EL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA – SEGURIDAD JURÍDICA EN INTERNET

O SERVIÇO QUALIFICADO - A SEGURANÇA JURÍDICA NA INTERNET

fdo. Pedro J. Canut Zazurca

Ldo. 2980 ReICAZ

RESUMEN

El Prestador de Servicios de Confianza es una figura jurídica, con precedentes en el Prestador de Servicios de Certificación (Unión Europea) y el Trusted Third Party (Estados Unidos), regulada por primera vez por el Reglamento U.E. 910/2014, de 23 de julio, 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.

Palabras clave: servicio cualificado. Internet. La seguridad jurídica.

RESUMO

O provedor de serviços de confiança é um conceito jurídico, com precedentes no Provedor de Serviços de Certificação (UE) e Trusted Third Party (USA), pela primeira vez, regulado pelo Regulamento da UE 910/2014 de 23 de Julho, relativa aos serviços de identificação e confiança eletrônicos para as transações eletrónicas no mercado interno e da Directiva 1999/93 / CE é revogada.

Palavras Chaves: Serviço Qualificado. Internet. Segurança Jurídica.

INDICE

- 7.- Conclusiones

1.- Introducción

Uno de los grandes frenos a la explosión del comercio electrónico es la falta de confianza del consumidor (en las relaciones B2C) y de las empresas (en las relaciones B2B). No en vano todos los días salen a la luz casos de estafas en Internet y de venta de datos personales (sobre todo referidos a grandes multinacionales respecto de las que el nivel de confianza de los usuarios había sido bastante alto).

Las partes interesadas llevan años buscando soluciones a esta falta de confianza con la creación de sellos de confianza respaldados por los Estados (por ejemplo el sello de confianza *online*), la sumisión a códigos de buenas prácticas o el uso cada vez más extendido de certificados de sitio o dominios (ccTLD) país, que nos garantizan, cuando menos, la procedencia de la tienda virtual en la que estamos.

Sin embargo todos estos esfuerzos han topado con la realidad; la realidad en Internet son los navegadores ¿quién no ha accedido a la sede electrónica de su Gobierno, protegida por un certificado de sitio, y se ha encontrado con un aviso de seguridad que desaconseja el acceso? No deja de ser sorprendente que los Estados no tengan la suficiente fuerza frente a los gigantes de Internet como para imponerles la inclusión en los navegadores de los certificados emitidos por prestadores de servicios de certificación con reconocimiento nacional ¿por qué recibo un aviso de seguridad si el sitio al que accedo está cifrado pero el navegador no lo ha incluido entre los certificados válidos y, sin embargo, ese mismo navegador no me pone sobre aviso cuando navego por páginas que no están cifradas (la mayoría).

El último hito, en el marco de la Unión Europea, ha sido la publicación del ***Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio, 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***[1] (más conocido por

1 http://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=0CDAQFjAC&url=http%3A%2F%2Fwww.boe.es%2Fdoue%2F2014%2F257%2FL00073-00114.pdf&ei=EASFVZ7PDMvkUp-ggbgH&usg=AFQjCNGACjfuFAgE0BVCHJi5JYmx414suQ&bvm=bv.96339352,d.d24

sus siglas en inglés: Reglamento eIDAS).

Se ha escogido la figura del Reglamento frente a la Directiva dado que aquel, a diferencia de ésta, es de aplicación directa en todos los Estados Miembros sin necesidad de transposición al Derecho nacional. Esta elección, con ser muy plausible, ya que unifica la normativa sobre firma electrónica y servicios de confianza en los 28 Estados de la U.E. lleva aparejados, no obstante, ciertos desajustes en la normativa interna, como veremos más adelante.

Las principales novedades del Reglamento son que sustituye el criterio actual de comunicación de inicio de actividad en la prestación del servicio por el de autorización previa por parte del organismo de supervisión y establece un régimen único y común para todos los Estados Miembros, imponiendo a éstos la obligación de admitir la identificación/ autenticación mediante cualquier certificado incluido en la Lista de Confianza del resto de Estados.

