CONVENIO DE COLABORACIÓN ENTRE LA ENTIDAD PÚBLICA EMPRESARIAL RED.ES Y EL CONSEJO GENERAL DE LA ABOGACIA ESPAÑOLA PARA EL ESTABLECIMIENTO DE LA RELACIÓN DE CONFIANZA EN LOS CERTIFICADOS EMITIDOS POR LA AUTORIDAD DE CERTIFICACIÓN DE LA ABOGACIA (ACA)

En Madrid, a 25 de abril de 2005

REUNIDOS

De una parte, Carlos Carnicer Diez, mayor de edad, con N.I.F. , en nombre y representación, en su calidad de Presidente, de del Consejo General de la Abogacía Española, domiciliada en Paseo de Recoletos, 13.

De otra, D. Ramón Palacio León, Director General de la Entidad Pública Empresarial Red.es, en nombre y representación de dicha Entidad Pública Empresarial en virtud de los dispuesto en el artículo 14.1. k) de su Estatuto aprobado por Real Decreto 164/2002 de 8 de febrero.

Ambas partes se reconocen la capacidad jurídica necesaria para suscribir el presente Convenio y en su virtud

EXPONEN

PRIMERO.- La Sociedad de la Información es un estadio de desarrollo social caracterizado por el empleo masivo de las nuevas tecnologías para el acceso, transacción y difusión de la información.

Su desarrollo representa un importante instrumento para superar las desigualdades consecuencia de las barreras geográficas, sociales y económicas que tradicionalmente han restringido el acceso a multitud de servicios, ofreciendo un ilimitado potencial para promover la igualdad de oportunidades entre los ciudadanos. Las nuevas tecnologías juegan ya un papel clave en la mejora de la eficiencia, siendo la causa de importantes mejoras de la productividad, y un poderoso motor para el crecimiento, la competitividad y el empleo.

Por ello, la implantación de la Sociedad de la Información constituye un factor clave para el aumento del bienestar económico y social, y es, por tanto, una herramienta estratégica y objetivo de primer nivel para el desarrollo de los países.

SEGUNDO.- La intervención pública a todos sus niveles se hace necesaria si se quiere acelerar dicha implantación, a través de actuaciones de largo

alcance por parte de las Administraciones, tanto en ciudadanos, empresas como en las propias Administraciones Públicas, garantizando la participación de toda la sociedad, y evitando la exclusión de determinados colectivos, previniendo, de esta forma, la llamada "brecha digital".

TERCERO.- El artículo 55 de la Ley 14/2000, de 29 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social, que modifica la Disposición Adicional 6ª de la Ley 11/1998 de 24 de abril, General de Telecomunicaciones, aun vigente en virtud de la letra b) de la Disposición Derogatoria Única de la Ley 32/2003, General de Telecomunicaciones, configura a Red.es como una Entidad Pública Empresarial atribuyéndole, entre otras funciones, la relativa al fomento y desarrollo de la Sociedad de la Información.

El Real Decreto 164/2002, de 8 de febrero, por el que se aprueba el Estatuto de la Entidad Pública Empresarial Red.es (en adelante, "Red.es"), establece que corresponde a Red.es la gestión de los programas de difusión dirigidos a promover el conocimiento de las telecomunicaciones y de la sociedad de la información.

CUARTO.- El Plan de Choque para el Impulso de la Administración Electrónica en España, de 8 de mayo de 2003, establece la necesidad para las Administraciones Públicas de reforzar la apuesta por la Administración Electrónica, avanzando en la optimización y eficacia del servicio global prestado a los ciudadanos y a las empresas por los distintos niveles de la Administración, tanto en el ámbito nacional, autonómico y local, como en el de la Unión Europea.

QUINTO.- La Entidad Pública Empresarial Red.es, adscrita al Ministerio de Industria, Turismo y Comercio a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, tiene encomendada la ejecución de determinadas medidas previstas en el Plan de Choque con el objeto de poner a disposición de las Administraciones Públicas diversos servicios de Administración Electrónica.

SEXTO.- Por su parte el Consejo General de la Abogacía Española (en adelante CGAE) es el órgano representativo, coordinador y ejecutivo superior de los Ilustres Colegios de Abogados de España, y tiene a todos los efectos la condición de corporación de Derecho Público, con personalidad jurídica propia y plena capacidad para el cumplimiento de sus fines, de conformidad con el artículo 67 del Estatuto General de la Abogacía Española, aprobado por Real Decreto 658/2001, de 22 de junio, publicado en el BOE de 10 de julio de 2001.

El CGAE se ha constituido en Prestador de Servicios de Certificación que emite certificados reconocidos a través de la Autoridad de Certificación de la Abogacía, de acuerdo con lo establecido en la Ley 59/2003 de 19 de diciembre, con el objeto de impulsar la utilización de las nuevas tecnologías en el ámbito de la abogacía y facilitar, mejorar y modernizar el ejercicio de

la profesión, identificando la condición de Abogado en la red con las garantías de seguridad que ofrece la legislación vigente.

