Dirección General de Tecnologías de la Información y las Comunicaciones

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN DEL SUMINISTRO DE CERTIFICADOS DE EMPLEADO PÚBLICO PARA LA ADMINISTRACIÓN DEL PRINCIPDO DE ASTURIAS. *Expediente nº 47/2018*

C/ Trece Rosas, 2, 5ª planta, sector derecho, 33005 Oviedo. Tfno: 985 10 59 59. Fax: 985 10 59 45

ÍNDICE

C/ Trece Rosas, 2, 5ª planta, sector derecho, 33005 Oviedo. Tfno: 985 10 59 59. Fax: 985 10 59 45

1. *OBJETO*

El objeto del contrato lo constituye el suministro de 3.000 licencias para certificados digitales de empleado público de Camerfirma, que estarán soportados en el HSM (Hardware Security Module) ubicado en el Centro de Proceso de Datos gestionado por la Dirección General de Tecnologías de la Información y las Comunicaciones (en adelante DGTIC).

2. *ANTECEDENTES*

El Servicio de Seguridad perteneciente a la DGTIC que, a su vez, depende de la Consejería de Empleo, Industria y Turismo, tiene atribuidas las competencias en cuanto a políticas de seguridad de los sistemas de información en el ámbito de la Administración del Principado de Asturias (en adelante APA). Los certificados electrónicos constituyen un medio para la identificación y autenticación de los participantes en transacciones electrónicas y el establecimiento de comunicaciones electrónicas seguras. La firma electrónica basada en certificados digitales permite comprobar la procedencia e integridad de los datos, y ofrece una base para el no repudio.

Los certificados electrónicos se basan en la criptografía asimétrica que utiliza dos claves criptográficas únicas y complementarias para las operaciones de cifrado. Una de las claves se debe mantener en secreto (clave privada) mientras que la otra se hace pública y se distribuye con el certificado.

Un certificado electrónico o digital es un documento electrónico emitido y firmado por una Autoridad de Certificación que acredita una identidad y le vincula una clave pública.

El titular o suscriptor de un certificado digital puede ser una persona física o jurídica. En el caso de certificados que identifican a dispositivos, componentes o aplicaciones informáticas, el propietario o titular del certificado es el responsable del dispositivo, componente o aplicación.

El contenido y estructura de los certificados digitales está recogida en la norma ITU-T X509. Además de la clave pública, un certificado electrónico también contiene un número de serie único que lo identifica, el nombre del suscriptor, el nombre de la Autoridad de Certificación emisora, la firma electrónica de la Autoridad de Certificación, el identificador del algoritmo de firma y el período de validez del certificado, pasado el cual, el certificado ya no sirve para sus propósitos.

C/ Trece Rosas, 2, 5ª planta, sector derecho, 33005 Oviedo. Tfno: 985 10 59 59. Fax: 985 10 59 45

3. CONDICIONES DEL SUMINISTRO

3.1.1 Normativa aplicable

El concepto de certificado electrónico está definido en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica. Esta ley también define una clase particular de certificados electrónicos denominados **certificados electrónicos reconocidos** que son aquellos que se han expedido cumpliendo requisitos establecidos en lo que se refiere a su contenido, a los procedimientos de comprobación de la identidad del firmante y a la fiabilidad y garantías de la actividad de certificación electrónica. Estos certificados constituyen la base de la firma electrónica reconocida, que se equipara a la firma manuscrita. La ley de Firma Electrónica también establece las obligaciones de los Prestadores de Servicios de Certificación (Autoridades de Certificación).

El REGLAMENTO (UE) N o 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE, también define el concepto de **certificado cualificado de firma electrónica**, que es aquel certificado de firma electrónica que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el Anexo I del propio reglamento en cuanto a su contenido.

La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece los mecanismos para la identificación electrónica de las administraciones públicas y la autenticación en el ejercicio de su competencia. De esta ley se derivan los certificados reconocidos o cualificados de **sede electrónica**, **sello electrónico** y **empleado público**.

El Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007 (aunque esta ley ha sido derogada con la Ley 39/2015) establece los usos y contenidos mínimos de los certificados de sede, sello y empleado público. El RD 1671/2009 también establece que el Esquema Nacional de Seguridad (Real Decreto 3/2010, de 8 de enero) determinará las características y requisitos que cumplirán los sistemas de firma electrónica, los certificados y los medios equivalentes que se establezcan en las sedes electrónicas para la identificación y garantía de una comunicación segura, así como, el modo de emitir los certificados de sello electrónico.

C/ Trece Rosas, 2, 5ª planta, sector derecho, 33005 Oviedo. Tfno: 985 10 59 59. Fax: 985 10 59 45

3.1.2 Tipos de certificados objeto del suministro

Certificados cualificados de empleado público derivados de la ley 40/2015:

- **Certificado cualificado de empleado público.** Vincula a un empleado público con la Administración Pública en la que presta sus servicios. Se emplea para identificación y para la firma electrónica de documentos y únicamente otorga a su titular las facultades que posee en el desempeño de sus competencias.
- En este caso los certificados serán soportados en el HSM (Hardware Security Module) corporativo. Dado que el HSM corporativo está vinculado por contrato a la Autoridad de Certificación Camerfirma y que la DGTIC del Principado de Asturias funciona como Autoridad de Registro de Camerfirma para la explotación de los certificados soportados en HSM, **los certificados deberán corresponder a la Autoridad de Certificación Camerfirma**.

3.1.3 Características técnicas del suministro

Los certificados digitales que se suministren cumplirán lo siguiente:

- Deberán cumplir los requisitos establecidos en la normativa legal aplicable a certificados de empleado público.
- Deberán estar soportados por la plataforma @firma del Ministerio de Hacienda y Función Pública.
- Algoritmo de firma SHA2RSA
- Algoritmo de hash SHA2
- Clave pública de 2048 bits

La emisión de un certificado se realizará siempre a petición expresa del responsable del contrato o representante.

Oviedo, 25 de julio de 2018

Juan Carlos Rodríguez Rodríguez
ANALISTA PROGRAMADOR

C/ Trece Rosas, 2, 5ª planta, sector derecho, 33005 Oviedo. Tfno: 985 10 59 59. Fax: 985 10 59 45