Sin embargo, opinión muy personal, la gran novedad de este Reglamento es el reconocimiento de los Servicios de Confianza y los Servicios Cualificados de Confianza, además de la regulación de la firma electrónica (para personas físicas) y el sello electrónico (para personas jurídicas). Efectivamente, la ***Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1.999, por la que se establece un marco comunitario para la firma electrónica***[2] se ocupaba exclusivamente de la regulación de la firma electrónica y los prestadores de servicios de certificación basados en certificados reconocidos, en tanto que el Reglamento eIDAS contempla y regula asimismo los servicios de confianza consistentes en la entrega electrónica certificada, la certificación de sitios web, los servicios de sellado de tiempo y los servicios relativos a los documentos electrónicos; servicios éstos que, sin sustento en la Directiva 1999/93/CE, de 13 de diciembre, ni en la legislación nacional (***Ley 59/2003, de 19 de diciembre, de firma electrónica***[3]) ya contaban, en España, con la cobertura del órgano de supervisión que, con una interpretación amplia de la Ley 59/2003, de 19 de diciembre, venía admitiendo las comunicaciones realizadas por prestadores de servicios que se dedicaban a otros servicios relacionados con la firma electrónica pero distintos a la

2 http://www.boe.es/buscar/doc.php?id=DOUE-L-2000-80059
3 http://www.boe.es/buscar/doc.php?id=BOE-A-2003-23399

generación de certificados de firma electrónica reconocida.[4]

La inclusión y - el sometimiento al Reglamento - de estos otros servicios de certificación (ahora denominados servicios de confianza) viene a ordenar el sector distinguiendo aquellas empresas que, con sujeción a las normas ETSI[5], prestan servicios de confianza con todas las garantías técnicas y jurídicas de aquellas otras que – aprovechándose de las lagunas jurídicas existentes hasta la fecha – salían al mercado con productos y servicios de ínfima calidad y nula garantía distorsionando el sector, y perjudicando tanto a las empresas cumplidoras como a los consumidores que, ante la especialidad de los servicios no sabían ni podían distinguir lo bueno de lo malo; entre otras cosas por que la inversión que unos habían realizado en la adquisición de *hardware* certificado y desarrollo conforme a los estándares internacionales (ETSI), otros la destinaban (y siguen destinando) a publicidad y comercialización lo que, a la postre, supone un engaño a los consumidores y, no menos importante, una distorsión del mercado con actuaciones que podrían calificarse de competencia desleal. Todo lo contrario a lo que se espera de un servicio para la sociedad de la información denominado “de Confianza”.

2.- Definición

La definición técnica de prestador de servicios de confianza la extractamos del artículo 3 del Reglamento 910/2014, de 23 de julio:

> *«**prestador de servicios de confianza**, es una persona física o jurídica que presta uno o más servicios de confianza, bien como prestador cualificado o como prestador no cualificado de servicios de confianzas;*
>
> ***prestador cualificado de servicios de confianza**, es un prestador de servicios de confianza que presta uno o varios servicios de confianza cualificados y al que el organismo de supervisión ha concedido la cualificación»*

Lo que nos lleva a preguntarnos qué entiende el Reglamento eIDAS por servicio de confianza y por servicio de confianza cualificado; según la definición del artículo 3:

> *«**servicio de confianza**, es el servicio electrónico prestado habitualmente a cambio de una remuneración, consistente en:*

4 https://sedeaplicaciones2.minetur.gob.es/prestadores/
5 ETSI

> *a) la creación, verificación y validación de firmas electrónicas, sellos electrónicos o sellos de tiempo electrónicos, servicios de entrega electrónica certificada y certificados relativos a estos servicios, o*
>
> *b) la creación, verificación y validación de certificados para la autenticación de sitios web, o*
>
> *c) la preservación de firmas, sellos o certificados electrónicos relativos a estos servicios;*
>
> ***servicio de confianza cualificado**, es un servicio de confianza que cumple con los requisitos aplicables establecidos en el presente reglamento»*

