European Agency of Digital Trust

Política de emisión de certificados de servidor web

Área Documental de Operaciones

Certificado	OID
Certificado cualificado de sitio web “Domain Validated” (QWAC)	1.3.6.1.4.1.501.2.1.1.0.41241
Certificado cualificado de sitio web “Organization Validated” (QWAC)	1.3.6.1.4.1.501.2.1.1.0.41242
Certificado cualificado de sitio web “Extended Validation” (QWAC)	1.3.6.1.4.1.501.2.1.1.0.41244
Certificado cualificado de sitio web “Organization Validated” para sede electrónica (QWAC) - Nivel de aseguramiento medio/sustancial	1.3.6.1.4.1.501.2.1.1.0.41245
Certificado cualificado de sitio web “Extended Validation” para sede electrónica (QWAC) - Nivel de aseguramiento alto	1.3.6.1.4.1.501.2.1.1.0.41246

Octubre: 2020
Versión 3.0

EADTrust Policy Committee
EADTRUST EUROPEAN AGENCY OF DIGITAL TRUST

Nota sobre derechos de autor

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	10242586 / 10242587
ISO 27001:2013	10242584 / 10242585
ISO 9001:2015	10242588 / 10242589

Tabla de Contenidos

1.- Introducción 8
1.1.- Definición 8
1.2.- Soporte y nivel de seguridad 9
2.- Participantes en la PKI 10
2.1.- Autoridades de Certificación 10
2.2.- Autoridades de Registro 10
2.3.- Suscriptores (titulares de certificado) 11
3.- Soporte y nivel de seguridad ..... **¡Error! Marcador no definido.**
4.- Uso del certificado 13
4.1.- Usos Adecuados del Certificado 13
4.2.- Usos Prohibidos del Certificado 13
5.- Administración de Políticas 13
5.1.- Organización que Administra el Documento 13
5.2.- Contacto 13
5.3.- Procedimiento de aprobación de las políticas de certificados 13
6.- Publicación de información y repositorio de certificados 14
6.1.- Publicación de la información de certificación 14
6.2.- Tiempo o Frecuencia de Publicación 15
6.3.- Repositorios 15
6.4.- Nombre 15
6.4.1.- Tipos de Nombres 15
6.5.- Identificación y validación de la identidad 16
6.5.1.- Método para probar la posesión de la clave privada 16
6.5.2.- Autenticación de la organización e identidad del dominio 16
6.6.- Identificación y autenticación para la solicitud de revocación 16
7.- Requisitos Operacionales del Ciclo de Vida de los Certificados 17
7.1.- Solicitud del Certificado 17
7.1.1.- Quién puede enviar una solicitud del certificado 17
7.1.2.- Proceso de inscripción y responsabilidades 18
7.2.- Procedimiento de Solicitud del Certificado 18
7.2.1.- Realización de funciones de identificación y autenticación 18
7.2.2.- Aprobación o Rechazo de Solicitudes de Certificado 18
7.2.3.- Tiempo para procesar las solicitudes de certificado 19
7.3.- Emisión del Certificado 19
7.3.1.- Acciones de la CA durante la emisión del certificado 19
7.3.2.- Notificación al suscriptor sobre la emisión del certificado por la CA 19
7.4.- Aceptación del Certificado 20
7.4.1.- Conducta que constituye la aceptación del certificado 20
7.4.2.- Publicación del certificado por la CA 20
7.4.3.- Notificación de la emisión del certificado por la CA a otras entidades 20

7.5.- Par de Claves y Uso del Certificado 20
7.5.1.- Clave privada del suscriptor y uso del certificado 20
7.5.2.- Uso de la clave pública por la parte que confía y uso del certificado 21
7.6.- Renovación del Certificado 22
7.6.1.- Circunstancias para la renovación del certificado 22
7.6.2.- Quién puede solicitar la renovación 22
7.6.3.- Procesamiento de solicitudes de renovación de certificados 22
7.6.4.- Notificación de una nueva emisión de certificado al suscriptor 22
7.6.5.- Conducta que constituye la aceptación de un certificado de renovación 22
7.6.6.- Publicación del certificado de renovación por la CA 22
7.6.7.- Notificación de la emisión del certificado por la CA a otras entidades 22
7.7.- Modificación del certificado 22
7.7.1.- Circunstancias para la modificación del certificado 22
7.7.2.- Quién puede solicitar la modificación del certificado 22
7.7.3.- Procesamiento de las solicitudes de modificación del certificado 23
7.7.4.- Notificación de la emisión de un nuevo certificado al suscriptor 23
7.7.5.- Conducta que constituye la aceptación de un certificado modificado 23
7.7.6.- Publicación del certificado modificado por la CA 23
7.7.7.- Notificación de la emisión del certificado por la CA a otras entidades 23
7.8.- Revocación y del certificado 23
7.8.1.- Circunstancias para la revocación 23
7.8.2.- Quién puede solicitar la revocación 24
7.8.3.- Procedimiento para la solicitud de revocación 24
7.8.4.- Periodo de gracia para comprobar certificados revocados 24
7.8.5.- Tiempo en el que una CA debe procesar la solicitud de revocación 25
7.8.6.- Requisitos de comprobación de revocación para las partes que confían 25
7.8.7.- Frecuencia de emisión de la CRL 25
7.8.8.- Actualización de las CRLs 25
7.8.9.- Servicios de estado de certificado 25
7.8.10.- Recuperación de Certificados 26
8.- Perfiles de Certificado 26
8.1.1.- Extensiones de certificado 26
8.2.- Perfiles de Certificados de Entidad Final 26
8.2.1.- Perfil de certificado cualificado de web “Domain Validated” (QWAC) 26
8.2.2.- Perfil de certificado cualificado de web “Organization Validated” (QWAC) 27
8.2.3.-Perfil de certificado cualificado de web “Extended Validation” (QWAC) 28
8.2.5.- Perfil de certificado cualificado de sede electrónica administrativa “Organization Validated” (QWAC) con nivel de aseguramiento medio/sustancial 29
8.2.4.- Perfil de certificado cualificado de sede electrónica administrativa “Extended Validation” (QWAC) con nivel de aseguramiento Alto 30
9.- Requisitos Empresariales y Legales 32
9.1.- Tarifas 32

9.2.- Consideraciones de protección de datos de carácter personal 32
9.2.1.- Consentimiento para usar datos de carácter personal 33
9.2.2.- Comunicación a terceros de datos de carácter personal 33
9.3.- Responsabilidad contractual y extracontractual 33
9.3.1.- Limitación de responsabilidad 33
9.3.2.- Responsabilidades 34
9.3.3.- Entidad de registro 34
9.3.4.- Responsabilidades del titular de los certificados 34
9.3.5.- Exención de responsabilidades de EADTrust 35
9.3.6.- Perjuicios derivados del uso de servicios y certificados 35
9.3.7.- Seguro de responsabilidad civil 35
9.3.8.- Quejas. Reclamaciones y jurisdicción 35

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	25/11/19	Ninguno	Inicio en la prestación del servicio de emisión de certificados cualificados conforme al Reglamento (UE) 910/2014 eIDAS.
2.0	22/04/2020	1.0	Revisión y actualización de la política como parte del proceso de mejora continua e introducción de la videoconferencia como medio de identificación ante la RA.
3.0	28/10/2020	2.0	Se introducen los perfiles de certificado de sello de órgano alineados con el documento “Perfiles de Certificados Electrónicos 2.0” de las AAPP.

TABLA2. DATOS DEL DOCUMENTO.

Propiedades del documento.	
Propietario	EADTrust European Agency of Digital Trust, S.L.
Fecha	28 de octubre de 2020
Distribución	Público
Nombre / Código	OPR-PC- V3.0-Emisión_certificados_Web_EADTrust

1.- Introducción

Este documento establece la Política de certificación que **EADTrust European Agency of Digital Trust, S.L.** (en adelante, EADTrust), ha definido para la creación, comprobación, validación y revocación de certificados para la autenticación de **sitios web**. Este documento comprende en su alcance varios tipos de certificados (agrupados por similitud) a una comunidad o un uso concretos[1], concretamente los siguientes:

- DVC (Domain Validation Certificates)
- OVC (Organizational Validation Certificates)
- OVEH (Organizational Validation for electronic head office) en particular, los OV de sede electrónica de administración pública
- EVC (Extended Validation Certificates).
- EVEH (Extended Validation for electronic head office) en particular, los EV de sede electrónica de administración pública

EADTrust ha definido una política específica para los certificados web (QWAC) expedidos para entidades PSD2. Para más información al respecto deberá consultar la política de referencia y la Declaración de Prácticas de Certificación.

