Pliego de Prescripciones Técnicas.

SERVICIOS DE CERTIFICACIÓN ELECTRONICA PARA EL SERVICIO MURCIANO DE SALUD

Ref. SGTI 0072/2015

Creación: Octubre 2015

Autor(es): Subdirección General de Tecnologías de la Información

ÍNDICE

1. OBJETO Y ALCANCE

Constituye el objeto del contrato la prestación de servicios de generación, distribución y soporte de certificados digitales para la persona que tenga condición de empleados públicos del Servicio Murciano de Salud (SMS).

2. DESCRIPCION DE LOS SERVICIOS

2.1 Alcance.

El adjudicatario, al menos, deberá expedir:

- Una cantidad ilimitada de certificados de empleado público, para todos los empleados públicos del SMS.
- Un mínimo de 12 certificados de Ámbito tributario.
- Certificados sede electrónica **1**
- Certificados de sello electrónico **4**
- Certificados de servidor seguro **60**
- Certificado firma de código **5**.

El Adjudicatario deberá instalar, formar, dar soporte funcional y facilitar la operativa al menos 15 Puntos de acreditación en 14 Puntos de Registro Único en los Órganos Centrales, Gerencias, Hospitales y puntos asistenciales que determine el SMS.

Como servicios asociados para el uso de los certificados por parte de sus titulares, el adjudicatario ofrecerá los siguientes servicios técnicos:

- Registro de usuarios.
- Emisión, revocación, archivo de certificados y de clave pública.
- Publicación de certificados y del Registro de certificados.
- Registro de eventos significativos.

El tiempo máximo en la emisión de un certificado electrónico de "Empleado Público" será de un máximo de 10 minutos desde el momento de la acreditación de la identidad y demás circunstancias asociadas que deban formar parte del citado certificado.

Los certificados de componentes deberán ser emitidos y puestos a disposición del solicitante en un plazo máximo de 24 horas tras su solicitud.

2.2 Características Técnicas

El formato de los certificados se basará en el definido por la Unión Internacional de Telecomunicaciones, sector de normalización de las telecomunicaciones, en la recomendación UITT x.509 v3.

Los certificados emitidos deberán:

- Ser conformes a:

- La Ley 59/2003, de Firma Electrónica,
- La ley 11/2007 de Acceso Electrónico del Ciudadano a los Servicios Públicos,
- El Decreto 302/2011 de Régimen Jurídico de la Gestión Electrónica de la Administración Pública de la Comunidad Autónoma de la Región de Murcia.

- Admitidos por el resto de administraciones Públicas.

- Soportados por la plataforma @firma del Ministerio de Hacienda y Administraciones Públicas.

La longitud mínima de la Clave RSA debe dar cumplimiento a la norma de seguridad CCN-STIC-807 (cristología de empleo en el esquema nacional de seguridad) para categoría de sistemas de información de nivel alto.

2.3 Otras características del servicio.

En el procedimiento de obtención de certificados, el adjudicatario desarrollará los elementos necesarios para activar, en el puesto del solicitante, el software que genere a través de su navegador "web' un par de claves, pública y privada, que le permitirá firmar e identificarse, así como proteger la seguridad de sus comunicaciones a través de mecanismos de cifrado.

Las claves privadas serán utilizadas bajo el control del software de navegación "web" del que disponga el propio usuario, enviando todas las claves públicas al adjudicatario con el fin de integrarlas en un certificado.

Las claves privadas de firma permanecerán siempre bajo el control exclusivo de su titular, y guardadas en el soporte correspondiente, no guardándose copia de ellas por el adjudicatario. Si se establecieran en los puntos de acreditación procedimientos de almacenaje intermedio de dichas claves, se definirán con los consiguientes controles de seguridad y posterior borrado seguro, de manera que se certifique que el titular es el único que las posee.

El adjudicatario garantizará que el usuario, Titular del certificado, puede tener el control exclusivo de las claves privadas correspondientes a las claves públicas que se consignan en el certificado, mediante la obtención de las pruebas de posesión oportunas, a través de la adjudicación del número de identificación único

Archivo de las claves públicas. Las claves públicas de los usuarios permanecerán archivadas, por si fuera necesario su recuperación, en archivos seguros, tanto física como lógicamente, durante un período no menor de 15 años.

Exclusividad de las claves. Las claves privadas son exclusivas para los Titulares de los certificados y son de uso personal e intransferible. Las claves públicas son exclusivas para los Titulares de los certificados, independientemente del soporte físico donde estén almacenadas y protegidas.