En definitiva, y como avanzábamos en la introducción de este artículo, se amplía el catálogo de servicios de confianza a los sellos de tiempo electrónicos, a los servicios de entrega electrónica certificada, a los servicios de autenticación de sitios web y a la preservación de firmas, sellos y certificados relativos a estos servicios; es decir, a la custodia de los mismos; y, en consecuencia, se considera Prestador de Servicios de Confianza no sólo a aquellas personas físicas o jurídicas que presten servicios de creación, verificación y validación de firmas electrónicas (para las personas físicas) y/o sellos electrónicos (equivalente de la firma electrónica para las personas jurídicas) como ocurría bajo la Directiva 1999/93/CE (que queda derogada por el Reglamento eIDAS), sino también a aquellas otras personas físicas o jurídicas que presten todos o alguno de los servicios de confianza descritos en el artículo 3 del Reglamento.

Merece mención aparte la distinción entre Prestadores de Servicios de Confianza y Prestadores Cualificados de Servicios de Confianza. Los primeros son aquellas personas físicas o jurídicas que prestan todos o alguno de los servicios de confianza arriba enumerados, en tanto que los segundos son aquellos que han merecido la calificación de **cualificados** por parte del organismo de supervisión, previa verificación del cumplimiento de los requisitos establecidos en el Reglamento para los prestadores cualificados de servicios de confianza[6] y

6 *Artículo 24* **Requisitos para los prestadores cualificados de servicios de confianza**

1. Al expedir un certificado cualificado para un servicio de confianza, un prestador cualificado de servicios de confianza verificará, por los medios apropiados y de acuerdo con el Derecho nacional, la identidad y, si procede, cualquier atributo específico de la persona física o jurídica a la que se expide un certificado cualificado.

La información a que se refiere el párrafo primero será verificada por el prestador de servicios de confianza bien directamente o bien por medio de un tercero de conformidad con el Derecho nacional:

a) en presencia de la persona física o de un representante autorizado de la persona jurídica, o

b) a distancia, utilizando medios de identificación electrónica, para los cuales se haya garantizado la presencia de la persona física o de un representante autorizado de la persona jurídica previamente a la expedición del certificado cualificado, y que cumplan los requisitos establecidos con el artículo 8 con respecto a los niveles de seguridad «sustancial» o «alto», o

c) por medio de un certificado de una firma electrónica cualificada o de un sello electrónico cualificado expedido de conformidad con la letra a) o b), o

d) utilizando otros métodos de identificación reconocidos a escala nacional que aporten una seguridad equivalente en términos de fiabilidad a la presencia física. La seguridad equivalente será confirmada por un organismo de evaluación de la conformidad.

2. Los prestadores cualificados de servicios de confianza que prestan servicios de confianza cualificados:

a) informarán al organismo de supervisión de cualquier cambio en la prestación de servicios de confianza cualificados, y de su intención de cesar tales actividades;

b) contarán con personal y, si procede, con subcontratistas, que posean los conocimientos especializados, la fiabilidad, la experiencia y las cualificaciones necesarios y hayan recibido la formación adecuada en materia de seguridad y normas de protección de datos personales y que apliquen procedimientos administrativos y de gestión que correspondan a normas europeas o internacionales;

c) con respecto al riesgo de la responsabilidad por daños y perjuicios de conformidad con el artículo 13, mantendrán recursos financieros suficientes u obtendrán pólizas de seguros de responsabilidad adecuadas, de conformidad con la legislación nacional;

d) antes de entrar en una relación contractual, informarán, de manera clara y comprensible, a cualquier persona que desee utilizar un servicio de confianza cualificado acerca de las condiciones precisas relativas a la utilización de dicho servicio, incluidas las limitaciones de su utilización;

e) utilizarán sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad y la fiabilidad técnicas de los procesos que sustentan;

f) utilizarán sistemas fiables para almacenar los datos que se les faciliten de forma verificable, de modo que:

i) estén a disposición del público para su recuperación solo cuando se haya obtenido el consentimiento de la persona a la que corresponden los datos,

ii) solo personas autorizadas puedan hacer anotaciones y modificaciones en los datos almacenados,

iii) pueda comprobarse la autenticidad de los datos;