La finalidad de esta política es definir las líneas generales de la prestación de estos servicios. Para una información más detallada y completa se recomienda la lectura de la Declaración de Practicas de Servicios Electrónicos de Confianza de EADTrust (en lo adelante DPC o Declaración de Prácticas de Certificación).

1.1.- Definición

Los certificados definidos en esta política son expedidos en correspondencia con 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, e IDAS). Esta política ha sido diseñada teniendo en consideración los estándares internacionales establecidos en ETSI e IETF, en particular el IETF RFC 3647.

Además de cumplir con la normativa técnica y jurídica desarrollada en el marco del Reglamento eIDAS, EADTrust cumple los requisitos denominados “Baseline Requirements” (en lo adelante BRG) 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

También cumple los requisitos denominados “Guidelines For The Issuance And Management Of Extended Validation Certificates” (en adelante EVCG) para la emisión de dicho tipo de certificados. La versión disponible en la última revisión de esta política es la 1.6.9.

Dentro de las políticas de certificación definidas en ETSI EN 319 411-1, EADTrust adopta como políticas de base para sus certificados de autenticación web siguientes:

- Política de Certificado de Validación Extendida (EVCP) para los certificados TLS/SSL que ofrece el nivel de garantía requerido por el Foro CAB para Validación Extendida (EV). Incluye, excepto cuando se indique explícitamente, todos los requisitos de la Política de Certificados Normalizados (NCP), más los requisitos adicionales, disposiciones adecuadas para apoyar la expedición y gestión de los certificados de validación extendida (EVC), como se especifica en el EVCG

- Política de Certificados de Validación de Dominio (DVCP) para certificados TLS/SSL que ofrece el nivel de garantía requerido por el Foro CAB para certificados de Validación de Dominio (DV). Los requisitos de la política para este CP se basan en los requisitos de la política para la emisión y gestión de certificados de LCP, mejorada para referirse a los requisitos del BRG, como aplicable a los certificados de validación de dominio. Incluye, excepto cuando se indique explícitamente, todos los certificados de Requisitos de la Política de Certificados (LCP), además de disposiciones adicionales adecuadas para apoyar la emisión de DVC y de gestión como se

[1] “indicates the applicability of a certificate to a particular community and/or class of application with common security requirements” RFC 3647

especifica en el BRG

- Política de Certificados de Validación de la Organización (OVCP) para los certificados TLS/SSL que ofrecen el nivel de garantía requerida por el Foro CAB para certificados de Validación de Organización (OV) (DVC. Los requisitos de la política para este CP se basan en la política requisitos para la emisión y gestión de certificados de LCP, mejorados para referirse a los requisitos de BRG como aplicable a los certificados de validación de la organización. Incluye, excepto cuando se indique explícitamente, todos los requisitos de la Política de Certificados de Peso Ligero (LCP), además de disposiciones adicionales adecuadas para apoyar a los OVC emisión y gestión como se especifica en el BRG.

Asimismo, EADTrust adopta las variaciones de política definidas en ETSI EN 319 411-2 para los certificados cualificados de sitio web conforme al Reglamento (UE) No 910/2014:

- Una política para los certificados de sitios web calificados de la UE (QCP-w) que ofrece el nivel de calidad definido en el Reglamento (UE) Nº 910/2014 para los certificados reconocidos por la UE (que requieren o no el uso de un dispositivo criptográfico seguro) utilizado en apoyo de la autenticación de sitios web:

- Cuando el certificado se emite a una persona jurídica, los requisitos para el QCP-w incluyen todos los EVCP requisitos, además de disposiciones adicionales adecuadas para apoyar la emisión de certificados cualificados de la UE y de la gestión según lo especificado en el Reglamento (UE) Nº 910/2014.

Para el certificado de sede electrónica administrativa, se ha tomado en consideración, además, lo establecido en el documento denominado "Perfiles de Certificados Electrónicos 2.0 en el marco de la Leyes españolas 39/2015 y 40/2015." [2]

1.2.- Soporte y nivel de seguridad

Tipo	Certificado	Standard Policy Identifier	EAD Trust Policy OID	Formato	Nivel de seguridad
Autenticación de sitio web	SSL DV (QWAC)	0.4.0.194112.1.4 (ETSI QCP-w) 2.23.140.1.2.1 (CAB/FORUM DV)	1.3.6.1.4.1.501.2.1.1.0.41241	Software	Sustancial
	SSL OV (QWAC)	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 (QWAC)	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 OVEH Sede (QWAC)	0.4.0.194112.1.4 (ETSI QCP-w) 2.23.140.1.2.2 (CAB/FORUM OV)	1.3.6.1.4.1.501.2.1.1.0.41245	Software	Sustancial Distancia***
	SSL EVEH Sede (QWAC)	0.4.0.194112.1.4 (ETSI QCP-w) 2.23.140.1.1 (CAB/FORUM EV)	1.3.6.1.4.1.501.2.1.1.0.41246	Software	Alto Distancia***

(*) Los dispositivos habituales son HSM (Hardware Security Module), token seguro y tarjeta chip. Los tokens USB se consideran equivalentes al uso de tarjetas inteligentes considerando que incorporan la tarjeta y la chaqueta lectora en el mismo dispositivo.
(**) Presencial: Identifica los OID de Políticas de certificados en los que la validación y autenticación de la identidad del Solicitante se realiza de manera presencial en las instalaciones de la RA.
(***) Distancia: Identifica los OID de Políticas de certificados en los que la validación y autenticación de la identidad del Solicitante se realiza por la RA, de manera remota (on line, también denominada telepresencia). Para ello pueden desplegarse medios de videoidentificación o videoconferencia.

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

2.- Participantes en la PKI

En este apartado se ofrece un resumen de los participantes en la PKI de EADTrust, sus responsabilidades, obligaciones y aspectos técnicos que los caracterizan. Puede consultarse una información ampliada al respecto en la Declaración de Prácticas de Certificación.

2.1.- Autoridades de Certificación

La Autoridad de Certificación de EADTrust (en lo adelante la CA) es la encargada de emitir los certificados definidos en esta política.

Las CAs están organizadas en una jerarquía de dos niveles, con varias CAs raíz offline, adaptadas a las normas y prácticas actuales del sector, desde el punto de vista tecnológico. Se diferencian por algoritmo de clave pública, tamaño de la clave y por diferentes usos de los certificados de entidad final, cualificados y no cualificados:

Para certificados cualificados web:

- RSA Root CA Web 4096-bit key size with SHA256 digest algorithm (Domain y Organization Validated).
- RSA Root CA Web 8192-bit key size with SHA512 digest algorithm (Domain y Organization Validated).
- ECC Root CA Web P-256 with SHA256 digest algorithm (Domain y Organization Validated).
- ECCRoot CA Web P-384 with SHA384 digest algorithm (Domain y Organization Validated).
- RSA Root CA Web 4096-bit key size with SHA256 digest algorithm (Extended Validation y PSD2).
- RSA Root CA Web 8192-bit key size with SHA512 digest algorithm (Extended Validation y PSD2).
- ECC Root CA Web P-256 with SHA256 digest algorithm (Extended Validation y PSD2).
- ECCRoot CA Web P-384 with SHA384digest algorithm (Extended Validation y PSD2).

Para certificados no cualificados

- RSA Root CA 2048-bit key size size with SHA256 digest algorithm para certificados No cualificados.

Para proporcionar un nivel de seguridad adecuado, las CA's raíz siempre se mantienen offline, emitiéndose los certificados para los subscriptores, desde las Sub-CA's correspondientes.

Pueden emitir Certificados bajo la jerarquía EADTrust las Autoridades de Certificación operadas por organizaciones externas cuyas Políticas o DPC estén conformes con las políticas de certificación de EADTrust y hayan sido previamente autorizadas. Existirá una relación escrita formal y contractual con EADTrust para dar cobertura a los compromisos mutuos. A la fecha de redacción de este documento solo la CA de EADTrust está habilitada para ofrecer el servicio.

En la Declaración de Prácticas de Certificación se ofrece información ampliada sobre la Autoridad de Certificación de EADTrust y los aspectos técnicos y de seguridad definidos para esta.

