Pliego de Prescripciones Técnicas.

SERVICIOS DE CERTIFICACIÓN ELECTRONICA 2020

Ref. SGTI 0073/2019

Creación: Octubre 2019

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 reconocido para la persona que tenga condición de empleados públicos del Servicio Murciano de Salud (SMS) y otros servicios de certificación electrónica.

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 **15**
- 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 15 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.
  - El Reglamento (UE) Nº 910/2014
- 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.

Actualmente el SMS tiene integrados estos equipos con la actual autoridad de certificación CA Camerfirma, mediante un middlware desarrollado específicamente que permite descargar automáticamente los certificados de empleado público desde la CA Camerfirma a los HSM. El adjudicatario deberá acreditar que puede prestar el servicio y desarrollar o proporcionar una middleware análogo.

En el anexo I se muestra un esquema del funcionamiento de la integración

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 menos 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 Web trust.
- Auditoría Autoridad de certificación para emitir certificados.

Se consideran requisitos obligatorios para la admisión de la oferta.

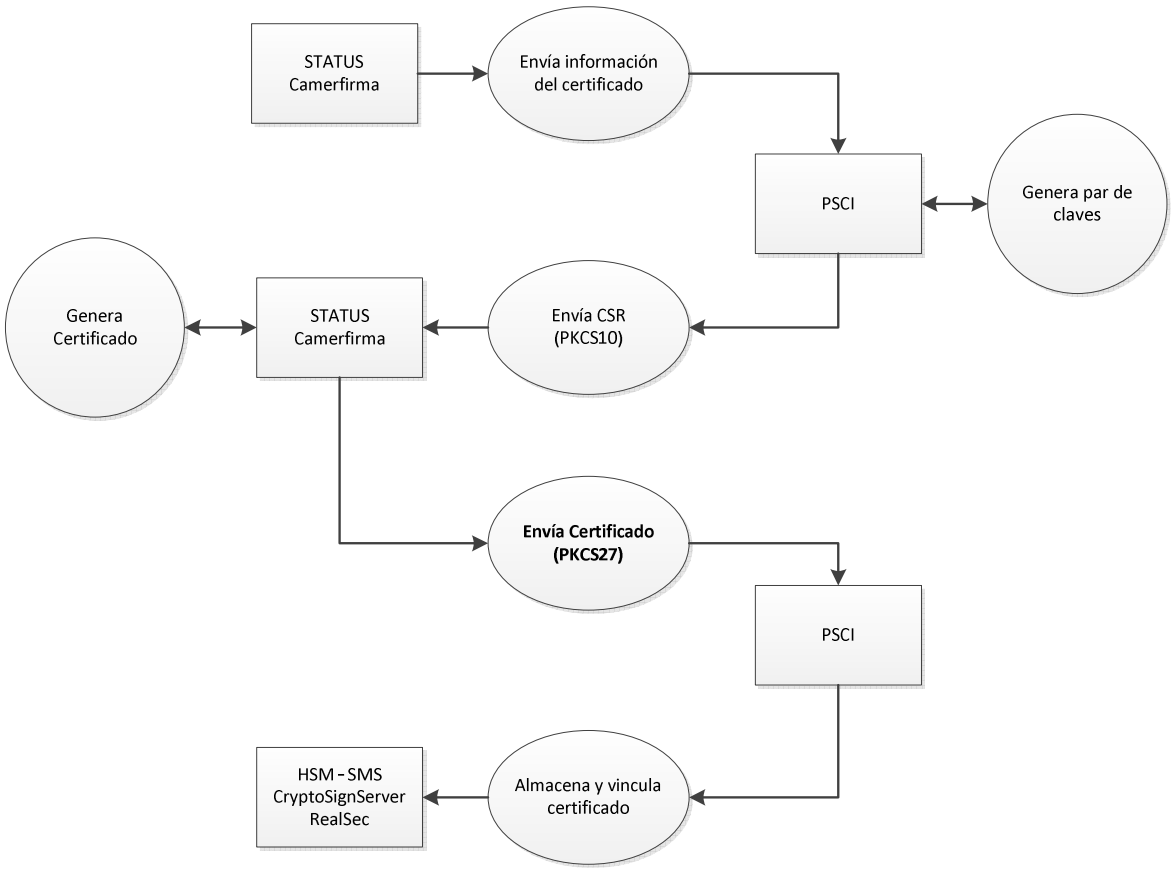
(Fecha y firma electrónica en el margen)
El Técnico Responsable

Fdo. Francisco Javier Francisco Verdú

ANEXO I. INTEGRACION STATUS (CA CAMERFIRMA) - HSM del SMS

PSCIntegration Service es un módulo que gestiona la integración entre Status, la plataforma de emisión de certificados de AC Camerfirma y los HSM de Realsec, la plataforma de almacenamiento y centralización de claves del SMS.

Descripción del proceso.



ANEXO II. CONDICIONES DEL ENCARGO DE TRATAMIENTO DE DATOS PERSONALES

1. **Objeto del encargo del tratamiento:** Se habilita a la parte adjudicataria, encargada del tratamiento, para tratar por cuenta del Servicio Murciano de Salud, responsable del tratamiento, los datos de carácter personal necesarios para la ejecución del presente contrato.