g) tomarán medidas adecuadas contra la falsificación y el robo de datos;

h) registrarán y mantendrán accesible durante un período de tiempo apropiado, incluso cuando hayan cesado las actividades del prestador cualificado de servicios de confianza, toda la información pertinente referente a los datos expedidos y recibidos por el prestador cualificado de servicios de confianza, en particular al objeto de que sirvan de prueba en los procedimientos legales y para garantizar la continuidad del servicio. Esta actividad de registro podrá realizarse por medios electrónicos;

i) contarán con un plan de cese actualizado para garantizar la continuidad del servicio, de conformidad con las disposiciones verificadas por el organismo de supervisión con arreglo al artículo 17, apartado 4, letra i);

j) garantizarán un tratamiento lícito de los datos personales de conformidad con la Directiva 95/46/CE;

k) en caso de los prestadores cualificados de servicios de confianza que expidan certificados cualificados, establecerán y mantendrán actualizada una base de datos de certificados.

3. Cuando los prestadores cualificados de servicios de confianza que expidan certificados cualificados decidan revocar un certificado, registrarán su revocación en su base de datos de certificados y publicarán el estado de revocación del certificado oportunamente y, en todo caso, en un plazo de 24 horas después de la recepción de la solicitud. La revocación será efectiva inmediatamente después de su publicación.

4. Con respecto a lo dispuesto en el apartado 3, los prestadores cualificados de servicios de confianza que expidan certificados cualificados proporcionarán a cualquier parte usuaria información sobre el estado de validez o revocación de los certificados cualificados expedidos por ellos. Esta información deberá estar

los servicios de confianza cualificados, y que han presentado un informe de evaluación de la conformidad expedido por un organismo de evaluación de la conformidad.

La distinción es relevante en orden a los efectos jurídicos de un servicio de confianza y un servicio de confianza cualificado prestado por un prestador cualificado; sólo una firma electrónica cualificada tendrá un efecto jurídico equivalente al de una firma manuscrita, aunque a la firma electrónica no cualificada, a tenor de lo dispuesto en párrafo 1 del artículo 25, no se le denegarán efectos jurídicos ni admisibilidad como prueba en juicio. Esta aparente contradicción significa que una firma no cualificada estará sometida al principio de la ***sana crítica*** del juzgador, en tanto que la firma cualificada es equivalente a la firma manuscrita. Asimismo, el artículo 35 del Reglamento dispone que a los sellos electrónicos (para persona jurídica) no se les negarán efectos jurídicos ni admisibilidad de prueba en juicio, aunque solo los sellos electrónicos cualificados disfrutarán de la presunción de integridad y corrección del origen de los datos a los que el sello esté vinculado.

Los diferentes efectos jurídicos que otorga el Reglamento a la firma electrónica cualificada respecto de otro tipo de firmas debemos ponerlo en relación con lo dispuesto en el capítulo III *«IDENTIFICACIÓN ELECTRÓNICA»*, artículo 6 y siguientes del Reglamento.

Tradicionalmente los certificados de firma-e se han venido empleando tanto para prestar el consentimiento (de ahí la equivalencia entre la firma electrónica cualificada y la firma manuscrita) como para identificarse *online* ante determinados organismos o aplicaciones web; y podría pensarse – de una lectura rápida del Reglamento – que ésta, la firma electrónica cualificada continúa siendo la única forma reconocida de identificarse *online*. Pero no es así.

Conforme a la definición de identificación electrónica del artículo 3 (definiciones):

---

disponible al menos por cada certificado en cualquier momento y con posterioridad al período de validez del certificado en una forma automatizada que sea fiable, gratuita y eficiente.

