en sistemas Linux Ubuntu 12.04 y Ubuntu 14.04.

Esta aplicación se puede considerar la unión entre el servidor de firma manuscrita y el dispositivo de firma dedicado. Deberá incluir toda la funcionalidad requerida de interconexión entre el dispositivo de firma dedicado y el servidor de firma manuscrita J2EE. Esta funcionalidad será la mínima posible para evitar distribuciones innecesarias

Dentro del presente contrato se suministrarán dos dispositivos digitales específicos para firma, con los que se demostrará el funcionamiento del desarrollo solicitado.

Se incluirá una interfaz para la invocación de sus servicios desde el resto de elementos actuantes en el proceso de firma.

En ambos elementos solicitados la interfaz será lo más sencilla (número de servicios mínimo a invocar para el proceso de firma manuscrita) y ligera posible para su interconexión con la aplicación actual de Registro Municipal Electrónico.

Se incluirá con la entrega de la funcionalidad la documentación técnica explicativa necesaria para posteriores trabajos e instalaciones en los dispositivos digitales específicos para firma por parte del Ayuntamiento de Zaragoza así como el código fuente de todos los trabajos desarrollados, siguiendo los formatos e indicaciones técnicas marcados por el Ayuntamiento a tal efecto.

3 CONDICIONES DE TRABAJO

3.1 Realización de los trabajos

Se requerirá la realización en dependencias municipales de los trabajos de entrega, formación y transferencia tecnológica a los empleados municipales. En estos trabajos se incluirá el apoyo a la integración en las aplicaciones municipales, tanto en entornos de pruebas como productivos.

3.2 Duración

Los trabajos se iniciarán de forma inmediata tras la adjudicación del contrato, siendo su duración máxima de 6 semanas desde el inicio de los mismos.

3.3 Garantía

La empresa garantizará la funcionalidad contratada durante al menos 1 año tras su validación por parte del Ayuntamiento de Zaragoza.