2.2.- Autoridades de Registro

EADTrust, como CA, emite algunos certificados directamente empleando su propia Autoridad de Registro (AR, en inglés RA, Registration Authoritie). Sin embargo, como empresa de servicios, el Mercado de certificados normalmente se alcanza a través de Autoridades de Registro operadas por organizaciones externas.

Estas RAs son entidades que actúan de acuerdo con esta Política de Certificación y las prácticas descritas en la Declaración de Prácticas de Certificación (DPC), junto con una relación escrita formal y contractual con EADTrust.

Las RAs que cooperan en la jerarquía de EADTrust, están obligadas a cumplir con todas las Políticas de Certificación de EADTrust, así como superar la evaluación anual de cumplimiento obligatoria realizada por EADTrust o cualquier tercero evaluador o auditor designado por EADTrust.

Su objetivo principal es la gestión de relaciones de suscriptores, que incluye la identificación y registro de los suscriptores, las solicitudes de certificados y cualquier otra obligación indicada en esta política y las políticas específicas de certificados en relación con la gestión del ciclo de vida de los certificados.

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 en persona o mediante videoconferencia (también descrita como mediante telepresencia) o videograbación ("digital onboarding"). A la fecha de redacción de esta política el servicio está disponible de manera presencial o por identificación remota mediante videoconferencia o firma electrónica cualificada conforme se describe en la política específica.

Para la videoconferencia[3] EADTrust cumple lo establecido en el Real Decreto-ley 11/2020, de 31 de marzo, por el que se adoptan medidas urgentes complementarias en el ámbito social y económico para hacer frente al COVID-19. Así como, lo previsto en la normativa española publicada por el servicio de prevención de Blanqueo de Capitales (SEPBLAC) y la Directiva (UE) 2015/2366 (PSD2) que se utilizará incluso en los servicios de iniciación de pagos como medio para proporcionar autenticación fuerte de los clientes.

Para más detalles se recomienda la lectura de la política definida al efecto.

Tanto si la suscripción es en persona o mediante telepresencia, cada RA está sujeta, pero no limitada, a las siguientes obligaciones:

- Identificación y autenticación de los titulares y suscriptores de certificados.
- Desarrollo de una relación contractual para la emisión de certificados con la entidad final o el suscriptor.
- Generación de certificado (por medio de comunicación autenticada con la CA online) y la entrega del certificado de forma que se pueda instalar en el servidor web. O con la relación del suscriptor con la RA.
- Proporcionar cualquier información requerida por EADTrust relacionada con sus servicios de certificación y operaciones, en cualquier momento, y, especialmente, durante la evaluación de cumplimiento anual con las Políticas de Certificación de EADTrust.

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.

2.3.- Suscriptores (titulares de certificado)

Entidades Finales

Las entidades finales son cualquier persona u organización que reciba servicios de emisión de certificado, gestión y uso de certificados digitales. Entre otros se incluyen (pero no están limitados a estos):

- Solicitantes de certificados, por sí mismos o cualquier otro interesado.
- Suscriptores de certificados que tienen la propiedad del certificado.
- Propietarios de la clave, quienes las utilizan para los propósitos específicos del certificado.
- Terceros representados.
- Terceros que confíen en los certificados.

Solicitantes de Certificados

Todo certificado debe solicitarse por una persona, en su propio nombre o en el de una entidad con la cual se establece una relación contractual especificando el alcance de la representación.

Por ello, los solicitantes de certificados pueden ser:

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

- Persona física actuando en nombre y representación de una persona jurídica con la cual se establece una relación contractual especificando el alcance de la representación.

Los **certificados de sede electrónica** los pueden solicitar funcionarios de las administraciones públicas que acrediten su identidad y su adscripción al organismo para el que solicitan el certificado. En caso de entidades de derecho público, los certificados de sede electrónica los puede solicitar personal laboral con poder o mandato que conste por escrito. En caso de concursos y licitaciones, los certificados de sede electrónica los pueden solicitar las personas designadas en cumplimiento de los pliegos por el poder adjudicador.

.

Suscriptores del Certificado

El suscriptor de un certificado es la persona jurídica que posee el certificado asociado a un servidor web que se vincula con una clave privada.

Propietarios de la clave

El propietario de la clave es una persona física o jurídica que tiene y puede utilizar exclusivamente las claves criptográficas del certificado en un servidor web.

En el contexto de la emisión de certificados QSEAL y QWAC para entidades PSD2 pueden intervenir otros participantes. Se recomienda la lectura de la política específica para aclaraciones al respecto.

Representante del solicitante

Cualquier persona jurídica se considerará como representada en caso de que cualquier solicitante de certificado solicite el certificado debidamente identificado y con documentación legal que acredite que actúa en nombre y representación de la persona que otorga la representación para obtener y gestionar dicho certificado.

Partes que Confían

Las entidades o individuos que actúan confiando en certificados u objetos firmados emitidos bajo esta PKI son partes que confían.

Las partes que confían acceden al certificado en virtud de una conexión SSL/TLS, y deberían verificar la validez del certificado y su propósito.

Deben comprobar por el campo AIA (Authority Information Access) 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 el servicio OCSP, o, cuando corresponda, por la lista CRL.

Un resumen de lo que deben conocer se encuentra disponible en el documento PDS (PKI Disclosure Statement), redactado de forma que se facilite la divulgación de los servicios con lenguaje sencillo de forma similar al prospecto de un medicamento.

- http://policy.eadtrust.eu/pds/

3.- Uso del certificado

A continuación, se describen los usos permitidos y prohibidos de los certificados emitidos por EADTrust.

3.1.- Usos Adecuados del Certificado

Los certificados de autenticación web se usarán para cifrar las comunicaciones entre el navegador y el servidor web e identificar el dominio y al propietario del dominio. En el caso de los certificados de sede electrónica se pueden usar para dotar a la misma de capacidades SSL/TSL.

También pueden usarse este tipo de certificados, para firmar mensajes de autenticación, en particular desafíos de cliente TLS. Esta firma digital de carácter técnico se utiliza para garantizar la identidad del suscriptor del certificado, pero no expresan conformidad con lo firmado. Los certificados cualificados se ajustan a la norma técnica En 319 412 (documentos 1 a 5) del Instituto Europeo de Normas de Telecomunicaciones ETSI.

3.2.- Usos Prohibidos del Certificado

Los certificados para sitio web solo deben ser utilizados para el establecimiento de comunicaciones seguras en base al protocolo TLS con sitios web. No se pueden utilizar para realizar firmas electrónicas o sellos electrónicos de documentos electrónicos ni para firmar otros certificados.

Los certificados sólo deben utilizarse de conformidad con la legislación aplicable. No se pueden usar en sitios web que desarrollen actividades ilegales en la jurisdicción en la que resida el propietario del sitio web.

Los Certificados no se pueden usar en equipos de control destinados su utilización en situaciones peligrosas o en los que un mal funcionamiento suponga un peligro para la vida humana o para objetos valiosos. Cualquier uso en estos contextos exime de responsabilidad al Prestador de servicios de confianza digital.

EADTrust incorpora en el certificado información sobre la limitación de uso, en campos estandarizados en los atributos “uso de la clave” (**Key usage**), “uso extendido de clave” (**Extended Key Usage**).

4.- Administración de Políticas

4.1.- Organización que Administra el Documento

EADTrust, con domicilio social en Calle Alba, 15 de Madrid (España) y NIF. B-85626240, es la Autoridad de Certificación que emite los certificados bajo esta Política.

4.2.- Contacto

Nombre del PSC	European Agency of digital Trust, S. L.
Dirección	C/ Alba,15, 28043 Madrid - Spain
Dirección de email	policy@eadtrust.eu
Teléfono	(+34) 902365612 / (+34) 917160555

4.3.- Procedimiento de aprobación de las políticas de certificados

El Órgano de Aprobación y Gestión de Políticas de Certificación de EADTrust aprueba los cambios finales realizados en este documento una vez que determine que cumplen con los requisitos establecidos.

Es posible contactar con el Órgano de Gestión y Aprobación de Políticas de certificados en: E- mail: policy@eadtrust.eu.

Las direcciones postales, teléfonos y fax se encuentran publicadas en https://www.eadtrust.eu.