5. La Comisión podrá, mediante actos de ejecución, establecer números de referencia de normas para sistemas y productos fiables que cumplan con los requisitos establecidos las letras e) y f) del apartado 2 del presente artículo. Se presumirá el cumplimiento de los requisitos establecidos en el presente artículo cuando los sistemas y productos fiables cumplan dichas normas. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

«identificación electrónica es el proceso de utilizar los datos de identificación de una persona en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona jurídica; » y a tenor de lo establecido en los artículos 8 existen tres niveles de seguridad **bajo, sustancial y alto**, donde el nivel alto se corresponde con la autenticación a partir de un certificado cualificado de firma electrónica y los niveles bajo y sustancial con otros medios de identificación electrónica que, a tenor del párrafo 3 del artículo 8 del Reglamento quedarán fijados *« a más tardar el 18 de septiembre de 2015»* mediante ***actos de ejecución*** de la Comisión.

Aunque resulta aventurado adelantarse al legislador comunitario podemos imaginar – atendiendo a un análisis empírico de la realidad en los diferentes Estados Miembros – que probablemente, al referirse a identificación electrónica con niveles de identificación bajo y sustancial se está pensando en en soluciones de firma en la nube, claves de un sólo uso (*one time password*) enviadas al correo electrónico y/o al teléfono celular de la persona que vaya a identificarse de manera electrónica, a la firma manuscrita sobre terminales celulares y tabletas o, incluso al tradicional *usuario y contraseña* facilitado mediante determinados protocolos.

Otro tanto ocurre con los efectos jurídicos de los servicios de sellado de tiempo electrónico y entrega electrónica certificada cualificados y no cualificados; así:

a) - No se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a un sello de tiempo electrónico no cualificado, pero sólo los sellos cualificados de tiempo electrónicos disfrutarán de una presunción de exactitud de la fecha y hora que indican y de la integridad de los datos a los que la fecha y hora estén vinculadas (artículo 41).

b) - No se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a a los datos enviados y recibidos mediante un servicio de entrega electrónica certificada no cualificado, pero sólo los datos enviados y recibidos mediante un servicio cualificado gozarán de presunción de integridad (artículo 43).

3.- Diferencias con la figura del Tercero de Confianza (TdC)

Desde su regulación positiva en derecho español vía artículo 25 ***Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico***[7] se ha pretendido su equivalencia con los «***trusted third party»***[8]***;*** sin embargo nada más lejos de la

7 http://www.boe.es/buscar/act.php?id=BOE-A-2002-13758
8 https://en.wikipedia.org/wiki/Trusted_third_party

realidad, a tenor de lo dispuesto en el artículo 24 LSSICE[9].

Los Terceros de Confianza, en derecho español, tienen limitada su actividad al archivo de las declaraciones de voluntad que integran los contratos electrónicos a instancias de todas las partes contratantes (*«las partes podrán pactar»)*, y a consignar la fecha fecha y hora de perfección de los contratos. Sin embargo la fecha y hora consignadas, en el mejor de los casos, tendrá la consideración de mera declaración de tercero; y nunca la presunción (*iuris tantum*) del sello de tiempo electrónico cualificado emitido por un Prestador Cualificado de Servicios de Confianza *«**trust service provider»*** (TSP por sus siglas en inglés).

El Prestador Cualificado de Servicios de Confianza, heredero del Prestador de Servicios de Certificación de la ***Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1.999, por la que se establece un marco comunitario para la firma electrónica*** supera en efectos jurídicos al Tercero de Confianza. En primer lugar por que, a diferencia de éste, el Prestador Cualificado de Servicios de Confianza es una figura regulada, y regulada del mismo modo en los 28 Estados de la Unión Europea, que precisa autorización previa, informe de evaluación de la conformidad y está sometido a auditoría por parte del organismo de supervisión. A diferencia del TdC no tiene límitado su ámbito de actuación a la contratación telemática; sino que extiende sus funciones de garante digital[10] a todo tipo de transacciones sin precisar la concurrencia de voluntades de todas las partes implicadas.

Frente a la inseguridad jurídica que representa la figura del Tercero de Confianza, que no está sujeto a previa autorización ni supervisión de ningún tipo, el Prestador Cualificado de Servicios de Confianza nace con vocación de trasladar al mundo digital la seguridad jurídica y la confianza que supone, en el mundo analógico el notariado latino.

