III. Otras Resoluciones

Consejería de Presidencia, Justicia y Seguridad

1917 *Dirección General de Telecomunicaciones y Nuevas Tecnologías.- Resolución de 15 de diciembre de 2009, por la que se dispone la publicación de la Adenda al Convenio suscrito el 30 de noviembre de 2008 entre el Gobierno de Canarias y la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, para la prestación de servicios técnicos y de seguridad aplicables a la certificación y firma electrónica en el ámbito de las Administraciones Públicas.*

De acuerdo con lo previsto en el artículo 8, apartado 2, de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, modificada por la Ley 4/1999, de 13 de enero,

R E S U E L V O:

Ordenar la publicación en el Boletín Oficial de Canarias de la Adenda al Convenio suscrito el 30 de noviembre de 2008 entre el Gobierno de Canarias y la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, para la prestación de servicios técnicos y de seguridad aplicables a la certificación y firma electrónica en el ámbito de las Administraciones Públicas, que figura como anexo a la presente Resolución.

Santa Cruz de Tenerife, a 15 de diciembre de 2009.- El Director General de Telecomunicaciones y Nuevas Tecnologías, Tomás Ríos Rull.

A N E X O

ADENDA AL CONVENIO SUSCRITO EL 30 DE DICIEMBRE de 2008 ENTRE EL GOBIERNO DE CANARIAS Y LA FÁBRICA NACIONAL DE MONEDA Y TIMBRE-REAL CASA DE LA MONEDA, PARA LA PRESTACIÓN DE SERVICIOS TÉCNICOS Y DE SEGURIDAD APLICABLES A LA CERTIFICACIÓN Y FIRMA ELECTRÓNICA EN EL ÁMBITO DE LAS ADMINISTRACIONES PÚBLICAS.

Santa Cruz de Tenerife, a 3 de noviembre de 2009.

REUNIDOS

De una parte, el Excmo. Sr. José Miguel Ruano León, Consejero de Presidencia, Justicia y Seguridad, actuando en nombre y representación de la Administración Pública de la Comunidad Autónoma de Canarias, en virtud de las facultades que le confiere el artículo 29.1.k) de la Ley 14/1990, de 26 de julio, de Régimen Jurídico de las Administraciones Públicas de Canarias.

Y de otra parte D. Ángel Esteban Paúl, Director General de la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda (en adelante FNMT-RCM), actuando en representación de esta Entidad Pública Empresarial, en virtud del nombramiento efectuado por el Real Decreto 1.869/2008, de 8 de noviembre, y de las competencias que le atribuye el artículo 19 del Estatuto de esta Entidad, aprobado por Real Decreto 1.114/1999, de 25 de junio.

Reconociéndose la capacidad legal necesaria para formalizar la presente Adenda al Convenio citado, ambas partes

EXPONEN

Primero.- Que el Gobierno de Canarias y la FNMT-RCM suscribieron, con fecha 30 de diciembre de 2008, un Convenio para la prestación de servicios de certificación de firma electrónica en el ámbito de actuación del Gobierno de Canarias, así como de los servicios relativos al ámbito de aplicación de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, con el alcance definido en tal convenio y sus documentos anexos.

Segunda.- Que por parte de la FNMT-RCM se han implementado, desde el 30 de diciembre de 2008 en que fue suscrito el Convenio entre el Gobierno de Canarias y la FNMT-RCM hasta el día de hoy, algunas ampliaciones en las prestaciones de servicios así como en sus dotaciones inicialmente previstas.

Con el fin de dotar al Gobierno de Canarias -en concordancia con el ámbito de aplicación para servicios del ámbito del artículo 81 establecido en el referido Convenio, detallado en su cláusula segunda- de los servicios relativos tanto a la prestación de servicios de certificación de firma electrónica como a los de la Administración Electrónica, recogidos en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, en el ámbito de actuación del Gobierno de Canarias, ambas partes acuerdan ampliar las dotaciones establecidas en el capítulo II del anexo I, en las del anexo IV y en las de los capítulos II y III del anexo V del Convenio, con arreglo a las siguientes

CLÁUSULAS

PRIMERA. AMPLIACIÓN DEL CAPÍTULO II DEL ANEXO I DEL CONVENIO.