2. **Identificación de la información afectada:**

   Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, el Servicio Murciano de Salud, responsable del tratamiento, pone a disposición de la parte adjudicataria, encargada del tratamiento, la información que se describe en el apartado correspondiente del presente pliego de prescripciones técnicas.

3. **Duración:** La duración del encargo de tratamiento tiene una duración igual a la del contrato.
   Una vez finalice el presente contrato, el encargado del tratamiento debe proceder según se establece en el apartado correspondiente del pliego de prescripciones técnicas.

4. **Obligaciones del encargado del tratamiento:**

   El encargado del tratamiento y todo su personal se obliga a:

   a) Utilizar los datos personales objeto de tratamiento, o los que recoja para su inclusión, sólo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios.

   b) Tratar los datos de acuerdo con las instrucciones del Servicio Murciano de Salud. Si el encargado del tratamiento considera que alguna de las instrucciones infringe el RGPD o cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembros, el encargado informará inmediatamente al Servicio Murciano de Salud.

   c) En el caso de que sea necesario según la normativa vigente, llevar por escrito un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del Servicio Murciano de Salud, que contenga:

      1. El nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado y, en su caso, del representante del responsable o del encargado y del delegado de protección de datos.

      2. Las categorías de tratamientos efectuados por cuenta de cada responsable.

3. En su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49.1.2º del RGPD, la documentación de garantías adecuadas.
4. Una descripción general de las medidas técnicas y organizativas de seguridad relativas a :

    a) La anonimización y el cifrado de datos personales, si procede.
    b) La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
    c) La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
    d) El proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

d) No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del Servicio Murciano de Salud, en los supuestos legalmente admisibles.

El encargado puede comunicar los datos a otros encargados del tratamiento del Servicio Murciano de Salud, de acuerdo con las instrucciones relativas a la entidad a la que se deben comunicar los datos, los datos a comunicar y las medidas de seguridad a aplicar que especifique el Servicio Murciano de Salud por escrito y de forma previa.

e) Subcontratación:

No subcontratar ninguna de las prestaciones que formen parte del objeto de este contrato que comporten el tratamiento de datos personales, salvo los servicios auxiliares necesarios para el normal funcionamiento de los servicios del encargado.

Si fuera necesario subcontratar algún tratamiento, este hecho se deberá comunicar previamente y por escrito al Servicio Murciano de Salud, con una antelación de quince días, indicando los tratamientos que se pretende subcontratar e identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto. La subcontratación podrá llevarse a cabo si el Servicio Murciano de Salud no manifiesta su oposición en el plazo establecido.

El subcontratista, que también tendrá la condición de encargado del tratamiento, está obligado igualmente a cumplir las obligaciones establecidas en este documento para el encargado del tratamiento y las instrucciones que dicte el Servicio Murciano de Salud. Corresponde al encargado inicial regular la nueva relación de forma que el nuevo encargado quede sujeto a las

mismas condiciones (instrucciones, obligaciones, medidas de seguridad…) y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En el caso de incumplimiento por parte del subencargado, el encargado inicial seguirá siendo plenamente responsable ante el Servicio Murciano de Salud en lo referente al cumplimiento de las obligaciones.

f) Mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del presente encargo, incluso después de que finalice su objeto.

g) Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que hay que informarles convenientemente.

h) Mantener a disposición del Servicio Murciano de Salud la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.

i) Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.

j) Asistir al Servicio Murciano de Salud en la respuesta al ejercicio de los derechos de:

1. Acceso, rectificación, supresión y oposición
2. Limitación al tratamiento
3. Portabilidad de datos
4. A no ser objeto de decisiones automatizadas individualizadas

Los interesados o personas afectadas deben ser siempre emplazados a ejercer sus derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas, ante el Servicio Murciano de Salud.

k) Derecho de información:

Corresponde al Servicio Murciano de Salud facilitar el derecho de información en el momento de la recogida de los datos.

l) Notificación de violaciones de la seguridad de los datos.

El encargado del tratamiento notificará al Servicio Murciano de Salud, sin dilación indebida, y en cualquier caso, antes del plazo máximo de 24 horas, las violaciones de la seguridad de los datos personales a su cargo de las que tengan conocimiento, juntamente

con toda la información relevante para la documentación y comunicación de la incidencia.

No será necesaria la notificación cuando sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

m) Realizar o dar apoyo al Servicio Murciano de Salud en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando el Servicio Murciano de Salud determine, además de realizar la evaluación de impacto relativa a la protección de datos inicial según se determina en el apartado correspondiente de este pliego de prescripciones técnicas.

n) Implantar las medidas de seguridad establecidas por el Servicio Murciano de Salud de acuerdo a sus estándares o según los resultados de las correspondientes evaluaciones de riesgos.

En todo caso, deberá implantar mecanismos para:
a) Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
b) Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
c) Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.
d) Seudonimizar y cifrar los datos personales, en su caso.

5. Obligaciones del Servicio Murciano de Salud

Corresponde al responsable del tratamiento:

a) Entregar al encargado los datos a los que se refiere la cláusula 2 de este anexo.
b) Velar por la realización de una evaluación del impacto en la protección de datos personales de las operaciones de tratamiento a realizar por el encargado.
c) Realizar las consultas previas que corresponda.
d) Velar, de forma previa y durante todo el tratamiento, por el cumplimiento del RGPD por parte del encargado.
e) Supervisar el tratamiento, incluida la realización de inspecciones y auditorías.