

29-6-2018

DIVULGACIÓN DE POLÍTICAS DE EMISIÓN DE CERTIFICADOS Y SELLO DE TIEMPO CUALIFICADOS (PKI-TSA-DP)



EADTrust Policy Committee
EADTRUST EUROPEAN AGENCY OF DIGITAL TRUST

Nota sobre derechos de autor

Este documento está protegido por derechos de autor que restringen su uso, copia, distribución y descompilación. No se puede reproducir ninguna parte de este documento de ninguna forma ni por ningún medio sin la autorización previa por escrito de European Agency of Digital Trust (EADTRUST).

Todos los nombres de productos mencionados en este documento son marcas comerciales de sus respectivos propietarios.

Versiones del documento

Esta publicación podría incluir inexactitudes técnicas o errores tipográficos.

Según evoluciona el estado de la técnica y el contexto legislativo, puede ser necesario incluir cambios en este documento, por lo que se recomienda comprobar en la página web de EADTrust S.L. la última versión de la publicación.

European Agency of Digital Trust S.L puede realizar mejoras y cambios en los productos y en los programas descritos en esta publicación en cualquier momento.

CONTENIDO

1. INTRODUCCIÓN	3
2 Información de contacto TSP	4
3 Tipos de certificados, procedimientos de validación y uso	5
4. Límites de los servicios	6
5.- Obligaciones de los suscriptores	7
6.- Obligaciones de los terceros que confían	7
7.-Garantía limitada y descargo de responsabilidad/limitaciones de responsabilidad	8
8.-Acuerdos aplicables y Declaración de políticas y prácticas.....	9
9.- Política de Privacidad y Protección de Datos Personales	9
10.- Política de Reembolso	10
11.- Ley aplicable, quejas y resolución de disputas	10
12.- Licencias y repositorio, marcas confiables y auditoría	11

1. INTRODUCCIÓN

EADTrust European Agency of Digital Trust, S.L. (en adelante, EADTrust), es un Prestador de Servicios Cualificados de Confianza Digital radicado en Madrid, España, que opera bajo la supervisión del Ministerio de Energía, Turismo y Agenda Digital, (en lo adelante MINETAD).

En el ejercicio de su actividad empresarial EADTrust ha definido sus prácticas de emisión de certificados electrónicos y de emisión de sellos de tiempo según los requisitos del REGLAMENTO (UE) No 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 que deroga la Directiva 1999/93/CE (en adelante, eIDAS) y los estándares internacionales establecidos en ETSI.

Estas prácticas también se estructuran y fundamentan en la Declaración de Prácticas de Certificación (DPC), la Política de Certificados (CP, en inglés) RFC 6484 (IETF, 2012), 6844 (IETF, 2013) y los Requisitos Básicos de la Política de Certificado para la Emisión y la Gestión de los Certificados de Confianza Pública (CA/ Browser Forum, 2018).

EADTrust S.L como Autoridad de Sellado de Tiempo (TSA), toma como referencia además, las recomendaciones PKIX RFC 3161 y estándares internacionales establecidos en ETSI.

En lo relacionado con el tratamiento de los datos personales recabados para la ejecución de estos servicios, EADTrust S.L. se rige por lo establecido en el su [CAL-PE-Política de Privacidad y Protección de Datos Personales](#) y el Reglamento (UE) 679/2016 Reglamento General de Protección de Datos Personales (conocido, abreviadamente, como RGPD).

En lo no expresamente derogado, también será de aplicación la Ley Orgánica de Protección de Datos de Carácter Personal (conocida, abreviadamente, como LOPD). La denominación completa de la citada Norma es “Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal”.

En este apartado se recoge la Declaración de Divulgación de Políticas de Emisión de Certificados Electrónicos y Sellado de Tiempo (PKI-TSA-DP) donde se presenta un resumen informativo de las características, requisitos y condiciones generales de los citados servicios.