---

9 Artículo 25. Intervención de terceros de confianza.

1. Las partes podrán pactar que un tercero archive las declaraciones de voluntad que integran los contratos electrónicos y que consigne la fecha y la hora en que dichas comunicaciones han tenido lugar. La intervención de dichos terceros no podrá alterar ni sustituir las funciones que corresponde realizar a las personas facultadas con arreglo a Derecho para dar fe pública.

2. El tercero deberá archivar en soporte informático las declaraciones que hubieran tenido lugar por vía telemática entre las partes por el tiempo estipulado que, en ningún caso, será inferior a cinco años.

10 También conocido en muchos ámbitos como notario digital.

4.- Las listas de confianza (TSL)

Las listas de confianza están recogidas en el artículo 22 del Reglamento y consisten en listas elaboradas en cada Estado Miembro con información relativa a los Prestadores Cualificados de Servicios de Confianza y los servicios de confianza cualificados prestados por ellos. Dichas listas deberán ser públicas, renovadas de forma periódica y susceptibles de tratamiento automatizado; de manera que los consumidores de la Unión Europea y todos los Estados Miembros tengan acceso a las mismas.

La existencia, y mantenimiento adecuado, de las listas de confianza tiene gran importancia en lo que respecta al cumplimiento de la obligación de reconocimiento mutuo de certificados cualificados por parte de las administraciones públicas de todos los Estados Miembros, y junto con la ***«trust mark»,*** la etiqueta de confianza *«UE»* para servicios de confianza cualificados, representa una de las mejores herramientas para que los consumidores y usuarios puedan identificar sin lugar a dudas a los Prestadores de Servicios de Confianza de la Unión Europea.

Las listas de confianza de los Estados Miembros de la U.E. pueden consultarse en las siguientes url´s[11]:

Austria

- https://www.signatur.rtr.at/currenttl.xml

Bélgica

- http://tsl.belgium.be/tsl-be.pdf
- http://tsl.belgium.be/tsl-be.xml

Bulgaria

- http://crc.bg/files/_bg/TSL-CRC-BG-signed.pdf

11 A fecha de hoy en España ya es de aplicación la obligación de aceptar los certificados recogidos en todas las listas de confianza europeas.

- http://crc.bg/files/_bg/TSL-CRC-BG-signed.xml

Chipre

- http://www.mcw.gov.cy/mcw/dec/dec.nsf/all/B28C11BBFDBAC045C2257E0D002937E9/$file/TSL-CY-sign.xml

Chequia

- http://tsl.gov.cz/publ/TSL_CZ.pdf
- http://tsl.gov.cz/publ/TSL_CZ.xtsl

Alemania

- http://www.nrca-ds.de/st/TSL-XML.xml

Dinamarca

- http://www.digst.dk/~/media/Files/Loesninger-og-infrastruktur/NemID/HumanReadabletldkxml.pdf
- http://www.digst.dk/~/media/Files/Loesninger-og-infrastruktur/NemID/TLDK.xml

Estonia

- http://sr.riik.ee/tsl/estonian-tsl.pdf
- http://sr.riik.ee/tsl/estonian-tsl.xml

Grecia

- https://www.eett.gr/tsl/EL-TSL.xml

España

- https://sede.minetur.gob.es/Prestadores/TSL/TSL.pdf
- https://sede.minetur.gob.es/Prestadores/TSL/TSL.xml

Finlandia

- https://www.viestintavirasto.fi/attachments/HumanReadable_TSL-Ficora.xml.pdf
- https://www.viestintavirasto.fi/attachments/TSL-Ficora.xml

Francia

- http://references.modernisation.gouv.fr/sites/default/files/TSL-FR_xml.pdf
- http://references.modernisation.gouv.fr/sites/default/files/TSL-FR.xml

Croacia

- http://www.mingo.hr/userdocsimages/trgovina/TSL_HR.xmlhttp://www.mingo.hr/userdocsimages/trgovina/TSL_HR.xml

Hungría

- http://www.nmhh.hu/tl/pub/HU_TL.pdf
- http://www.nmhh.hu/tl/pub/HU_TL.xml

Irlanda

- http://www.dcenr.gov.ie/NR/rdonlyres/A2D966E8-48E1-4709-BFAA-83FA07F3C7F7/0/HumanReadable_signed_tresignedxml.pdf
- http://www.dcenr.gov.ie/NR/rdonlyres/52E803DA-EBB0-4C33-882C-

