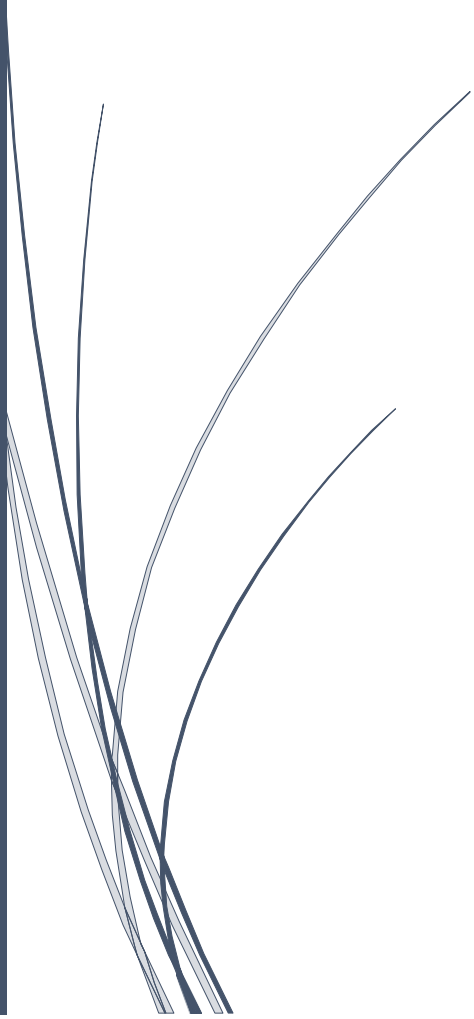
09-10-2019

Declaración de Divulgación de Políticas (PDS)

Servicios y Certificados



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 la última versión de la publicación.

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

Certificación ISO 9001. ISO 27001 e ISO 20000-1

EADTrust ha superado diversas auditorías, y, en particular las relativas a las normas ISO 9001. ISO 27001 e ISO 20000-1, 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 v2.2.1, EN 319 411-1 v1.2.2, EN 319 411-2 v2.2.2, 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.

Certificados

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

ISO 9001 ISO/IEC 20000-1 ISO/IEC 27001 001

Tabla de contenidos

Control documental

Esta sección refleja la información del documento, sus propiedades y el historial de versiones.

TABLA1. HISTORIAL DE VERSIONES.

Versión	Fecha	Documentos sustituidos	Descripción
1.0	09/10/19	Ninguno	Declaración de divulgación de políticas de emisión de certificados cualificados conforme al Reglamento (UE) 910/2014 eIDAS.

TABLA2. HISTORIAL DE VERSIONES.

Propiedades del documento.	
Propietario	EADTrust European Agency of Digital Trust, S.L.
Fecha	09 de octubre de 2019
Distribución	Público
Nombre / Código	OPR-PG- V1.0-PKI_Disclosure_Statement_PDS_EADTrust

1.- Introducción

EADTrust es un Prestador de Servicios de Confianza Digital radicado en Madrid, España, que opera bajo la supervisión del Ministerio de Economía y Empresa (Secretaría de Estado para el Avance Digital), si bien la denominación del organismo puede cambiar por criterios políticos e incluso adscribirse a diferente Ministerio.

Presta servicios de confianza digital cualificados (definidos en el 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 EN 319 401, ETSI EN 319 411-1 y 2; ETSI EN 319 412-1 al 5, ETSI EN 319 421, ETSI EN 319 422 y sus actualizaciones.

Estas prácticas también se estructuran y fundamentan en la Declaración de Prácticas de Servicios Electrónicos de Confianza (DPC) de la empresa; considerando además las recomendaciones técnicas siguientes: Política de certificados y marco de prácticas de certificación RFC3647, Política de Certificados (CP, en inglés) RFC6484 (IETF, 2012), RFC 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 Fórum, 2019).

En relación con la expedición de certificados para sitios web, además de cumplir con la normativa técnica y jurídica desarrollada en el marco del Reglamento eIDAS; EADTrust cumple los requisitos denominados “Baseline Requirements” para la emisión y la gestión de certificados confiables publicados por la entidad CAB fórum y disponibles en su sitio web: http://www.cabforum.org.