En la Declaración de Prácticas de Servicios de Confianza, así como en la políticas y prácticas específicas puede accederse a la totalidad de las condiciones, responsabilidades, especificaciones, derechos y obligaciones por los cuales se rigen los servicios de EADTrust.

2 INFORMACIÓN DE CONTACTO TSP

Datos de Contato	European Agency of Digital Trust
Domicilio Social	Calle Alba 15 CP: 28043 Madrid España
Teléfono:	+34. 902. 365. 612
fax	+34. 917. 160. 557
web:	www.eadtrust.eu
mail contacto:	policy@eadtrust.eu

3 TIPOS DE CERTIFICADOS, PROCEDIMIENTOS DE VALIDACIÓN Y USO

EADtrust S.L. ofrece **servicios cualificados de emisión de certificados electrónicos** que consisten en la creación, verificación y validación de certificados cualificados para autenticación y firma electrónica de:

- **Personas físicas**, basados en sus documentos de identidad, tales como el pasaporte, DNI, NIE u otro documento de identificación pertinente, dependiendo del país.
- **Personas físicas que están vinculadas a una persona jurídica** mediante un nombramiento como representante legal o administrador u apoderado, basados en sus documentos de identidad, tales como el pasaporte, DNI, NIE u otro documento de identificación pertinente de la persona física. También se tienen en cuenta los documentos que avalan la identidad u existencia de la persona jurídica y los documentos que acreditan el vínculo de representación con la persona jurídica en cuestión. Estos documentos también se emplean para la emisión de certificados cualificados de autenticación y sello electrónico de **persona jurídica**.
- **Sitios web** de entidades. El certificado emitido por EADTrust permite identificar a la persona jurídica que controla el sitio web en cuestión; toda vez que, el certificado emitido contiene datos sobre su denominación o razón social, dirección e identificación fiscal. También permite identificar la URL y relacionarla con la entidad que ha registrado el dominio, demostrando la vinculación de su clave privada con la clave pública contenida en el certificado y ofreciendo al usuario una garantía razonable de que la comunicación cliente - servidor es segura y previniendo la suplantación y otros fraudes de identidad. Favorece el establecimiento de canales de comunicación cifrados entre el navegador y el sitio web.

De esta manera el suscriptor puede identificarse en el ámbito de su actividad cotidiana de forma segura y confiable, con la vinculación de su clave privada con la respectiva clave pública contenida en el certificado. Además permite garantizar la integridad del documento firmado por el suscriptor y que este no repudie el citado documento con posterioridad, negando su autoridad o la integridad del mismo.

Por otro lado, el **servicio de sellado de tiempo** que ofrece EADTrust S.L se estructura de la manera siguiente:

Su fuente de tiempo se basa en el servicio brindado por el Real Instituto Español y el Observatorio de la Marina, que se encargan de calcular y establecer la hora legal oficial en España (conocida como Tiempo ROA). Se proporciona bajo las directivas y el marco de la "Oficina Internacional Poids et Mesures"; que tiene la función de garantizar la uniformidad de las medidas y su trazabilidad en el sistema de la unidad internacional.

Los tokens de sellado de tiempo se sellan con los certificados EADTrust TSU, emitidos bajo la Cadena de Certificación Roots. La validez de los certificados cualificados orientados al sellado de tiempo se establece en los propios certificados.

- La Política de Sellado de Tiempo se identifica y referencia en ETSI OID 0.4.0.2023.1.1

-El OID del proveedor de servicios de confianza con respecto al servicio de sellado de tiempo es:

TimeStamping: 1.3.6.1.4.1.501.2.2

No calificado: 1.3.6.1.4.1.501.2.2.0

Calificado: 1.3.6.1.4.1.501.2.2.1 Este árbol OID se identifica con el nombre de la plataforma de gestión de identidades SPRITEL (Plataforma Segura para identidades registradas y Trusted Electronic Ledger) base de la Autoridad de Registro de EADTrust.