Para la prestación de servicios de certificación y de firma electrónica, la Autoridad de Certificación de la Abogacía relaciona una determinada clave pública con una entidad concreta a través de la emisión de un certificado electrónico reconocido.

SÉPTIMO.- La Ley 59/2003, de 19 de diciembre, de firma electrónica regula el uso de la firma electrónica, el reconocimiento de su eficacia jurídica y la prestación al público de servicios de certificación, extendiendo el ámbito subjetivo a todos los prestadores de servicios establecidos en España, y derogando el Real Decreto Ley 14/1999, de 17 de septiembre, de firma electrónica.

OCTAVO.- Ambas partes están interesadas en la firma del presente Convenio para establecer las relaciones de confianza adecuadas en los certificados emitidos por la Autoridad de Certificación de la Abogacía, para su utilización en los servicios telemáticos que Red.es pone a disposición de los ciudadanos, las empresas y, las Administraciones Públicas.

Por ello formalizan el presente Convenio de colaboración de acuerdo con las siguientes

CLÁUSULAS

PRIMERA.- Objeto

El presente Convenio tiene por objeto establecer los términos y condiciones en los que la Entidad Pública Empresarial Red.es y el CGAE colaborarán en el intercambio de información técnica para que el módulo de identificación de usuarios de los servicios electrónicos y telemáticos de Red.es reconozca la validez de los certificados electrónicos emitidos por la Autoridad de Certificación de la Abogacía.

SEGUNDA.- Ámbito de aplicación

La aplicación de este Convenio abarcará el conjunto de servicios electrónicos y telemáticos de Red.es que requieran de la utilización de certificados digitales con fines de identificación, de generación de firma electrónica o de cifrado de información.

TERCERA: Obligaciones del CGAE

El CGAE asume las siguientes obligaciones:

a) Cumplir con las obligaciones de los prestadores de servicios de certificación que expiden certificados electrónicos reconocidos, conforme a lo establecido en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

b) Facilitar a Red.es la información necesaria para que pueda conocer las especificaciones técnicas de su sistema de certificación, que cumplirán con lo dispuesto en el Anexo.

CUARTA.- Obligaciones de Red.es

Red.es asume las siguientes obligaciones:

a) Reconocer la validez de los certificados emitidos por la Autoridad de Certificación de la Abogacía a los efectos de identificación de usuarios y su condición de Colegiado de un Colegio de Abogados o empleado, así como de generación de firma electrónica empleados en sus servicios electrónicos y telemáticos.

b) Comprobar el estado de vigencia de los certificados digitales cada vez que éstos sean empleados por sus titulares, haciendo uso de los medios que con este fin pone Autoridad de Certificación de la Abogacía, a disposición de los usuarios y que se concretan en los sistemas basados en consulta de listas de certificados revocados (CRLs), o sistemas de comprobación en línea (OCSP) o cualesquiera otros sistemas que hayan sido aprobados.

QUINTA.- Obligaciones comunes

La prestación de los servicios de certificación que se recogen en el presente Convenio se realizará de acuerdo con lo dispuesto en la Ley 59/2003, de 19 de diciembre, de firma electrónica, y en aquellas que sean de aplicación.

SEXTA.- Plazo de duración del Convenio

El presente Convenio comenzará su vigencia a partir del día de su firma, y tendrá una duración de un año. El Convenio se prorrogará automáticamente por períodos anuales si no concurre manifestación en contra por alguna de las partes con una antelación mínima de un mes a la fecha de vencimiento.

SÉPTIMA.- Revisión del Convenio

Tanto Red.es como el CGAE podrán proponer la revisión de este Convenio en cualquier momento para introducir las modificaciones que estimen pertinentes.

OCTAVA.- Protección de Datos Personales

El régimen de protección de datos de carácter personal en las actuaciones que se desarrollen en ejecución del presente Convenio será el previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en su normativa de desarrollo.

NOVENA.- Resolución del Convenio

El CGAE podrá resolver el presente Convenio cuando Red.es incumpliese con sus obligaciones, recogidas en la cláusula cuarta de este Convenio.

Por su parte, Red.es podrá instar la resolución del Convenio cuando hubiese incumplimiento de las obligaciones que corresponden al CGAE

DÉCIMA.- Régimen Jurídico

El presente Convenio tiene la naturaleza de los Convenios de colaboración previstos en el artículo 3.1 d) del Texto Refundido de la Ley de Contratos de las Administraciones Públicas, aprobado por el Real Decreto Legislativo 2/2000, de 16 de junio.

Y en prueba de cuanto antecede, las Partes suscriben el Convenio, en dos ejemplares y a un solo efecto, en el lugar y fecha señalados en el encabezamiento.