Igualmente, cumplirá los requisitos denominados “Guidelines For The Issuance And Management Of Extended Validation Certificates” para la emisión de dicho tipo de certificados. La versión disponible en la última revisión de esta PDS es la 1.6.9. Además de lo indicado en dicha versión, se han tenido en cuenta los resultados de la aprobación del Ballot SC 17 en relación con la codificación del campo **organizationIdentifier** para incluir datos identificativos específicos necesario para el cumplimiento de la normativa PSD2.

Cuando los certificados se expidan a empleados públicos o a personas o entidades que por su relación con las administraciones públicas deban hacer constar determinados datos en los certificados, se tendrán en cuenta las normas que les afecten.

Las normas ya identificadas que afectan a los perfiles de los certificados son:

- Perfil de certificados 2.0[1] en el marco de la Leyes españolas 39/2015 y 40/2015. Incluye el perfil de certificado de representante.
- Perfil de certificados del ámbito judicial aprobado por el CTEAE en el marco de la Ley 18/2011 española.

EADTrust también ofrece servicios de confianza digital no cualificados (basados en otros enfoques de uso de la criptografía y de la gestión de evidencias digitales). La indicación de servicios “no cualificados” simplemente identifica los servicios de confianza no previstos en el citado Reglamento eIDAS y no indica una menor calidad en el diseño del servicio o su prestación.

EADTrust, como CA, emite algunos certificados directamente. Sin embargo, como empresa orientada a servicios, el mercado de certificados se alcanza generalmente a través de sus Autoridades de Registro.

Como tal, hay dos formas principales que la RA puede adoptar en la estructura de EADTrust respecto a la verificación de identidad de los solicitantes: inscripción en persona con personación ante una agente de RA e inscripción mediante videoconferencia (también descrita como telepresencia) o videograbación verificada. La plataforma que se está proyectando emplear, cumplirá con la normativa española publicada por el Servicio de Prevención de Blanqueo de

[1] https://administracionelectronica.gob.es/pae_Home/dam/jcr:474ae40a-fe06-45fa-aa8f-113049e9c889/2016_Perfiles_de_certificados_1-ed.pdf

Capitales (SEPBLAC) para video identificación[2] y videoconferencia[3] y con la Directiva (UE) 2015/2366 (PSD 2), que se utilizará incluso en los servicios de iniciación de pagos como medio para proporcionar autenticación fuerte de los clientes.

EADTrust S.L. como Autoridad de Sellado de Tiempo (TSA), toma como referencia además, ETSI EN 319 422 V1.1.1 (2016-03) - Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time- stamp token profiles; IETF RFC 3161: Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP); IETF RFC 3628: Policy Requirements for Time-Stamping Authorities (TSAs); XML Timestamping Profile of the OASIS Digital Signature Services Version 1.0. OASIS Standard. 11 April 2007

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 Reglamento (UE) 679/2016 Reglamento General de Protección de Datos Personales (conocido, abreviadamente, como RGPD); la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (conocida, abreviadamente, como LOPD GDD).

También se toma en consideración la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (abreviadamente LSSI o LSSI-CE). Para más información sobre el tratamiento de datos personales que lleva a cabo la organización puede consultarse el siguiente enlace: http://eadtrust.rgpd.de/

En este apartado se recoge la PKI Disclosure Statement (PDS) de EADTrust donde se presenta un resumen informativo de las características, requisitos y condiciones generales de los citados servicios.

En la Declaración de Prácticas de Servicios Electrónicos 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 del Prestador

Nombre del PSC	**European Agency of digital Trust, S. L.**
Domicilio social	C/ Alba,15, 28043 Madrid - Spain
Dirección de email para consultas sobre los servicios	info@eadtrust.eu
Dirección email para políticas	policy@eadtrust.eu
Dirección de email para PSD2	CA-request@eadtrust.eu
Página web	www.eadtrust.eu
Teléfonos	(+34) 902365612 / (+34) 917160555

Contacto solicitud revocación certificados: Personación en la sede del PCS o de una RA de EADTrust/solicitud vía telefónica. El formulario y procedimiento de solicitud de revocación está disponible en: www.eadtrust.eu.