Para poder usar el servicio, la organización que que desea marcar los documentos debe firmar un acuerdo con el proveedor de servicios de confianza. Dentro de este marco, la entidad usuaria obtendrá suficientes instrucciones y privilegios para autenticarse ante el proveedor del servicio y para enviar datos electrónicamente a la TSA con el fin de crear un sello de tiempo electrónico vinculado a esos datos.

4. LÍMITES DE LOS SERVICIOS

El servicio cualificado de emisión de certificados digitales de EADTrust admite, solamente, el uso del certificado en el ámbito de actividad del SOLICITANTE, de acuerdo con la finalidad establecida en la Declaración de Prácticas de Certificación y en la política específica para este tipo de certificados. Una vez emitido el certificado, el SOLICITANTE no podrá hacer un uso de este con fines comerciales. Se entiende por uso comercial del certificado, cualquier actuación mediante la cual el SOLICITANTE ofrezca a terceras personas, a título oneroso o gratuito, servicios que requieran el uso del certificado de referencia.

El incumplimiento por parte del suscriptor o de las partes que confían facultará a la CA a revocar el certificado y a reclamar la indemnización de los daños y perjuicios que se le hubieren causado por el incumplimiento, incluyendo lucro cesante y daños indirectos.

El servicio de sellado de tiempo tiene las siguientes particularidades:

La precisión declarada para la sincronización de la TSU con UTC es de 1 segundo, cumpliendo así con los requisitos establecidos en la norma europea (ETSI EN 319 421). Por lo tanto, el Servicio de Sellado de Tiempo Cualificado de EADTrust TSA no emitirá ningún sello de tiempo electrónico cualificado, durante el periodo de tiempo en el que existe un desajuste de más de 1 segundo entre los relojes de TSU y la fuente de tiempo UTC del Observatorio Real de la Armada (ROA).

EADTrust TSA registra y archiva los eventos significativos necesarios para verificar la actividad de este servicio de confianza durante un período no inferior a 15 años, de acuerdo con la legislación aplicable.

5.- OBLIGACIONES DE LOS SUSCRIPTORES

Constituyen obligaciones de los suscriptores de los servicios ofrecidos por EADTrust, las siguientes:

Abonar las tarifas por los servicios de certificación digital y sellado de tiempo solicitados en los términos y condiciones previstos por la CA/TSA;

Custodiar el certificado y las claves secretas, incluida la clave privada, passwords o pines de forma diligente, tomando precauciones razonables para evitar su pérdida, revelación, modificación o uso no autorizado;

Suministrar toda la información y documentación exigida, responsabilizándose de su veracidad y corrección;

Notificar inmediatamente a la CA/TSA en caso de que detecte que se ha incluido cualquier información incorrecta o inexacta o en caso de que, de forma sobrevenida, la información del certificado no se corresponda con la realidad;

Autorizar a la CA a que a través de la RA, utilice los datos personales aportados por el SOLICITANTE para validar, comprobar y autenticar la identidad declarada por este;

Informar inmediatamente a la CA/TSA acerca de cualquier situación que pueda afectar la validez del certificado, o a la seguridad de las claves;

Solicitar la modificación/renovación/suspensión/revocación del Certificado cuando se cumpla alguno de los supuestos previstos en las políticas y prácticas específicas y en la legislación vigente para los diferentes status del ciclo de vida de los certificados;

Utilizar el Certificado conforme a la Ley y a los límites de uso definidos en las políticas y prácticas específicas, en las condiciones generales y particulares de uso del certificado suscritas y en el propio Certificado;

Todas las que se deriven de la DPC, la política de certificado y sellado de tiempo específica y de la legislación vigente.