26FCF550EDB7/0/IrelandTSLSIGNED.xml

Islandia

- http://www.neytendastofa.is/library/Files/TSl/tsl.pdf
- http://www.neytendastofa.is/library/Files/TSl/tsl.xml

Italia

- https://applicazioni.cnipa.gov.it/TSL/IT_TSL_HR.pdf
- https://applicazioni.cnipa.gov.it/TSL/IT_TSL_signed.xml

Liechtenstein

- http://www.llv.li/xml-llv-ak-tsl.xml
- http://www.rrt.lt/failai/LT-TSL.xml

Luxemburgo

- http://www.portail-qualite.public.lu/fr/publications/confiance-numerique/liste-confiance-nationale/tsl-pdf/TSL-PDF.pdf
- http://www.portail-qualite.public.lu/fr/publications/confiance-numerique/liste-confiance-nationale/tsl-xml/TSL-XML.xml

Latvia

- http://www.dvi.gov.lv/en/wp-content/uploads/TSL/tsl-lv-6.pdf
- http://www.dvi.gov.lv/en/wp-content/uploads/TSL/tsl-lv.xml

Malta

- http://www.mca.org.mt/tsl/MT_TSL.xml

Holanda

- https://www.acm.nl/download/bestand/current-tsl.xml

Noruega

- http://www.npt.no/TSL/NO_TSL.pdf
- http://www.npt.no/TSL/NO_TSL.xml

Polonia

- https://www.nccert.pl/tsl/PL_TSL.xml

Portugal

- http://www.gns.gov.pt/media/1891/TSLPTHR.pdf
- http://www.gns.gov.pt/media/1894/TSLPT.xml

Rumanía

- http://www.mcsi.ro/Minister/Domenii-de-activitate-ale-MCSI/Tehnologia-Informatiei/Servicii-electronice/Semnatura-electronica/TrustedList-v8-pdf
- http://www.mcsi.ro/Minister/Domenii-de-activitate-ale-MCSI/Tehnologia-Informatiei/Servicii-electronice/Semnatura-electronica/TrustedList-v8-xml

Suecia

- http://www.pts.se/upload/Ovrigt/Internet/Branschinformation/Trusted-List-SE-

MR.xml

Eslovenia

- http://www.mizks.gov.si/fileadmin/mizks.gov.si/pageuploads/Storitve/Info_druzba/Overitelji/SI-TL.pdf
- http://www.mizks.gov.si/fileadmin/mizks.gov.si/pageuploads/Storitve/Info_druzba/Overitelji/SI_TL.xml

Eslovaquia

- http://ep.nbusr.sk/kca/tsl/tsl_hrf.zip
- http://ep.nbusr.sk/kca/tsl/tsl.xml

Reino Unido

- http://www.tscheme.org/UK_TSL/HR_TSL-UKsigned.pdf
- http://www.tscheme.org/UK_TSL/TSL-UKsigned.xml

5.- Repercusión en España de la publicación del Reglamento eIDAS

Si bien el Reglamento 910/2014, de 23 de julio deroga expresamente la Directiva 1999/93/CE de firma electrónica ello no implica, necesariamente, la derogación total de la Ley 59/2003, de 19 de diciembre de firma electrónica por cuanto, en España, al realizar la transposición de la Directiva de firma electrónica se introdujeron conceptos nuevos que, o bien permanecerán en la Ley 59/2003, de 19 de diciembre, o bien integrarán un nuevo *corpus* jurídico destinado a regular aspectos de la firma electrónica no recogidos en el Reglamento eIDAS que, por otra parte, en algunos aspectos se remite a la legislación nacional de cada Estado Miembro. Cual sea la elección final dependerá de la técnica legislativa escogida por el legislador; si bien, en aras de la seguridad jurídica abogo por mantener la Ley 59/2003, de 19 de diciembre con la derogación de los artículos que se vean afectados por el nuevo Reglamento, en lugar de generar nuevas disposiciones en la materia, que contribuiría a una dispersión normativa poco aconsejable en aras de facilitar la labor a los operadores jurídicos.