[2] http://www.sepblac.es/espanol/sujetos_obligados/Autorizacion_video_identificacion_11052017.pdf

[3] http://www.sepblac.es/espanol/sujetos_obligados/autorizacion_identificacion_mediante_videoconferencia.pdf

3.- Tipos de certificados, procedimientos de validación y uso

Las especificidades para cada tipo de certificado emitido por EADTrust están reguladas en la Declaración de Practicas de Certificación (DPC) y en las políticas específicas.

Tipo	Certificado	Policy Identifier	Policy OID	Formato	Nivel de seguridad
Persona física	Individuo	0.4.0.194112.1.0 (QCP-n)	1.3.6.1.4.1.501.2.1.1.0.41221 1.3.6.1.4.1.501.2.1.1.1.41221 0.4.0.194112.1.2	Dispositivo Software HSM/Secure token	Alto Sustancial Alto
	Representante	0.4.0.194112.1.0 (QCP-n) 2.16.724.1.3.5.8 (OID MPR)	1.3.6.1.4.1.501.2.1.1.0.41222 1.3.6.1.4.1.501.2.1.1.1.41222 0.4.0.194112.1.2	Dispositivo Software HSM/Secure token	Alto Sustancial Alto
	Empleado Público[4]	0.4.0.194112.1.0 (ETSI QCP-n) 2.16.724.1.3.5.7.2	1.3.6.1.4.1.501.2.1.1.0.41223 1.3.6.1.4.1.501.2.1.1.1.41223 0.4.0.194112.1.2	Dispositivo Software HSM/Secure token	Alto Sustancial Alto
	Empleado público (Seudónimo/Firma)	0.4.0.194112.1.2 (ETSI QCP-n-qscd) 2.16.724.1.3.5.4.1	1.3.6.1.4.1.501.2.1.1.1.41224	Dispositivo Software HSM/Secure token	Alto Sustancial Alto
	Empleado público (Seudónimo/ Autenticación)[5]	0.4.0.194112.1.2 (ETSI QCP-n-qscd) 2.16.724.1.3.5.4.1	1.3.6.1.4.1.501.2.1.1.1.41225	Dispositivo Software HSM/Secure token	Alto Sustancial Alto
Entidad legal	Sello corporativo	4.0.194112.1.1 (OID ETSI QCP-l)	1.3.6.1.4.1.501.2.1.1.0.421 1.3.6.1.4.1.501.2.1.1.1.421 0.4.0.194112.1.3	HSM/Secure token Browser HSM	Alto Sustancial Alto
	Sello Corporativo		1.3.6.1.4.1.501.2.1.1.0.3161	HSM/Secure token Browser HSM	No cualificado
	Sello Corporativo	0.4.0.194112.1.1 (OID ETSI QCP-l)	1.3.6.1.4.1.501.2.1.1.0.41231 1.3.6.1.4.1.501.2.1.1.1.41231 0.4.0.194112.1.3	HSM/Secure token Browser HSM	Alto Sustancial Alto
Entidad legal PSD2	Sello Corporativo	0.4.0.194112.1.1 (OID ETSI QCP-l)	1.3.6.1.4.1.501.2.1.1.0.41232 1.3.6.1.4.1.501.2.1.1.1.41232 0.4.0.194112.1.3	HSM/Secure token Browser HSM	Alto Sustancial Alto
Autenticación de sitio web	SSL DV	0.4.0.194112.1.4 (ETSI QCP-w)	1.3.6.1.4.1.501.2.1.1.0.41241	Software	Sustancial

[4] Se podrán emitir certificados con otros niveles de aseguramiento para empleado público en el futuro, siguiendo las directrices definidas en el documento "Perfiles de Certificados Electrónicos de la administración pública" que define los perfiles de certificados derivados de la aplicación del Real Decreto 1671/2009 y está adaptado a las disposiciones de la Ley 39/2015 de 1 de Octubre, de Procedimiento Administrativo Común de las Administraciones Públicas, la Ley 40/2015 de 1 de Octubre, de Régimen Jurídico del Sector Publico (LRJ) y al Reglamento (UE) 910/2014.