Renovación de claves. El adjudicatario identifica una relación uno a uno entre la clave pública de un usuario y su certificado de clave pública, no previéndose utilizar distintos certificados para una misma clave. Es por eso que las claves se renovarán con los certificados cuando dicha renovación esté contemplada en la normativa específica aplicable.

La emisión de certificados supone la generación de documentos electrónicos que acreditan la identidad u otras propiedades del usuario y su correspondencia con la clave pública asociada; del mismo modo, la emisión de los certificados implica su posterior envío al directorio de manera que sea accesible por todas las personas interesadas en hacer uso de sus claves públicas.

La emisión de certificados por parte de la Autoridad de Certificación adjudicataria, sólo puede realizarla ella misma, no subrogando a ningún otro organismo o entidad con capacidad de emisión de estos certificados.

El adjudicatario, por medio de su firma electrónica, garantizará los certificados, así como la verificación de la identidad y cualesquiera otras circunstancias personales de sus titulares, Por otro lado, y con el fin de evitar la manipulación de la información contenida en los certificados, el adjudicatario utilizará mecanismos criptográficos para asegurar la autenticidad e integridad de dicho certificado.

El adjudicatario, una vez emitido el certificado, lo publicará y mantendrá una relación de certificados emitidas durante todo el período de vida del mismo en un servicio de acceso telemático, universal, en línea y siempre disponible.

El adjudicatario garantiza para un certificado emitido:

- Que el usuario dispone de la clave privada correspondiente a la clave pública del certificado, en el momento de su emisión.
- Que la información incluida en el certificado se basa en la información proporcionada por el usuario.
- Que no omite hechos conocidos que puedan afectar a la fiabilidad del certificado.

Publicación de certificados de clave pública. El adjudicatario publicará los certificados emitidos en un directorio seguro.

Cuando el certificado sea revocado, temporal o definitivamente, éste será publicado en el Registro de certificados que incluirá una lista de certificados revocados, comprensiva de los certificados expedidos por el adjudicatario cuya vigencia se ha extinguido o suspendido al menos hasta un año después de su fecha de caducidad.

El adjudicatario deberá proporcionar un servicio de validación de los certificados emitidos vía CRL, OCSP y también a través de la Plataforma @firma.

2.4 Otros aspectos del servicio

El SMS dispone de dos dispositivos HSM (Hardware Security Module) de Realsec modelo Crytpsec 2014 con el para la custodia y gestión de certificados externos y generación custodia de llave PKI.

El sistema cumple con las certificaciones de seguridad FISPS 140-2 Nivel 3 y Commond criteria EAL 4+.

Está dotado con APIs criptográficas que cumplen PKCS#11, Microsoft CAPI and CNG y Open SSL

El sistema puede generar peticiones PKCS10 junto con la clave privada e importar certificados en formato PKCS12 o X509.

Se valorará la integración de este sistema con los servicios de la autoridad certificadora o su sustitución servicios similares proporcionados por el adjudicatario.

2.5 Formación

El adjudicatario deberá impartir la formación necesaria para el correcto funcionamiento de los servicios ofrecidos.

3. SOPORTE TECNICO

El adjudicatario pondrá a disposición del SMS un servicio de resolución de incidencias y/o consultas técnicas, en horario de lunes a viernes 8:00 a 20:00, sin limitación en el número de incidencias ni en horas consumidas.

El servicio se prestará tanto por vía telefónica como por correo electrónico.

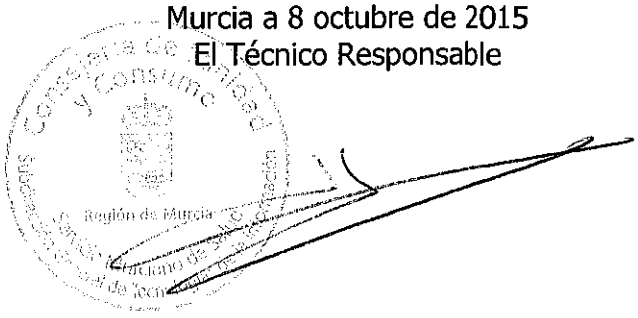
4. CERTIFICACIONES EXIGIDAS

Para la prestación efectiva de los servicios, la empresa deberá disponer al enos de las siguientes certificaciones y auditorias:

- Certificación ISO/IEC 27001, para acreditar la seguridad del sistema.
- Certificación ISO 20000 para acreditar la calidad del sistema
- Certificación Webtrust.
- Auditoría Autoridad de certificación para emitir certificados.

Se consideran requisitos obligatorios para la admisión de la oferta.

Murcia a 8 octubre de 2015
El Técnico Responsable



Fdo. Francisco Javier Francisco Verdú