Inclusión de nuevo texto sobre el ya existente en los términos siguientes:

Validación de certificados vía OCSP.

CONSULTA DEL ESTADO DE VALIDEZ DE CERTIFICADOS VÍA OCSP (ON-LINE CERTIFICATE STATUS PROTOCOL).

INTRODUCCIÓN.

Uno de los usos de los certificados electrónicos por parte de terceras personas es la verificación de firmas electrónicas efectuadas por el titular del certificado. Sin embargo, aunque la firma electrónica de un determinado documento sea verificada y sea correcta, puede que el poseedor haya invalidado ese certificado con anterioridad a la realización de esa firma. Este proceso, efectuado a petición del propio titular, se denomina revocación del certificado y siempre que se verifique una firma se debe comprobar la validez del certificado del firmante.

Uno de los usos de los certificados electrónicos por parte de terceras personas es la verificación de firmas electrónicas efectuadas por el usuario del certificado. Sin embargo, la firma electrónica de un determinado documento ha de ser verificada en el momento de su utilización, ya que puede que el usuario haya invalidado ese certificado con anterioridad a la realización de esa firma (revocación/suspensión del certificado) o se haya producido la caducidad del mismo por las causas legales correspondientes. Por tanto, es necesario que siempre que se utilice un certificado para generar una firma electrónica se debe comprobar, en tiempo real, la validez de dicho certificado del firmante.

Para realizar esta comprobación existen varios métodos:

Comprobación de CRLs: cuando se solicita la revocación de un certificado, la CA emite y firma una CRL en la que se incluyen los certificados revocados. El usuario que desee verificar el estado de un certificado deberá acceder al directorio donde se publican las CRLs y comprobar si en la CRL que corresponda se encuentra ese certificado.

Verificación OCSP: la verificación OCSP se realiza accediendo al servicio de OCSP. Este servicio abstrae al usuario del acceso al directorio y de la comprobación de la CRL, devolviendo al usuario el estado del certificado objeto de consulta tras una petición de verificación.

PROCEDIMIENTO.

Básicamente el procedimiento podrá realizarse de la siguiente manera, sin perjuicio de otras opciones posibles, según las condiciones técnicas del servicio:

Un usuario, persona física, que dispone de un certificado electrónico “Clase 2” de la FNMT-RCM desea acceder a los servicios electrónicos del Gobierno de Canarias utilizando, como medio de identificación, su certificado.

El usuario accede a la página Web o a las aplicaciones con conexión a Internet del Gobierno de Canarias con el fin de utilizar los servicios electrónicos disponibles, utilizando la identificación que proporciona el certificado emitido por la FNMT-RCM a través de la firma electrónica que genera.

Una vez producido el acceso se abre una ventana en la que el usuario obtiene la autorización de uso por parte de la FNMT-RCM y presta consentimiento expreso para que se lleven a cabo los servicios de consulta del estado de validez y poder utilizar su certificado en el ámbito de actuación correspondiente (según la advertencia que figura), y en la que se informará al mismo del régimen de protección de datos y demás condiciones de uso.

Simultáneamente el sistema del Gobierno de Canarias solicita la validación (OCSP) del certificado al servidor de la FNMT-RCM, el cual le devuelve la información precisa sobre la vigencia, o no, del certificado. En caso de que el certificado esté suspendido o revocado, rechazará la petición de acceso impidiendo continuar con la gestión.

En caso de que el certificado esté vigente y sea válido, el sistema permitirá el acceso a los servicios del Gobierno de Canarias finalizando, en este momento, los servicios prestados por la FNMT-RCM.

DESCRIPCIÓN DEL SERVICIO.

El servicio de consulta del estado de validez de certificados vía OCSP se basa en una arquitectura cliente-servidor. El usuario solicitante de la verificación de un certificado vía OCSP será el que haga uso de la aplicación cliente y la autoridad de validación OCSP hará las labores de servidor.