6.- ¿hacia un estándar global?

La Unión Europea, partiendo de la figura anglosajona del «***trusted third party***», pero dando un paso más, aborda la regulación positiva de quienes están llamados a ofrecer

servicios de confianza (servicios de certificación en términos de la Directiva 1999/93/CE) al mercado red. Como hemos visto en este breve ensayo de aproximación al Reglamento 910/2014, de 23 de julio la diferencia fundamental con su equivalente anglosajón es la necesidad de autorización previa, dejando a un lado el principio de libre prestación de servicios que se predicaba en la Directiva 2000/31/CE, para poner el acento en la necesidad de, por un lado verificar la adecuación de los servicios prestados a los estándares internacionales (ETSI), y por otro lado, a partir del organismo de supervisión, conservar la prerrogativa de auditoría (cada 24 meses en todos los casos y, a elección del organismo de supervisión, en cualquier momento).

La decisión de establecer cauces de supervisión y auditoría de los Prestadores Cualificados de Servicios de Confianza tiene sin duda su origen en la tradición del derecho romano-germánico que impera en la Unión Europea, y que ha trascendido a los Estados que conforman Iberoamérica, por oposición al *«Common law»*, y como equivalente digital del notariado latino que opera desde hace siglos en los Estados que se rigen por el *«Civil Law»*.

El hecho de que los Estados de Iberoamérica abracen las soluciones propuestas por la vieja Europa en materia de identificación digital y servicios de confianza (del mismo modo que recientemente han abrazado las soluciones jurídicas sobre protección de datos de carácter personal) es una cuestión política respecto de la que poco o nada corresponde decir a quien firma este artículo; si bien, atendido el acervo cultural y jurídico que une a Europa con Iberoamérica entendemos que la solución reglada propuesta por la Unión Europea incardina mejor en el ordenamiento jurídico de los países de tradición latina que las propuestas estadounidenses de libre prestación de servicios, que implican abandonar a los consumidores y usuarios a su suerte, privando a una institución capital para la seguridad jurídica en Internet (autenticación de personas físicas y jurídicas en las transacciones online y servicios de certificación de las comunicaciones) del imprescindible control y supervisión de los organismos reguladores nacionales.

La asunción por parte de los Estados Iberoamericanos del Prestador Cualificado de Servicios de Confianza como garante de las transacciones en redes telemáticas supondría la hegemonía global de una forma de entender la fehaciencia digital equivalente al modelo

analógico ínsito en el ordenamiento jurídico de los Estados Iberoamericanos desde una concepción de las libertades y la seguridad jurídica más cercana y conocida a los operadores jurídicos que la libre prestación de servicios que se propugna desde el neoliberalismo estadounidense.

7.- Conclusiones

PRIMERA.- La figura del ***Trush Services Provider*** (Prestador Cualificado de Servcios de Confianza) regulada en el Reglamento U.E. 910/2014, de 23 de julio es, sin lugar a dudas, la más avanzada a nivel internacional en orden a garantizar la identidad de las personas (físicas y jurídicas) y la certeza de de actos y procesos *online*.

SEGUNDA.- El nuevo marco de reconocimiento mutuo de certificados cualificados y otras formas de identificación distintas de la firma electrónica cualificada abre un campo estratégico para el comercio electrónico y la identificación en línea en la Unión Europea, posibilitando y favoreciendo el mercado único y mejorando la competitividad.

TERCERA.- Sería deseable la extensión a nivel mundial de la figura del Prestador Cualificado de Servicios de Confianza, a partir de los estándares técnicos ETSI, y desde un enfoque jurídico que contemple la creación de organismos de supervisión en todos los Estados a fin de alcanzar un estándar jurídico de garantía de la identificación *online* y la seguridad jurídica en las transacciones internacionales.

En Zaragoza (España), junio 2015

Recebido 02/06/2015
Aprovado 15/06/2015
Publicado 30/06/2015