[5] Se podrán emitir certificados con otros niveles de aseguramiento para empleado público con seudónimo en el futuro, siguiendo las directrices definidas en el documento Perfiles de Certificados Electrónicos de la administración pública que define los perfiles de certificados derivados del Real Decreto 1671/2009 y está adaptado a las disposiciones de la Ley 39/2015 de 1 de Octubre, de Procedimiento Administrativo Común de las Administraciones Públicas, la Ley40/2015 de 1 de Octubre, de Régimen Jurídico del Sector Publico (LRJ) y al Reglamento (UE) 910/2014.

Autenticación de sitio web		2.23.140.1.2.1 (CAB/FORUM DV)			
	SSL OV	0.4.0.194112.1.4 (ETSI QCP-w) 2.23.140.1.2.2 (CAB/FORUM OV)	1.3.6.1.4.1.501.2.1.1.0.41242	Software	Sustancial
	SSL EV	0.4.0.194112.1.4 (ETSI QCP-w) 2.23.140.1.1 (CAB/FORUM EV)	1.3.6.1.4.1.501.2.1.1.0.41244	Software	Sustancial
	SSL PSD2	0.4.0.194112.1.4 (ETSI QCP-w) 2.23.140.1.1 (CAB/FORUM EV)	1.3.6.1.4.1.501.2.1.1.0.41243	Software	Sustancial

3.1.- Identificación de políticas de sello de tiempo

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 cualificado: 1.3.6.1.4.1.501.2.2.0

Cualificado: 1.3.6.1.4.1.501.2.2.1

4.- Límites de los Servicios

Los servicios electrónicos de confianza de emisión de certificados de EADTrust, admiten solamente el uso del certificado en el ámbito de actividad del SOLICITANTE, de acuerdo con la finalidad establecida en la Declaración de Prácticas de Servicios Electrónicos de Confianza y en la política específica para cada 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 período 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).

El período de conservación para cualquier documentación es de 15 años, excepto en aquellos casos en los que se especifique un período de conservación más corto en la política del certificado.

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, en particular en el procedimiento de solicitud de certificado, 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.
- Comprender y aceptar los términos y condiciones de uso del certificado, y cualquier modificación que se realice a estos
- Garantizar el uso adecuado y la conservación de los soportes en que se entregan los certificados
- No comprometer intencionalmente la seguridad de los servicios de certificación
- No monitorear, manipular o realizar ingeniería inversa en la implementación técnica de los servicios de certificación

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 identificar 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 sí mismo.
- Determinar que el sello de tiempo electrónico proporciona suficientes garantías para el uso previsto.
- No comprometer intencionalmente la seguridad de los servicios de certificación
- No monitorear, manipular o realizar ingeniería inversa en la implementación técnica de los servicios de certificación
- El usuario de certificado cualificado debe reconocer, en el debido instrumento legal, que dichas firmas electrónicas son firmas electrónicas equivalentes a las firmas manuscritas, según eIDAS.

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 usuarias, 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 electrónico 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 Electrónicos de Confianza " y las políticas específicas para cada servicio 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 Electrónicos de Confianza (DPC) y los contratos y acuerdos formalizados con las entidades que realizan tales actividades.

9.- Política de Privacidad y Protección de Datos Personales

INFORMACION BÁSICA SOBRE PROTECCION DE DATOS	
Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos	
Responsable del tratamiento	EAD TRUST, EUROPEAN AGENCY OF DIGITAL TRUST SL. C/ Alba 15 28043 – Madrid España. CP: 28043
Finalidad	Gestionar servicios de emisión de certificados electrónicos
Legitimación	Este tratamiento de datos tiene como base jurídica el artículo 6.1 b) del Reglamento General de Protección de Datos: **ejecución de un contrato**.

Período de Conservación	Podrán conservarse durante un plazo mínimo de **15 años,** tal y como establece el artículo 20 letra f) de la **Ley 59/2003, de 19 de diciembre, de firma electrónica** y el Reglamento (UE) eIDAS, Artículos 34 y 40 respectivamente.
Destinatarios	No se cederán datos a terceros, salvo obligación legal.
Derechos	Acceder, rectificar y suprimir los datos, así como el resto de derechos recogidos en la normativa de protección de datos.
Puede consultar la totalidad de la Política de Privacidad de EAD TRUST en http://eadtrust.rgpd.de/	

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.