Servidor OCSP Responder.

El servidor de OCSP (OCSP responder) comprueba la firma de la petición OCSP efectuada por un cliente OCSP registrado en el sistema (base de datos de clientes de los cuales se admiten peticiones) y verifica el estado de los certificados objeto de consulta incluidos en dicha petición. En caso de que la firma de la petición OCSP sea inválida (certificado revocado o caducado, por ejemplo), la petición se rechaza y se retorna al cliente OCSP una respuesta negativa. En la respuesta de OCSP se informará del estado en el que se encuentran los certificados en ese momento.

Las librerías utilizadas son de BouncyCastle (http://www.bouncycastle.org/).

OCSP Cliente.

Herramienta cliente para hacer peticiones de OCSP. Se pueden utilizar los productos del mercado. La FNMT-RCM facilitará una relación con productos de libre distribución, pero en ningún caso suministrará un OCSP cliente, pues se pueden encontrar con facilidad en el mercado de forma estándar.

Los intercambios de información entre las partes cliente y servidor OCSP se ajustarán a las estructuras definidas por el estándar RFC 2560, correspondiente a la norma de OCSP (Online Cetificate Status Protocol) de IETF-PKIX.

Una petición de OCSP contiene los siguientes datos:

Versión del protocolo.

Identificador/es del/los certificado/s a verificar.

Extensiones.

Firma.

Cuando se recibe la petición, el servidor de OCSP determina si el mensaje está correctamente formado y contiene la información necesaria para poder componer una respuesta satisfactoria.

Todas las respuestas proporcionadas por el servidor de OCSP deben ser firmadas digitalmente, y además deben componer los siguientes campos:

Versión de la respuesta.

Nombre del OCSP Responder.

Respuestas para cada uno de los certificados.

Extensiones opcionales.

OID del algoritmo de firma.

Firma.

La respuesta para cada uno de los certificados consiste en:

Identificador del certificado.

Estado del certificado.

Intervalo de validez de la respuesta.

Extensiones opcionales.

El estado de un certificado puede ser:

Good.

Revoked.

Unknown.

SEGUNDA. AMPLIACIÓN DEL ANEXO IV DEL CONVENIO.

Inclusión de nuevo texto sobre el ya existente en los términos siguientes:

CERTIFICADO DE FIRMA ELECTRÓNICA DEL PERSONAL AL SERVICIO DE LAS ADMINISTRACIONES PÚBLICAS.

FNMT-RCM no regula el uso de este certificado, dado que se establece en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y demás legislación aplicable, limitándose a crear una infraestructura técnica a disposición de la Administración, Organismo o Entidad pública titular correspondiente. Asimismo, todas aquellas circunstancias y requisitos referentes a los usuarios, por la propia naturaleza de los certificados de empleado público, serán controlados, exclusivamente, por la Administración, informando a la FNMT-RCM de su alteración o modificación; todo ello, a través de las Oficinas de Registro habilitadas por las Administraciones, Organismos y Entidades públicas.

La infraestructura de servicios de certificación y firma electrónica de la FNMT-RCM permite diferentes usos y funcionalidades:

1) Uso principal. El uso principal del certificado de empleado público es la identificación electrónica y autenticación conjunta de la Administración, Organismo o Entidad pública actuante en el ejercicio de sus competencias y de la identidad, cargo o empleo del personal a su servicio. Este certificado es la certificación electrónica emitida por la FNMT-RCM que vincula a su titular (la Administración, Órgano, Organismo o Entidad pública) con unos datos de verificación de firma y confirma: (1) la identidad del firmante y custodio de las claves (personal al servicio de las Administraciones Públicas que realiza firmas electrónicas utilizando el certificado en nombre de la Administración actuante), su número de identificación personal, cargo, puesto de trabajo y/o condición de autorizado, y (2) al titular del certificado, que es el Órgano, Organismo o Entidad de la Administración pública, bien sea ésta General, Autonómica, Local o Institucional.