POR LA ENTIDAD PÚBLICA EMPRESARIAL RED.ES	POR EL CONSEJO GENERAL DE LA ABOGACÍA ESPAÑOLA
	CONSEJO GENERAL DE LA ABOGACIA ESPAÑOLA 10 MAY 2005 Núm. 1637 SALIDA
D. RAMÓN PALACIO LEÓN DIRECTOR GENERAL	D. CARLOS CARNICER DIEZ PRESIDENTE

ANEXO TÉCNICO

Las aplicaciones de Red.es serán compatibles técnicamente con todos los certificados expedidos por prestadores de certificación que cumplan los requisitos técnicos descritos más abajo.

Requisitos para la Interoperatividad Técnica:

1- Se admitirán los certificados compatibles con la norma UIT-T X509 v3 de formato de certificado electrónico y además se exigirá la compatibilidad con el perfil de certificado para uso en Internet definido en el documento RFC3280 (sucesor del RFC2459) del Internet Engineering Task Force (IETF). Se advierte que el uso de extensiones críticas fuera de las recomendadas en RFC3280 (RFC2459) pueden prevenir su uso en las aplicaciones de Red.es. El objetivo último en la aceptación de los certificados, es la identificación fehaciente de personas físicas y jurídicas en su relación con los servicios de Red.es, así como la capacidad de expresión de su voluntad mediante firma electrónica (reconocida). Este propósito exige que sea posible determinar un identificador unívoco de la persona a partir del certificado. Red.es utiliza en sus sistemas un identificador unívoco basado en el identificador legal en el ámbito español; NIF y/o nombre, NIE, CIF y/o razón social. Para codificar el identificador único del usuario se recomienda el uso del campo "subject" del certificado o las siguientes extensiones: "subjectAltName".

2- Los certificados contarán con una referencia a la política bajo la que se emiten. Red.es aceptará la política de certificación a los efectos de uso del certificado para identificación fehaciente y firma electrónica de manera general como se indica en el presente convenio. Otras limitaciones presentes en el certificado, que supongan responsabilidades para el confiante (en este caso Red.es), como el respeto al límite de importe de transacciones, requerirán de convenios específicos para el uso de los certificados en aplicaciones específicas, de manera que éstas puedan reforzar las limitaciones expresadas en el certificado y política.

3- Los algoritmos de firma y resumen cryptográfico (hash) soportados por Red.es aún no están determinados pero se soportará al menos RSA y los algoritmos de hashing más extendidos (md2, md5, sha-1). Los certificados no deberán utilizar algoritmos no soportados por Red.es pues no serán admitidos.

4- Para ser admitidos, los certificados deberán incluir las extensiones "subjectKeyIdentifier" y "authorityKeyIdentifier" que permitan una validación eficiente del certificado y la cadena de confianza asociada.

5- Los Prestadores de Servicios de Certificación (PSCs) dispondrán de sistemas de recuperación información de estado de certificados o validación, que permitan comprobar el estado de los certificados en todo momento. Red.es soportará los mecanismos de obtención de estado de certificados más extendidos en el mercado, tanto actuales como futuros. De acuerdo con el estado actual del arte, se requiere al menos uno de los siguientes:

- Publicación de listas de certificados revocados (CRLs). Las listas de certificados revocados cumplirán la especificación CRLv2 establecida en el RFC3280 (RFC2459). Se requerirá al menos acceso mediante protocolo LDAP (RFC2251 y/o RFC1777), o bien http/https (RFC2585).

- Servidor de estado de certificados en línea (OCSP). El servidor deberá responder al protocolo estándar definido en el documento RFC2560 del IETF, y soportará todas las opciones, en particular la extensión "nonce". El protocolo no impone ningún tipo de transporte para los mensajes allí descritos, pero se exigirá al menos el transporte mediante http/https según especifica el documento aludido.

Los prestadores de certificación pondrán a disposición de Red.es estos sistemas de manera que sea posible comprobar el estado de los certificados con la disponibilidad acordada. En el caso del uso de OCSP, se requerirá disponibilidad total. En el caso de publicación de listas de certificados revocados, el frecuencia de publicación de listas vendrá determinada por la política de certificación del tipo de certificado o especificado en el convenio con el prestador. Esto permitirá a Red.es configurar sus caches sin pérdida de información o perjuicio a las aplicaciones confiantes.

6- Los PSCs deberán informar previamente a Red.es de cualquier cambio en las políticas de certificación o en los certificados emitidos por el prestador, ya sean cambios en el formato o en el valor de los campos que suponga una diferencia en la sintaxis y/o semántica del certificado. El aviso se producirá con una antelación de al menos 40 días hábiles a su puesta en producción. El aviso se acompañará con certificados de prueba que permitan probar los cambios en la infraestructura de Red.es. La infraestructura de validación de los certificados de pruebas estará disponible para las pruebas de Red.es con la misma antelación mencionada.

7- Los PSCs deberán informar previamente a Red.es de cualquier cambio en la infraestructura, protocolos, direcciones, transportes soportados por los sistemas de validación. En todo caso deberán mantener operativas las especificaciones previas como soporte de compatibilidad hacia atrás, al menos seis (6) meses tras la notificación a Red.es.