5.- Publicación de información y repositorio de certificados

5.1.- Publicación de la información de certificación

La CA divulga públicamente sus Políticas de Certificados y la Declaración de Prácticas de Certificación a través de su web (un medio on line apropiado y fácilmente accesible que está disponible 24 horas al día, 7 días a la semana).

La URL en la que está disponible la información de políticas y la Declaración de Prácticas de Certificación es:

- policy.eadtrust.eu

La divulgación incluye todo el material requerido por la norma RFC 3647 y se estructura de acuerdo con dicha norma.

La CA destinada a la emisión de certificados para SSL/TLS se ajusta a la versión actual de los Requisitos Básicos para la Emisión y Gestión de Certificados de Confianza Pública publicados en http://www.cabforum.org. En caso de cualquier incoherencia entre este documento y los Requisitos, dichos Requisitos prevalecerán sobre este documento.

EADTrust aloja páginas web de prueba que permiten a los Proveedores de Software de Aplicación probar su software con Certificados de Suscriptor que encadenan cada Certificado Raíz de confianza pública. EADTrust aloja páginas web separadas utilizando Certificados de Suscriptor de diversos tipos: (i) válidos, (ii) revocados y (iii) expirados.

Los dominios de los sitios web de pruebas que permiten comprobar el uso de certificados para SSL/TLS son los siguientes

- https://ecc-256-dv-tst.eadtrust.eu/
- https://ecc-256-ev-tst.eadtrust.eu/
- https://ecc-256-ov-tst.eadtrust.eu/
- https://ecc-256-psd2-tst.eadtrust.eu/
- https://ecc-384-dv-tst.eadtrust.eu/
- https://ecc-384-ev-tst.eadtrust.eu/
- https://ecc-384-ov-tst.eadtrust.eu/
- https://ecc-384-psd2-tst.eadtrust.eu/
- https://rsa-2048-dv-tst.eadtrust.eu/
- https://rsa-2048-ev-tst.eadtrust.eu/
- https://rsa-2048-ov-tst.eadtrust.eu/
- https://rsa-2048-psd2-tst.eadtrust.eu/
- https://rsa-2048-evsedealto-tst.eadtrust.eu/
- https://rsa-2048-ovsedemedio-tst.eadtrust.eu/
- https://rsa-4096-dv-tst.eadtrust.eu/
- https://rsa-4096-ev-tst.eadtrust.eu/
- https://rsa-4096-ov-tst.eadtrust.eu/
- https://rsa-4096-psd2-tst.eadtrust.eu/
- https://rsa-8192-dv-tst.eadtrust.eu/
- https://rsa-8192-ev-tst.eadtrust.eu/

- https://rsa-8192-ov-tst.eadtrust.eu/
- https://rsa-8192-psd2-tst.eadtrust.eu/

Sobre los mismos dominios se pueden comprobar certificados vigentes, caducados y revocados, accediendo por puertos diferentes:

Certificados vigentes (443):

- https://rsa-2048-dv-tst.eadtrust.eu Certificados vigentes

Certificados revocados no expirados (8443):

- https://rsa-2048-dv-tst.eadtrust.eu:8443 Certificados revocados no expirados

Certificados caducados (9443):

- https://rsa-2048-dv-tst.eadtrust.eu:9443 Certificados Caducados

5.2.- Tiempo o Frecuencia de Publicación

EADTrust se compromete a desarrollar, implementar, hacer cumplir y actualizar con periodicidad bienal, su Política de Certificación y su Declaración de Prácticas de Certificación, como uno de los elementos asociados a la auditoría bienal. El intervalo de actualización será menor cuando se produzcan cambios técnicos o legales que hagan necesaria una actualización.

Las auditorías de la CA destinada a la emisión de certificados para SSL/TLS serán anuales.

5.3.- Repositorios

La CA proporciona información de revocación para los Certificados Subordinados y los Certificados de Suscriptor disponibles de acuerdo con esta Política.

La URL en la que está disponible la información de revocación (y que se indica en el campo AIA del certificado) es:

- ocsp.eadtrust.eu

Además, la posible revocación de las CA raíz y las CAs subordinadas quedará registrada en la URL:

- crl.eadtrust.eu

Las políticas de certificación, la declaración de prácticas de certificación y la declaración abreviada para terceros que confían (PDS, Policiy Disclosure Statement) estarán disponles en la URL:

- policy.eadtrust.eu

6.- Identificación y Autenticación

6.1.- Nombre

6.1.1.- Tipos de Nombres

Para los certificados amparados en esta política, el dato principal es el nombre de dominio o dominios y también podrán utilizarse nombres que identifiquen subdominios mediante una referencia genérica (wildcard). Es necesario acreditar la

relación con el dominio, con la organización o con datos extendidos de la organización (domain validation, organization validation, extended validation).

6.2.- Identificación y validación de la identidad

6.2.1.- Método para probar la posesión de la clave privada

- El solicitante aporta una solicitud de certificado PKCS#10 generada en su servidor web, lo que implica la posesión de la clave privada.

- Si las claves se entregan en un fichero PKCS#12 (o PFX) la prueba de posesión de la clave privada se demuestra en virtud del procedimiento confiable de entrega y aceptación del fichero y de la clave de descifrado, que podrán hacer uso de técnicas de comunicación de doble factor de autenticación (por ejemplo, un mensaje de correo electrónico o un SMS) o un secreto compartido determinado en el momento de completar la solicitud de certificado.

6.2.2.- Autenticación de la organización e identidad del dominio

Como parte del proceso de autenticación de EADTrust, en el caso de expedición de certificados para servidor web, se valida el nombre de la organización introducido durante la inscripción, que se hace constar en el campo apropiado del certificado.

La organización a la que se atribuye un certificado debe ser una entidad activa, confirmada por una autoridad oficial responsable del registro de empresas dentro de la jurisdicción específica (localidad, estado, país) indicada en la solicitud del certificado. El nombre de la organización inscrita y el nombre alegado deben coincidir literalmente. En caso de existir abreviaturas, solo se aplicarán a las partes que identifican el tipo legal de sociedad o entidad (S.A., S.L., S. COOP., LLC, Ltd). Cuando las entidades no sean sociedades se utilizarán de referencia los poderes notariales aportados y publicaciones de nombramientos en los boletines oficiales.

Además, se comprobará que la titularidad del nombre de dominio corresponde a la organización, y se solicitará confirmación a las direcciones de correo que figuran asociadas al dominio a través del servicio WHOIS. EADTrust también podrá utilizar otros medios para llevar a cabo esta comprobación.

Si la entidad hace uso en su DNS de las extensiones[4] que restringen la emisión de certificados a determinados Prestadores de Servicios de Certificación, EADTrust solo emitirá certificados de servidor web en caso de que se indique expresamente esta preferencia. EADTrust revisa los registros CAA (Certification Authority Authorization) al comprobarlos datos de Dominios Completamente Cualificados dejando constancia de las acciones de comprobación en sus registros y logs.

El dominio atribuido al certificado, se verificará de acuerdo a los requerimientos definidos en las “Baseline Requirements for the issuance and management of publicly-trusted certificates” y “Guidelines for the issuance and management of extended validation certificates” of CA/Browser Forum”, en sus últimas versiones.

6.3.- Identificación y autenticación para la solicitud de revocación

El inicio de una solicitud de revocación se produce:

- A solicitud de un representante de la entidad propietaria del sitio web.
- Por el titular, por compromiso de sus claves o por cualquier otra razón que lo requiera.

[4] RFC 6844: DNS Certification Authority Authorization (CAA) Resource Record

Para solicitar la revocación se requiere la personación física del solicitante de la revocación en una Entidad de Registro, o bien que el solicitante haga uso del servicio de revocación remota proporcionado al efecto, que podrá requerir la aportación de información específica para ello.

7.- Requisitos Operacionales del Ciclo de Vida de los Certificados

7.1.- Solicitud del Certificado

El interesado en un certificado "Organization validated" y "Extended Validated" de los definidos en esta política, deberá cumplimentar el formulario de solicitud de emisión de certificados disponible en la página web: www.eadtrust.eu

En el citado formulario, podrá agendar, además, una cita con la Autoridad de Registro de EADTrust para la verificación de su identidad.

La cita con la Autoridad de Registro de EADTrust se llevará a cabo mediante videoconferencia conforme a los requisitos definidos en la Política especifica definida por EADTrust al efecto.