6.- OBLIGACIONES DE LOS TERCEROS QUE CONFÍAN

Constituyen obligaciones de los terceros que confían en un certificado o sello de tiempo generado por EADTrust, las siguientes:

- Verificar la validez de los certificados y su propósito;
- Comprobar por el campo AIA de los certificados que pueden reconstruir la cadena de confianza desde el certificado de entidad final hasta la autoridad Raíz, y que pueden indentificar el punto de consulta de validez de certificados por OCSP, o, cuando corresponda, por CRL;
- Identificar las autoridades incluidas en las listas TSL administradas por la entidad supervisora correspondiente al país, en España el Ministerio de Energía, Turismo y Agenda Digital y por el organismo europeo que consolida las TSL nacionales;

- Conocer y sujetarse a las garantías, límites y responsabilidades aplicables en la aceptación y uso de los certificados en los que confía, y aceptar sujetarse a las mismas;
- Limitar la fiabilidad de los certificados los usos permitidos de los mismos, en conformidad con lo expresado en las extensiones de los certificados y la política específica de certificados de que se trate;
- Notificar cualquier hecho o situación anómala relativa al certificado y que pueda ser considerado como causa de revocación del mismo.
- Asegurar que la confianza en los sellos de tiempo electrónicos emitidos por el Servicio de Sellado de Tiempo Cualificado se restrinja a los usos apropiados (ver la Política y Prácticas del Servicio de Sellado de Tiempo de EADTrust TSA).
- Verificar que el sello de tiempo electrónico este sellado adecuadamente con el certificado utilizado por la TSU.
- Verificar la validez del certificado utilizado por la TSU perteneciente a la Autoridad de Sellado de Tiempo que emite el sello de tiempo electrónico, asegurándose de que no haya expirado.
- Asegurarse de que el certificado no haya sido revocado accediendo a la información sobre el estado de revocación actual, disponible en la dirección especificada en el certificado en si mismo.
- Determinar que el sello de tiempo electrónico proporciona suficientes garantías para el uso previsto.

7.- GARANTÍA LIMITADA Y DESCARGO DE RESPONSABILIDAD/LIMITACIONES DE RESPONSABILIDAD

EADTrust S.L posee mecanismos financieros para garantizar sus servicios y a estos fines ha contratado un seguro de responsabilidad civil que respalda su actividad empresarial. No obstante, EADTrust solo responderá por deficiencias en los procedimientos propios de su actividad como prestador de servicios de confianza y de conformidad con las disposiciones de su Declaración de políticas y las prácticas específicas de emisión de certificados y del servicio de sellado de tiempo cualificado.

En especial, asumirá de conjunto con la RA toda la responsabilidad por la correcta identificación y validación de la identidad declarada por el SOLICITANTE.

En ningún caso será responsable de las acciones o pérdidas en las que incurran los solicitantes del servicio, entidades usuarios, en su caso, terceros involucrados, que no se deba a errores atribuibles a EADTrust en la expedición de los sellos electrónicos de tiempo

La CA y la RA no serán responsables de los daños derivados de o relacionados con la no ejecución o ejecución defectuosa de las obligaciones a cargo del SOLICITANTE, ni de la incorrecta utilización de los certificados y las claves, ni de cualquier daño indirecto que pueda resultar de la utilización del Certificado o de la información suministrada a la CA, en particular, el lucro cesante, la pérdida de ingresos o pedidos o pérdida de datos, no dando lugar a ningún tipo de derecho indemnizatorio.

Tampoco serán responsables del contenido de aquellos documentos firmados o cifrados digitalmente, ni por el correcto funcionamiento con aplicaciones que no estén aprobadas, y por daños generados por la imposibilidad del uso con dichas aplicaciones.

La CA y la RA no serán responsables de las eventuales inexactitudes en el Certificado que resulten de la información facilitada por el SOLICITANTE, a condición de haber actuado siempre con la máxima diligencia exigible.

EADTrust TSA no responderá a las personas cuyo comportamiento en el uso de sellos de tiempo electrónicos haya sido negligente y deberá considerarse a estos fines y, en cualquier caso, como negligencia, incumplimiento de las disposiciones de la Declaración de Política y Prácticas de Servicio Cualificado de Sellado de Tiempo, y en especial, lo dispuesto en las secciones referidas a las obligaciones y responsabilidad de las partes.