2) Otros usos. Este certificado podrá ser utilizado por el personal (firmante/custodio) para actuaciones funcionariales, administrativas o laborales, relacionadas con los diferentes derechos y obligaciones del personal al servicio de las Administraciones Públicas en el ámbito de su Administración, Organismo o Entidad pública de dependencia o, en su caso, con el resto del Sector Público.

3) Uso no autorizado. El personal usuario no está autorizado para utilizar estos certificados para usos distintos a los establecidos en los apartados 1) y 2) anteriores.

4) Marco legislativo. El uso del certificado de empleado público se realizará en el ámbito de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y de conformidad con las competencias de la Administración, Organismo o Entidad pública actuante y de las facultades conferidas a su personal (independientemente de su condición: funcionarial, laboral, estatutaria, etc.) en virtud de su nombramiento, designación, contrato o instrumento jurídico que regule su relación con tales Administraciones.

El perfil del certificado es el descrito en las declaraciones de prácticas de certificación.

SELLO ELECTRÓNICO DE LAS ADMINISTRACIONES PÚBLICAS.

FNMT-RCM no regula el uso de este certificado, dado que se establece en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y demás legislación aplicable, limitándose a crear una infraestructura técnica a disposición de los usuarios y custodios de la Administración, Organismo o Entidad pública titular del certificado, propietario o responsable de la unidad administrativa y del componente informático correspondiente. Asimismo, todas aquellas circunstancias y requisitos referentes a los usuarios y custodios, por la propia naturaleza de los certificados de Sello electrónico de las AA.PP., serán controlados, exclusivamente, por la Administración, informando a la FNMT-RCM de su alteración o modificación; todo ello, a través de las Oficinas de Registro habilitadas por las Administraciones, Organismos y Entidades públicas.

La infraestructura de servicios de certificación y firma electrónica de la FNMT-RCM permite diferentes usos y funcionalidades:

1) Uso principal. El uso principal del certificado de Sello electrónico de las AA.PP. es la identificación y autenticación del ejercicio de la competencia en la actuación administrativa automatizada y la autenticación de documentos y actuaciones de la Administración, Organismo o Entidad pública titular del mismo. Los certificados de Sello electrónico de las AA.PP. son aquellos certificados expedidos por la FNMT-RCM que vinculan unos datos de verificación de firma a los datos identificativos y de autenticación de determinada Administración, Organismo o Entidad pública y sus respectivas unidades organizativas (unidad que realiza la actuación administrativa automatizada a través de componentes informáticos -área, sección, departamento-) y vinculan a la persona física responsable de la Oficina de Registro y/o representante de la Administración, Organismo o Entidad titular del certificado en quien se delegue y que actuarán como custodios del certificado y sus claves.

2) Uso no autorizado. El usuario y/o custodio no está autorizado para utilizar estos certificados para usos distintos a los establecidos en el apartado 1) anterior.

3) Marco legislativo. El uso del certificado de Sello electrónico de las AA.PP. se realizará en el ámbito de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y de conformidad con las competencias de la unidad perteneciente a la Administración, Organismo o Entidad pública titular de la misma y de la infraestructura que alberga el certificado de Sello electrónico de las AA.PP.

El perfil del certificado es el descrito en las declaraciones de prácticas de certificación.

SEDES ELECTRÓNICAS DE LAS ADMINISTRACIONES ELECTRÓNICAS.

FNMT-RCM no regula el uso de este certificado, dado que se establece en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y demás legislación aplicable, limitándose a crear una infraestructura técnica a disposición de los usuarios y custodios de la Administración, Organismo o Entidad pública titular de la Sede electrónica correspondiente. Asimismo, todas aquellas circunstancias y requisitos referentes a los usuarios y custodios, por la propia naturaleza de los certificados para la identificación de Sedes electrónicas, serán controlados, exclusivamente, por la Administración, informando a la FNMT-RCM de su alteración o modificación; todo ello, a través de las Oficinas de Registro habilitadas por las Administraciones, Organismos y Entidades públicas.