Una vez cumplimentado el formulario de solicitud, EADTrust enviará un e mail con la información de la fecha y hora de la cita; así como de la documentación que deberá enviar a la RA antes de la fecha de la cita agendada. La documentación requerida es la siguiente:

- Documento Identificación: DNI, NIE, PAS
- Poder que acredita la Representación vigente
- Debe conocer además la siguiente información:
    a) deberá identificar además la categoría de la entidad
        i. Organización privada.
        ii. Entidad gubernamental.
        iii. Entidad comercial.
        iv. Entidad no comercial.
    b) Indicar el tipo de certificado web que se desea adquirir:
        i. Certificado cualificado de web domain validated (DV).
        ii. Certificado cualificado de web organización validated (OV).
        iii. Certificado cualificado de web organización validated (OV).de sede electrónica.
        iv. Certificado cualificado de web extended validación (EV).
        v. Certificado cualificado de web extended validation (EV).de sede electrónica.

- Indicar el nombre del dominio/dominios que desea autenticar (DNS/CSR).

La documentación remitida debe encontrarse en buen estado de conservación, legible, y vigente en la fecha de la cita.

Los interesados en los certificados "Domain Validation" podrán ponerse en contacto con EADTrust vía email: info@eadtrust.eu indicando además el nombre del dominio/dominios que desea autenticar (DNS/CSR).

EADTrust se pondrá en contacto con el solicitante para gestionar la firma del contrato de prestación del servicio mediante una firma electrónica cualificada y una vez que este haya sido devuelto firmado. EADTrust procederá a expedir el certificado correspondiente.

En el caso de licitaciones se tendrán en cuenta las condiciones establecidas por el poder adjudicador.

7.1.1.- Quién puede enviar una solicitud del certificado

- Pueden solicitar un certificado las personas físicas representantes de personas jurídicas propietarias de un sitio web que necesiten: el uso de comunicaciones cifradas en su sitio web de forma que se confirme la identidad

del dominio. En el caso de licitaciones se tendrán en cuenta las condiciones establecidas por el poder adjudicador.

7.1.2.- Proceso de inscripción y responsabilidades

Las tareas de identificación y validación de la información en el certificado y validación y aprobación de las solicitudes de emisión yrevocación serán realizadas por las Oficinas de Registro.

Las Oficinas de Registro Propias de EADTrust o de las entidades usuarias con las que EADTrust firme el correspondiente instrumento legal deberán asumir las siguientes obligaciones:

- Validar la identidad y otros detalles personales del solicitante, del suscriptor y del propietario de la clave en los certificados o la información relevante para el fin de los certificados según estos procedimientos.
- Verificar la pertenencia del dominio al solicitante.
- Mantener toda la información y documentación relativa a los certificados, y gestionar su emisión, renovación, revocación o reactivación.
- Notificar a EADTrust sobre las solicitudes de revocación de certificados con la debida diligencia y de una manera rápida y confiable.
- Permitir a EADTrust el acceso a sus archivos de procedimiento y registros de auditoría para desempeñar sus funciones y mantener la información necesaria.
- Informar a EADTrust sobre las solicitudes de emisión, y revocación; así como, cualquier otro aspecto relacionado con los certificados emitidos por EADTrust.
- Validar, con la debida diligencia, las circunstancias de revocación que puedan afectar a la validez del certificado.
- Cumplir con los procedimientos establecidos por EADTrust y con la legislación vigente en esta materia, en sus operaciones de gestión relacionadas con la emisión, renovación y revocación de certificados.
- Cuando proceda, puede realizar la función de poner a disposición del titular de la clave los procedimientos técnicos para la creación de firmas (clave privada) y la comprobación de la firma electrónica (clave pública).

7.2.- Procedimiento de Solicitud del Certificado

Una vez haya tenido lugar una petición de certificado y se ha agendado la cita conforme indica esta Política, el operador de la RA procederá durante la videoconferencia a iniciar el proceso de identificación y validación de identidad declarada.

El proceso de emisión del certificado se llevará a cabo en una plataforma de gestión interna. En esta la RA introduce los datos declarados y posteriormente verificará que la información proporcionada es correcta.

7.2.1.- Realización de funciones de identificación y autenticación

Se comprobará la identidad del solicitante y la posesión del dominio, siguiendo las pautas marcadas por las “Baseline Requirements for the issuance and management of publicly-trusted certificates” y “Guidelines for the issuance and management of extended validation certificates” of CA/Browser Forum”, en sus últimas versiones.

En el caso de licitaciones se tendrán en cuenta las condiciones establecidas por el poder adjudicador.

7.2.2.- Aprobación o Rechazo de Solicitudes de Certificado

Una vez que se haya solicitado el certificado, la RA comprobará la información proporcionada por el solicitante, incluida la validación de la identidad del suscriptor, y en su caso, de la suficiencia de poderes de representación.

Si la información no es correcta, la RA denegará la solicitud y se pondrá en contacto con el solicitante para explicar la razón. Si la información es correcta, se emitirá el certificado.
En el proceso de expedición de certificados de EADTrust, se aplican controles duales, de modo que la decisión de expedición del certificado no la pueda tomar la misma persona que comprueba la información asociada a la solicitud.

En el proceso de expedición de los certificados web (extended validation, organization validation, domain validation) definidos en esta Política, además, se aplica un tercer control para la comprobación de que el dominio esté bajo el control exclusivo del solicitante del certificado.

7.2.3.- Tiempo para procesar las solicitudes de certificado

Una vez verificada la información requerida en el proceso de solicitud de certificados, se podrá proceder a la emisión del certificado que se requiera. El tiempo estimado de emisión de certificados tras la verificación es de 24 horas en días laborables.

7.3.- Emisión del Certificado

Todas las solicitudes deben ser aprobadas en su totalidad antes de que los certificados puedan ser emitidos. Una vez aprobada la solicitud EADTrust emitirá el certificado y lo entregará personalmente o lo remitirá por vía telemática.

7.3.1.- Acciones de la CA durante la emisión del certificado

Los certificados se pueden emitir en un soporte de software.

I. **Procedimiento de emisión de certificados emitidos mediante un mecanismo de software, con clave privada generada por el solicitante:**

- Junto con el formulario de solicitud, el solicitante genera un par de claves en su propio ordenador, y hace llegar a EADTrust la solicitud de certificado con formato PKCS#10.
- La Autoridad de Registro autentica la validez de la documentación remitida por el solicitante.
- Después de recibir la documentación, EADTrust emite el certificado, que se deberá insertar en el dispositivo en el que se generó la solicitud.

II. **Procedimiento de emisión de certificados emitidos mediante un mecanismo de software, con clave privada generada por el Prestador:**

- El solicitante genera el formulario de solicitud.
- La Autoridad de Registro autentica la validez de la documentación remitida por el solicitante.
- Después de recibir la documentación, EADTrust emite el certificado vinculado con la clave privada, en formato PKCS#12 cifrado, que se puede insertar en cualquier dispositivo, incluso aunque no sea el dispositivo en el que se generó la solicitud.
- Por una vía diferente a la de la entrega del fichero PKCS#12 se hace llegar al solicitante la clave que permite el descifrado e instalación del fichero PKCS#12.
- EADTrust elimina la clave privada y el fichero PKCS#12 tras su remisión al solicitante.

7.3.2.- Notificación al suscriptor sobre la emisión del certificado por la CA

Generalmente dentro de las 24 horas en que se solicitó el certificado; salvo que en el proceso de identificación y verificación de la identidad ante la Rase detecte alguna irregularidad a ser subsanada o que impida la expedición del certificado.

7.4.- Aceptación del Certificado

La aceptación de un certificado supone la aceptación por el suscriptor de los términos y condiciones del contrato que determinan los derechos y obligaciones de EADTrust y la comprensión por el suscriptor de las disposiciones de esta Política que rigen los aspectos técnicos y operativos de los servicios de certificación digital proporcionado por EADTrust.

El suscriptor/propietario de la clave tiene un plazo determinado de 10 días desde la entrega del certificado para asegurarse de que funciona correctamente y, si es necesario, devolverlo a la Autoridad de Registro.

Si se devuelve un certificado debido a defectos técnicos (por ejemplo, funcionamiento defectuoso del almacenamiento en soportes de los certificados, problemas con la compatibilidad del programa, error técnico en el certificado, etc.) o a errores en los datos contenidos en el certificado, EADTrust revocará el certificado emitido y emitirá uno nuevo.