Ni asumirá responsabilidad alguna por la no ejecución o el retraso en la ejecución de cualquiera de las obligaciones en virtud de las DPC y las políticas y prácticas específicas para cada tipo de servicio, si tal falta de ejecución o retraso resultara o fuera consecuencia de un supuesto de fuerza mayor, caso fortuito o, en general, cualquier circunstancia sobre la que la AC/TSA no pueda tener un control razonable y entre otros: los desastres naturales, la guerra, el estado de sitio, las alteraciones de orden público, la huelga en los transportes, el corte de suministro eléctrico y/o telefónico, los virus informáticos, deficiencias en los servicios de telecomunicaciones, violaciones de seguridad del sistema de certificación o cualquier perjuicio que se derive de un hecho causado por un avance imprevisible de la técnica.

Cualquiera que sea la causa por la que pudiera reclamarse responsabilidad a la EADTrust S.L, la pretensión indemnizatoria no podrá exceder, salvo en el supuesto de culpa grave o dolo, la cifra prevista en la Póliza de Seguro de EADTrust dependiendo del tipo del hecho acaecido.

En caso de finalización de la actividad del prestador de servicios de confianza; EADTrust S.L se regirá por las disposiciones de la legislación vigente. A estos fines, informará de manera adecuada y con suficiente antelación a los usuarios del servicio con los que tenga el correspondiente contrato de prestación de servicios.

8.- ACUERDOS APLICABLES Y DECLARACIÓN DE POLÍTICAS Y PRÁCTICAS

Los documentos "Declaración de Prácticas de Servicios de Confianza " y las políticas específicas para cada servicios de emisión de certificados y sellado de tiempo, publicados en la dirección www.policy.eadtrust.eu, recogen la información pública de las condiciones y características del servicio cualificado ofrecido por EADTrust.

Las actividades que EADTrust CA/TSA puede subcontratar para llevar a cabo su actividad como autoridad de certificación se desarrollan de acuerdo a su Declaración de Prácticas de Servicios de Confianza Digital (DPC) y los contratos y acuerdos formalizados con las entidades que realizan tales actividades.

9.- POLÍTICA DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES

EADTrust S.L como autoridad de servicios de confianza electrónica adopta las medidas de seguridad técnicas y organizativas necesarias para garantizar la seguridad de los datos personales y evitar su alteración, tratamiento o acceso no autorizado, y

determinará la información que deba ser considerada como confidencial de acuerdo con lo establecido en el Real Decreto 1720/2007, por el que se aprueba el Reglamento de la Ley Orgánica 15/1999, de Protección de Datos Personales y sus normas de desarrollo.

También cumple lo dispuesto en el Reglamento (UE) 2016/679 sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de dichos datos.

LA CA y RA verificarán que el SOLICITANTE de un certificado es informado y presta su consentimiento al tratamiento de sus datos de carácter personal, la finalidad de su uso por la CA y la RA para la ejecución del servicio.

EADTrust CA/TSA devolverá o destruirá todos los datos personales sujetos a tratamiento una vez que la relación con la parte contratante llegue a su fin. Como excepción, EADTrust custodiará cualquier dato personal que esté obligado por ley en virtud de una disposición general de quince (15) años.

Los datos personales en custodia de EADTrust, obtenidos en el marco de la prestación de este y otros servicios, se consideran de carácter personal a efectos de lo previsto en el Reglamento (UE) 679/2016 y demás normativa complementaria; en consecuencia, no se permite su acceso por parte de terceros.

10.- POLÍTICA DE REEMBOLSO

EADTrust S.L no ha definido una política específica de reembolso y en este sentido se acoge a lo establecido en la legislación vigente.