- Decisión de Ejecución (UE) 2015/296 de la Comisión de 24 de febrero de 2015. Por la que se establecen las modalidades de procedimiento para la cooperación entre los Estados miembros en materia de identificación electrónica con arreglo al artículo 12, apartado 7, del Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

- Reglamento de Ejecución (UE) 2015/806 de la Comisión de 22 de mayo de 2015. Por el que se establecen especificaciones relativas a la forma de la etiqueta de confianza «UE» para servicios de confianza cualificados.

- Reglamento de Ejecución (UE) 2015/1501 de la Comisión de 8 de septiembre de 2015. Sobre el marco de interoperabilidad de conformidad con el artículo 12, apartado 8, del Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

- Reglamento de Ejecución (UE) 2015/1502 de la Comisión de 8 de septiembre de 2015. Sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica con arreglo a lo dispuesto en el artículo 8, apartado 3.

- Decisión de Ejecución (UE) 2015/1506 de la Comisión de 8 de septiembre de 2015. Por la que se establecen las especificaciones relativas a los formatos de las firmas electrónicas avanzadas y los sellos avanzados que deben reconocer los organismos del sector público de conformidad con los artículos 27, apartado 5, y 37, apartado 5, del Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

- Decisión de Ejecución (UE) 2015/1984 de la Comisión, de 3 de noviembre de 2015. Por la que se definen las circunstancias, formatos y procedimientos de notificación con arreglo al artículo 9, apartado 5, del Reglamento

(UE) N.º 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior [notificada con el número C(2015) 7369].

- Decisión de Ejecución (UE) 2016/650 de la Comisión, de 25 de abril de 2016. Por la que se fijan las normas para la evaluación de la seguridad de los dispositivos cualificados de creación de firmas y sellos con arreglo al artículo 30, apartado 3, y al artículo 39, apartado 2, del Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

- Ley 59/2003, de 19 de diciembre, de Firma Electrónica en lo que no contravenga a lo establecido en el Reglamento No. 910/2014 (eIDAS).

- Ley Orgánica 03/2018, de 05 de diciembre, de Protección de Datos y Garantía de Derechos Digitales.

Cuando los certificados se expidan a empleados públicos o a personas o entidades que por su relación con las administraciones públicas deban hacer constar determinados datos en los certificados, se tendrán en cuenta las normas que les afecten.

Las normas ya identificadas que afectan a los perfiles de los certificados son:

- Perfil de certificados 2.0[6] en el marco de la Leyes españolas 39/2015 y 40/2015. Incluye el perfil de certificado de representante.
- Perfil de certificados del ámbito judicial aprobado por el CTEAE en el marco de la Ley 18/2011 española.

En relación con la expedición de certificados para sitios web, además de cumplir con la normativa técnica y jurídica desarrollada en el marco del Reglamento eIDAS, EADTrust cumple los requisitos denominados “Baseline Requirements” para la emisión y la gestión de certificados confiables publicados por la entidad CA/B fórum y disponibles en su sitio web: http://www.cabforum.org

Además, cumplirá los requisitos denominados “Guidelines For The Issuance And Management Of Extended Validation Certificates” para la emisión de dicho tipo de certificados. La versión disponible en la última revisión de esta DPC es la 1.6.9. Además de lo indicado en dicha versión, se han tenido en cuenta los resultados de la aprobación del Ballot SC 17 en relación con la codificación del campo **organizationIdentifier** para incluir datos identificativos específicos necesario para el cumplimiento de la normativa PSD2.

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.

[6] https://administracionelectronica.gob.es/pae_Home/dam/jcr:474ae40a-fe06-45fa-aa8f-113049e9c889/2016_Perfiles_de_certificados_1-ed.pdf

12.- Licencias y repositorio, marcas confiables y auditoría

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.

Para certificados de servidor seguro que siguen las Políticas de certificados de validación extendida (EVCP), certificados de servidor seguro que siguen la Política de certificados de validación organizativa (OVCP) y certificados de servidor seguro que siguen la Política de certificados de validación de dominios (DVCP), las guías aprobadas por la CA/B Fórum.