7.4.1.- Conducta que constituye la aceptación del certificado

Con la firma del contrato de condiciones generales y particulares del servicio, EADTrust entiende que el Suscriptor/Titular de las claves ha aceptado las condiciones de uso, obligaciones y deberes especificadas en el propio clausulado del contrato y por ende ha aceptado el certificado.

7.4.2.- Publicación del certificado por la CA

Los certificados destinados a sitios web se registrarán cuando corresponda en el sistema de “Certificate Transparency” desde el que estarán disponibles para terceros. Esta es una medida de seguridad definida en el marco de CAB Forum.

7.4.3.- Notificación de la emisión del certificado por la CA a otras entidades

EADTrust podrá publicar los certificados de sitio web (utilizados en contextos de securización de comunicaciones mediante protocolos de tipo TLS) según la normativa “CertificateTransparency”[5]

7.5.- Par de Claves y Uso del Certificado

7.5.1.- Clave privada del suscriptor y uso del certificado

El suscriptor que tiene la custodia de las claves:

- Garantizará el uso correcto y el mantenimiento de los soportes de almacenamiento del certificado.
- Facilitará a EADTrust y a sus entidades de registro información completa y adecuada, conforme a los requerimientos de esta política de certificado y de las políticas específicas, en especial en lo relativo al procedimiento de registro.
- Hará uso adecuado del certificado y, en particular, cumplirá con las limitaciones de uso del mismo.
- Salvaguardará diligentemente la clave privada (sea cual sea su soporte, e incluso si se trata de una copia de respaldo) y la clave o código PIN que permite su activación para evitar el uso no autorizado
- Notificará a EADTrust, y a cualquier otra persona que el suscriptor piense que pueda confiar en el certificado, sin demora razonable, si se produce alguna de las siguientes situaciones:
    - La clave privada del suscriptor se ha perdido, ha sido robada o se ha visto potencialmente comprometida.
    - El control sobre la clave privada del suscriptor se ha perdido debido a que los datos de activación se han visto comprometidos (por ejemplo, código PIN del dispositivo criptográfico) o debido a otras razones.
    - Inexactitud o cambios en el contenido del certificado, según lo notificado o sospechado por el suscriptor, solicitando la revocación del certificado cuando tales cambios constituyan una causa de revocación.
- Dejará de usar la clave privada al final del período de validez del certificado.

[5] https://www.certificate-transparency.org/

- Se abstendrá de supervisar, interferir o realizar un proceso de ingeniería inversa de la implementación técnica de los servicios de certificación sin la previa aprobación por escrito de la Autoridad de Certificación.
- Se abstendrá de comprometer intencionadamente la seguridad de los servicios de certificación.
- Se abstendrá de utilizar las claves privadas correspondientes a las claves públicas incluidas en los certificados con el fin de firmar un certificado como si desempeñara la función de una Autoridad de Certificación.
- Los suscriptores de certificados cualificados que generen firmas digitales utilizando la clave privada correspondiente a la clave pública incluida en el certificado deben asumir que tales firmas electrónicas son equivalentes a firmas manuscritas, siempre que se utilice un dispositivo criptográfico (dispositivo cualificado de creación de firma electrónica), según las disposiciones del Reglamento eIDAS.
- Los suscriptores de certificados cualificados que generen sellos digitales utilizando la clave privada correspondiente a la clave pública incluida en el certificado deben asumir que tales sellos digitales gozan de presunción de integridad de los datos y de la corrección del origen de los datos a los que el sello electrónico cualificado esté vinculado, siempre que se utilice un dispositivo criptográfico (dispositivo cualificado de creación de sello electrónico), según las disposiciones del Reglamento eIDAS.
- Abonar las tarifas por los servicios de certificación solicitados en los términos y condiciones previstos por la CA, cuando el titular coincida con el suscriptor.
- Autorizar a la CA a que, a través de la RA, utilice los datos personales aportados por el titular para validar, comprobar y autenticar la identidad declarada por este.
- Solicitar la revocación del Certificado cuando se cumpla alguno de los supuestos previstos en esta política y en las prácticas específicas y en la legislación vigente para los diferentes status del ciclo de vida de los certificados
- Comprender y aceptar los términos y condiciones de uso del certificado, y cualquier modificación que se realice a estos
- No comprometer intencionalmente la seguridad de los servicios de certificación
- Todas las que se deriven de la DPC, de esta política de certificado específica y de la legislación vigente.

7.5.2.- Uso de la clave pública por la parte que confía y uso del certificado

Los terceros que confían en los certificados expedidos por EADTrust deben verificar la validez de los certificados y están sujetos a las siguientes obligaciones:

- Evaluar independientemente la idoneidad del uso de un certificado y determinar que, de hecho, se utilizará para un propósito apropiado.
- Ser consciente de las condiciones para usar los certificados de conformidad con lo establecido en la Declaración de Práctica de Certificación, y especialmente, en la PDS (Policy Disclosure Statement), es decir, la declaración abreviada para terceros que confían.
- Comprobar la validez, o revocación de los certificados emitidos, utilizando la información sobre el estado del certificado, disponible en el servicio OCSP.
- Comprobar todos los certificados en la jerarquía de certificados antes de confiar en una firma digital o en cualquiera de los certificados de la jerarquía. En relación con los certificados cualificados, comprobar que la autoridad de certificación raíz de EADTrust en cuya jerarquía se encuentra el certificado, está incluida en la lista TSL correspondiente[6].
- Tener en cuenta las limitaciones de uso de los certificados, ya estén contenidas en el propio certificado, en la PDS o en su caso, en el contrato de verificador.
- Tener en cuenta las precauciones incluidas en un contrato u otro instrumento, independientemente de su naturaleza legal.
- Notificar a EADTrust cualquier inexactitud o defecto en un certificado que pueda considerarse causa de revocación.
- Abstenerse de supervisar, interferir o realizar ingeniería inversa en la implementación técnica de los servicios de certificación sin la previa aprobación por escrito de la Autoridad de Certificación.
- Abstenerse de comprometer intencionalmente la seguridad de los servicios de certificación.
- Asumir que las firmas electrónicas cualificadas son equivalentes a firmas manuscritas, de conformidad con el artículo 25.2 del Reglamento UE 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

Cada tercero que confía en los certificados expedidos por EADTrust al aceptar el uso de tales certificados reconoce:

[6] En España, la lista TSL la publica el Ministerio de Energía, Turismo y Agenda Digital y está disponible en: http://www.minetad.gob.es/telecomunicaciones/es-es/servicios/firmaelectronica/paginas/prestadores.aspx

- Que dispone de suficiente información para tomar una decisión informada con el objeto de confiar en el certificado o no.
- Que es el único responsable de confiar o no en la información contenida en el certificado.
- Que será el único responsable si incumple sus obligaciones como tercero que confía en el certificado.

7.6.- Renovación del Certificado

EADTrust no renueva los certificados emitidos con anterioridad. El suscriptor que posea un certificado vigente, próximo a expirar, podrá solicitar la emisión de un nuevo certificado. Para lo cual se seguirá el procedimiento técnico de emisión descrito en los apartados anteriores de esta Política.

7.6.1.- Circunstancias para la renovación del certificado

No Aplica.

7.6.2.- Quién puede solicitar la renovación

No Aplica.

7.6.3.- Procesamiento de solicitudes de renovación de certificados

No Aplica.

7.6.4.- Notificación de una nueva emisión de certificado al suscriptor

No Aplica.

7.6.5.- Conducta que constituye la aceptación de un certificado de renovación

No Aplica.

7.6.6.- Publicación del certificado de renovación por la CA

No Aplica.

7.6.7.- Notificación de la emisión del certificado por la CA a otras entidades

No Aplica.

7.7.- Modificación del certificado

Cualquier necesidad de modificación de certificados implicará una nueva solicitud, y llevará aparejado que se realice una revocación del certificado previo y una nueva emisión de certificado, con los datos corregidos.

7.7.1.- Circunstancias para la modificación del certificado

No Aplica.

7.7.2.- Quién puede solicitar la modificación del certificado

No Aplica.

7.7.3.- Procesamiento de las solicitudes de modificación del certificado

No Aplica.

7.7.4.- Notificación de la emisión de un nuevo certificado al suscriptor

No Aplica.