11.- LEY APLICABLE, QUEJAS Y RESOLUCIÓN DE DISPUTAS

Las operaciones y funcionamiento de la PKI de EADTrust y su actuación como TSA, así como las políticas específicas aplicables a cada tipo de certificado, estarán sujetas a la normativa que les sea aplicable, en especial las siguientes:

- Reglamento (UE) 910/2014 eIDAS 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 .
- Reglamento (UE) 2016/679 sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de dichos datos.
- Directiva 1999/93/CE, del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal. Por otro lado, cualquier litigio, discrepancia, pregunta o reclamación, relacionadas directa o indirectamente, con la ejecución o interpretación de las políticas y prácticas específicas y/o la Declaración de

Prácticas de Servicios de Confianza, se resolverán de acuerdo con lo establecido en los contratos correspondientes, condiciones generales y/o particulares o acuerdos específicos pactados, en consonancia con lo establecido en las citadas normas jurídicas.

En el caso de que los contratos, condiciones generales y/o particulares o acuerdos, no especifiquen los mecanismos de resolución de diferencias, todas las partes estarán sujetas a la jurisdicción exclusiva de los tribunales españoles de la ciudad de Madrid.

Sin perjuicio de lo previsto en el párrafo anterior, las partes podrán acordar la utilización de medios alternativos de solución de diferencias, concretamente arbitraje, cuando las circunstancias así lo ameriten. El proceso de arbitraje se llevará a cabo el marco de la Corte Española de Arbitraje, de conformidad con su Reglamento y Estatuto, a la que se encomienda la administración del arbitraje y la designación del árbitro o tribunal arbitral. Las partes harán constar su compromiso de cumplir el laudo que se dicte.

12.- LICENCIAS Y REPOSITORIO, MARCAS CONFIABLES Y AUDITORÍA

EADTrust ha superado anualmente desde 2009 diversas auditorías de su **Sistema Integrado de Gestión** con respecto a varias normas. En estos momentos, EADTrust está certificado respecto a las normativas UNE EN ISO 9001:2015; UNE ISO/IEC 27001:2014; UNE ISO/IEC 200001:2011, a través de la entidad **LRQA Business Assurance**, con el siguiente alcance:

El Sistema Integrado de Gestión de la Información que da soporte a consultoría, auditoría, desarrollo y provisión de los siguientes servicios electrónicos de confianza: Autoridades de Certificación (PKI) que cumplen los requerimientos de las normas EN 319 401 v2.1.1, EN 319 411-1 v1.1.1, EN 319 411-2 v2.1.1, EN 319 421 v1.1.1 para Sellado de Tiempo, Emisión de Certificados, Validación de OCSP, Firma Electrónica Centralizada, Extensión de Firma Electrónica, Notificación Electrónica Fehaciente (Correo Electrónico Certificado), Publicación Electrónica Fehaciente, Comprobación fehaciente de contenidos digitales, Foro Electrónico de Accionistas, Emisión y Gestión de Claves, Cartulario (Custodia Digital de Documentos Electrónicos), Custodia de Evidencias Electrónicas (Retención de Datos), Voto Electrónico, Facturación Electrónica, Digitalización Certificada, Gestión de firma manuscrita digitalizada y Gestión de firma avanzada vocal, para garantizar la validez legal de todo tipo de gestiones que las utilizan, de acuerdo a la declaración de aplicabilidad vigente. Estos son los certificados:

Norma	Certificado
ISO 20000-1:2011	SGI 6015629/114
ISO 27001:2013	SGI 6015629/19
ISO 9001:2015	SGI 6015629/11

EADTRUST ha superado una auditoría de tipo “Penetration testing” para verificar la resistencia de su infraestructura a diversos ataques de seguridad potenciales.

EADTRUST se somete con la periodicidad indicada en el Reglamento UE 910/2014 eIDAS a auditorías de cumplimiento de los requisitos relativos a los prestadores de servicios de electrónicos de confianza cualificados en base a los estándares internacionales previstos en ETSI.