La infraestructura de servicios de certificación y firma electrónica de la FNMT-RCM permite diferentes usos y funcionalidades:

1) Uso principal. El uso principal del certificado es la identificación de Sedes electrónicas y establecimiento de comunicaciones seguras con dichas Sedes. Los certificados para la identificación de Sedes electrónicas son aquellos certificados expedidos por la FNMT-RCM y que vinculan unos datos de verificación de firma a (1) los datos identificativos de una Sede electrónica en la que existe una persona física

que actúa como custodio del certificado y sus claves y (2) el titular del certificado que es la Administración, Organismo o Entidad pública a la que pertenece y que es, además, titular de la dirección electrónica, dominio e infraestructura a través de la que se accede a la Sede electrónica.

2) Uso no autorizado. El usuario y/o custodio no está autorizado para utilizar estos certificados para usos distintos a los establecidos en el apartado 1) anterior.

3) Marco legislativo. El uso del certificado para la identificación de Sedes electrónicas se realizará en el ámbito de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y de conformidad con las competencias de la Administración, Organismo o Entidad pública titular del dominio y de la infraestructura que alberga la Sede electrónica.

El perfil del certificado es el descrito en las declaraciones de prácticas de certificación

TERCERA. AMPLIACIÓN DEL CAPÍTULO II DEL ANEXO V DEL CONVENIO.

Inclusión de nuevo texto sobre el ya existente en los términos siguientes:

Servicio de validación de certificados vía OCSP.

Queda incluida en las condiciones económicas del Convenio firmado el 30 de diciembre de 2008, la prestación del presente servicio.

CUARTA. MODIFICACIÓN DEL CAPÍTULO III DEL ANEXO V DEL CONVENIO.

Modificación del texto sobre el ya existente, manteniéndose el resto de los demás apartados del capítulo III, según sigue:

Certificados de sede electrónica y de sello electrónico para actuaciones automatizadas para los servicios del ámbito de la Ley 11/2007.

El precio anual de los servicios del ámbito de la Ley 11/2007 establecido en el apartado 1 del Capítulo I del presente anexo II de Precios incluye:

a) Para el Gobierno de Canarias, 150 certificados de sede electrónica o de sello electrónico.

b) Para cada Cabildo Insular, 10 certificados de sede electrónica o de sello electrónico.

c) Para los municipios adheridos al Convenio con población igual o superior a 50.000 habitantes, 6 certificados de sede electrónica o de sello electrónico.

d) Para los municipios adheridos al Convenio con población inferior a 10.000 habitantes, 2 certificados de sede electrónica o de sello electrónico.

e) Para el resto de entidades y organismos adheridos al Convenio, 3 certificados de sede electrónica o de sello electrónico.

El precio de los certificados adicionales tanto de sede electrónica como de sello electrónico será de 900,00 euros por cada unidad y año de certificado siendo emitidos todos ellos por tres años.

QUINTA. RESTO DE CONDICIONES. COMUNICACIÓN.

Quedan subsistentes y sin alteración el resto de condiciones, no modificadas en este acto, que integran el Convenio suscrito entre el Gobierno de Canarias y la FNMT-RCM, con fecha 30 de diciembre de 2008 del que esta Adenda constituye parte integrante a todos los efectos.

El Gobierno de Canarias comunicará, a los organismos y entidades locales adheridas al Convenio principal, la ampliación del objeto que se recoge en esta Adenda. Para ello, se establecerán calendarios de implantación de los nuevos servicios de acuerdo con las disponibilidades técnicas y presupuestarias de las partes y el alcance de los citados calendarios.

SEXTA. ENTRADA EN VIGOR.

La presente Adenda entrará en vigor el día de su firma.

Y, en prueba de conformidad, ambas partes suscriben la presente Adenda, por duplicado ejemplar, en el lugar y fecha indicados en el encabezamiento.- El Director General de la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, Ángel Esteban Paúl.- El Consejero de Presidencia, Justicia y Seguridad del Gobierno de Canarias, José Miguel Ruano León.