7.7.5.- Conducta que constituye la aceptación de un certificado modificado

No Aplica.

7.7.6.- Publicación del certificado modificado por la CA

No Aplica.

7.7.7.- Notificación de la emisión del certificado por la CA a otras entidades

No Aplica.

7.8.- Revocación y del certificado

Se entenderá por revocación aquel cambio en el estado de un certificado motivado por la pérdida de validez de éste en función de alguna circunstancia distinta a la de su caducidad.

7.8.1.- Circunstancias para la revocación

Las circunstancias que se tomarán en cuenta para la revocación de certificados son las siguientes:

- La solicitud de revocación ha sido realizada por el firmante, la persona física o jurídica representada por el firmante, un tercero autorizado o una persona física que solicitó un certificado digital para una persona jurídica.
- Los datos de creación de firma del firmante o del prestador de servicios de certificación han sido comprometidos o si el firmante o un tercero han utilizado los datos de forma incorrecta.
- Cuando se haya emitido una orden legal o administrativa a tal efecto.
- La muerte del firmante o la extinción de la persona jurídica titular del certificado de sello, la incapacidad total o parcial imprevisible del firmante o de la persona jurídica representada por el firmante, la terminación de la representación, la disolución de la persona jurídica representada, el cambio en las circunstancias de la custodia o uso de los datos de creación de firma o de sello incluidos en los certificados expedidos a una persona jurídica.
- El caso de que EADTrust termine su actividad, excepto en los casos en que el firmante haya dado su consentimiento para que los servicios de gestión de certificados electrónicos sean transferidos a otro prestador de servicios de certificación.
- Cambio en los datos suministrados para obtener el certificado o modificación de las circunstancias verificadas para la emisión del certificado.
- Que haya perdido la clave privada asociada al certificado, que haya sido robada o no sea útil debido a daños en el soporte del certificado o cuando se haya cambiado a otro soporte no previsto en la política de certificación.
- Una de las partes incumple sus obligaciones, como, por ejemplo, el pago.
- Se detecta un error en el procedimiento de emisión del certificado, ya sea porque uno de los requisitos previos no se ha cumplido o debido a problemas técnicos durante el proceso de emisión del certificado.
- Existe una amenaza potencial para la seguridad de los sistemas y para la fiabilidad de los certificados emitidos por EADTrust por razones distintas del compromiso de los datos de creación de firmas.
- Fallo técnico en la emisión o distribución de certificados o de la documentación asociada.
- Si EADTrust recibe una solicitud para la emisión del certificado y ya existe un certificado válido de la misma clase y unicidad, el certificado válido será revocado a petición del solicitante.

7.8.2.- Quién puede solicitar la revocación

La revocación de un certificado podrá solicitarse por

- El sujeto/Firmante.
- El Solicitante responsable.
- La Entidad (a través de un representante de la misma).
- La RA o la CA.
- Podrá realizarse de oficio si a EADTrust le consta por otra vía que se han producido circunstancias que hagan necesaria la revocación.
- En caso de licitaciones, la solicitud de revocación la podrán realizar las personas designadas en cumplimiento de los pliegos por el poder adjudicador.

7.8.3.- Procedimiento para la solicitud de revocación

El suscriptor puede ponerse en contacto con EADTrust y solicitar la revocación de un certificado. EADTrust le informará sobre cómo formalizar su solicitud.

El certificado puede ser revocado en cualquier momento y se debe revocar en todos los casos de pérdida o robo.

Se registra y archiva la solicitud de revocación autenticada y la información que justifica la revocación.

Si la revocación es solicitada por otra persona que no sea el solicitante, suscriptor o titular de la clave, antes o simultáneamente a la revocación, EADTrust informará al propietario de la clave del certificado y al suscriptor sobre la revocación de su certificado y especificando el motivo de la revocación.

El solicitante puede solicitar la revocación del certificado a través de los siguientes canales:

a) En línea, cumplimentando el formulario de solicitud de revocación disponible en la dirección www.eadtrust.eu
b) Por correo electrónico con solicitud firmada electrónicamente utilizando un certificado cualificado.
c) Por correo postal dirigido al domicilio de EADTrust, enviando la solicitud de revocación de certificado firmada y validada ante notario.
d) Por un sistema de entrega certificada cualificada que acredite la identidad del remitente, que debe coincidir con uno de los sujetos legitimados para solicitar la revocación.

Posteriormente, se le darán indicaciones al solicitante para que agende una cita con la Autoridad de Registro de EADTrust con el fin de verificar la identidad del solicitante de la revocación. Este proceso se llevará a cabo mediante videoconferencia o firma electrónica cualificada.

Una vez comprobado que la solicitud de revocación cumple con los requisitos definidos en esta Política y en la Declaración de Prácticas de EADTrust, se procederá a la revocación del certificado.

En el caso de licitaciones se tendrán en cuenta las condiciones establecidas por el poder adjudicador.

7.8.4.- Periodo de gracia para comprobar certificados revocados

Una vez que la revocación haya sido debidamente procesada por la RA, la información de revocación estará disponible a través del servicio OCSP[7].

El período de precaución o período de gracia que corresponda aplicar para la validación de los certificados es el máximo tiempo transcurrido entre renovaciones de CRL (cuando se aplica este procedimiento para comprobar si un certificado está revocado).

En la relación de firmas electrónicas, este periodo podrá ser, desde el momento en que se realiza la firma o el sellado de tiempo, como mínimo, el tiempo máximo permitido para el refresco completo de las CRLs (CertificateRevocationLists)

[7] IETF RFC 6960 Online Certificate Status Protocol – OCSP

o el tiempo máximo de actualización del estado del certificado en el servicio OCSP (Online Certificate Status Protocol). Esta definición tendrá en cuenta también la posibilidad de que estos tiempos varíen según el Prestador de Servicios de Certificación. El período de gracia recomendado es de 24 horas.

EADTrust mantiene, en las CRLs, información sobre certificados revocados hasta la fecha de caducidad. No obstante, mantendrá disponible, más allá de la fecha de caducidad, un repositorio de las CRLs anteriores que permitirá comprobar si un certificado se revocó antes de su fecha de caducidad con esa información histórica. Este repositorio mantendrá CRL de hasta 1900 días de antigüedad.

7.8.5.- Tiempo en el que una CA debe procesar la solicitud de revocación

Para los certificados de entidad final. El periodo de revocación desde que EADTrust o una RA tiene conocimiento autenticado de la revocación de un certificado, ésta se produce de manera inmediata, como máximo 10 minutos tras la finalización de la comunicación que da noticias de las razones de la revocación, incorporándose en la próxima CRL a emitir y en la base de datos de la plataforma de gestión que consulta el respondedor OCSP.

7.8.6.- Requisitos de comprobación de revocación para las partes que confían

La comprobación del estado de los certificados es obligatoria para cada uso del certificado, ya sea consultando el servicio OCSP o la lista de revocación de certificados (CRL).

EADTrust suministra información a los verificadores sobre cómo y dónde encontrar las CRL y el servicio OCSP correspondientes, en particular en el campo AIA (Authority Information Access) del certificado y en el campo “CRL Distribution Point”.

7.8.7.- Frecuencia de emisión de la CRL

EADTrust emite inmediatamente una Lista de Revocación de Certificados (en adelante CRL, en inglés) en el momento en que se revoca un certificado.

La CRL contiene el tiempo estipulado para la emisión de una nueva CRL, aunque se puede emitir una CRL antes del tiempo indicado en la anterior. Si no hay revocaciones, la lista de revocación de certificados se regenera diariamente.

La CRL para los certificados de entidad final se emite cada 24 horas o como máximo 10 minutos más tarde desde que se confirma una revocación. La CRL para los certificados de CA (ARL) se emite cada 12 meses o cuando se produce una revocación.

Los certificados revocados que caducan no se mantienen en la CRL. No obstante, se publica cada día una CRL que se mantiene en un repositorio hasta un máximo de 1900 días. Además, se conservan todos los certificados caducados (revocados o no) en el registro interno de EADTrust por un período total de 10 años adicionales, contados desde la fecha de caducidad.

No se generan “Last CRLs”. Si una CRL caduca y no se ha emitido otra en el período estipulado (fecha en el campo NextUpdate), no se emitirá ninguna posterior. En caso de que se revoque una CA, se revocarán todos los certificados y se emitirá una CRL con todos los certificados revocados.

7.8.8.- Actualización de las CRLs

El tiempo máximo de latencia, es decir, el tiempo que transcurre tras la finalización de la comunicación que da noticias de las razones de la revocación, hasta que la información está disponible en el servicio OCSP o en la lista CRL se establece en 10 minutos.

7.8.9.- Servicios de estado de certificado

EADTrust proporciona a las Entidades Usuarias un servicio de comprobación de certificados en tiempo real basado en OCSP (Online CertificateStatusProtocol).

Este servicio está disponible las 24 horas del día, los 7 días de la semana. Conforme establece el Reglamento (UE) 910/2014 eIDAS, este servicio se ofrece de manera gratuita.

7.8.10.- Recuperación de Certificados

EADTrust no contempla en ningún caso la recuperación de certificados. En caso de que el propietario de un certificado haya perdido el acceso al mismo, será necesario generar uno nuevo, revocando previamente el anterior.

8.- Perfiles de Certificado

Los certificados incluyen como mínimo, los siguientes campos:

- Número de serie, que es un código único con respecto al nombre distinguido del emisor.
- Algoritmo de firma.
- El nombre distinguido del emisor.
- Inicio de validez del certificado, en Tiempo Coordinado Universal, codificado conforme a la RFC 3280.
- Fin de validez del certificado, en Tiempo Coordinado Universal, codificado conforme a la RFC 3280
- Nombre distinguido del sujeto.
- Clave pública del sujeto, codificada de acuerdo con RFC 3280
- Firma, generada y codificada, de acuerdo con RFC 3280 los certificados son conformes con las siguientes normas:
    - RFC 3280: Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile, April 2002
    - ITU-T Recommendation X.509 (1997): Information Technology – Open Systems Interconnection - The Directory: Authentication Framework, June 1997, con sus actualizaciones y correcciones posteriores.

8.1.1.- Extensiones de certificado

Las extensiones utilizadas dependiendo del perfil en cada caso son:

- Authority key Identifier.
- subjectKeyIdentifier.
- basicConstraints.
- keyUsage.
- certificatePolicies.
- subjectAltName.
- issuerAltName.
- extKeyUsage.
- cRLDistributionPoint.
- Authority Information Access.

8.2.- Perfiles de Certificados de Entidad Final

8.2.1.- Perfil de certificado cualificado de web “Domain Validated” (QWAC)

Campos/Extensiones	Crítico	Contenido
Versión		3
serialNumber		Unique non-sequential positive number of minimum length 64 bits
Signature		Sha256WithRSAEncryption ó ecdsa-with-SHA256 ó ecdsa-with-SHA384
Issuer		Same as the Subject field of the issuing CA certificate
Validity		2 años
Subject		
OrganizationalUnit		Type of web certificate
subjectPublicKeyInfo		RSA 2048 bits minimum or ECDSA 256 bits (prime256v1) or 384 bits (secpr384r1)
Extensions		
subjectAltName		
dnsName		DNS name(s)
extendedKeyUsage		serverAuth, clientAuth

Campos/Extensiones	Crítico	Contenido
subjectKeyIdentifier		Derived from the result of applying the hash to the public key of the subject
authorityKeyIdentifier		Derived from the result of applying the hash to the Public key of the issuing CA
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.0.41241
cpsURI		http://policy.eadtrust.eu
userNotice		European Agency of Digital Trust, S.L. EU qualified website authentication certificates.
policyIdentifier		0.4.0.194112.1.4 (ETSI QCP-w)
policyIdentifier		2.23.140.1.2.1 (CAB/FORUM DV)
cRLDistributionPoints		http://crl.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eaddvov<Año>.crl
authorityInfoAccess		
calssuers		http://ca.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eaddvov<Año>.crt
Ocsp		http://ocsp.eadtrust.eu
basicConstraint	Crítica	CA false
qcStatements		
QcRetentionPeriod		15 years
QcCompliance		Present
QcType		id-etsi-qct-web
keyUsage	Crítica	digitalSignature, keyEncipherment
CT RFC6962		Certificate Transparency

Este tipo de certificados se expiden bajo las jerarquías cualificadas de web (QWAC) de domain validation y organization validation y admite diferentes variantes.

8.2.2.- Perfil de certificado cualificado de web "Organization Validated" (QWAC)

Campos/Extensiones	Crítico	Contenido
version		3
serialNumber		Unique non-sequential positive number of minimum length 64 bits
signature		Sha256WithRSAEncryption or ecdsa-with-SHA256 or ecdsa-with-SHA384
issuer		Same as the Subject field of the issuing CA certificate
validity		2 años
subject		
OrganizationalUnit		Type of web certificate
OrganizationName		Organization Name
LocalityName		Locality Name
StateOrProvinceName		State or province name
CountryName		CountryName
subjectPublicKeyInfo		RSA 2048 bits minimum or ECDSA 256 bits (prime256v1) or 384 bits (secpr384r1)
Extensions		
subjectAltName		
dnsName		DNS name(s)
extendedKeyUsage		serverAuth, clientAuth
subjectKeyIdentifier		Derived from the result of applying the hash to the public key of the subject
authorityKeyIdentifier		Derived from the result of applying the hash to the Public key of the issuing CA
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.0.41242
cpsURI		http://policy.eadtrust.eu
userNotice		European Agency of Digital Trust, S.L. EU qualified website authentication certificates.
policyIdentifier		0.4.0.194112.1.4 (ETSI QCP-w)
policyIdentifier		2.23.140.1.2.2 (CAB/FORUM OV)
cRLDistributionPoints		http://crl.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eaddvov<Año>.crl
authorityInfoAccess		
calssuers		http://ca.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eaddvov<Año>.crt
ocsp		http://ocsp.eadtrust.eu
basicConstraint	Crítica	CA false

Campos/Extensiones	Crítico	Contenido
qcStatements		
QcCompliance		Present
QcType		id-etsi-qct-web
QcRetentiodPeriod		15
keyUsage	Crítica	digitalSignature, keyEncipherment
CT RFC6962		Certificate Transparency

Este tipo de certificados se expiden bajo las jerarquías cualificadas de web (QWAC) de domain validation y organization validation y admite diferentes variantes.
Los certificados OV pueden ser multidominio y se pueden emitir con calificadores de subdominio de tipo “wildcard” (*).

8.2.3.-Perfil de certificado cualificado de web “Extended Validation” (QWAC)

Campos/Extensiones	Crítico	Contenido
version		3
serialNumber		Unique non-sequential positive number of minimum length 64 bits
signature		Sha256WithRSAEncryption or ecdsa-with-SHA256 or ecdsa-with-SHA384
issuer		Same as the Subject field of the issuing CA certificate
validity		2 años
subject		
OrganizationalUnit		Type of web certificate
businessCategory		Private Organization, Government Entity, Business Entity or Non-Commercial Entity
jurisdictionCountryName		Country of Jurisdiction of Incorporation or Registration Field
jurisdictionStOrProvName		State or Province of Jurisdiction of Incorporation or Registration Field
jurisdictionLocalityName		Locality of Jurisdiction of Incorporation or Registration Field
OrganizationName		Organization Name
LocalityName		Locality Name
StateOrProvinceName		State or province name
CountryName		CountryName
serialNumber		Registration Number
subjectPublicKeyInfo		RSA 2048 bits minimum or ECDSA 256 bits (prime256v1) or 384 bits (secpr384r1)
Extensions		
subjectAltName		
dnsName		DNS name(s)
extendedKeyUsage		serverAuth, clientAuth
subjectKeyIdentifier		Derived from the result of applying the hash to the public key of the subject
authorityKeyIdentifier		Derived from the result of applying the hash to the Public key of the issuing CA
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.0.41244
cpsURI		http://policy.eadtrust.eu
userNotice		European Agency of Digital Trust, S.L. EU qualified website authentication certificates.
policyIdentifier		0.4.0.194112.1.4 (ETSI QCP-w)
policyIdentifier		2.23.140.1.1 (CAB/FORUM EV)
cRLDistributionPoints		http://crl.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadevpsd2<Año>.crl
authorityInfoAccess		
caIssuers		http://ca.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadevpsd2<Año>.crt
ocsp		http://ocsp.eadtrust.eu
basicConstraint	Crítica	CA false
qcStatements		
QcCompliance		Present
QcType		id-etsi-qct-web
QcRetentiodPeriod		15
keyUsage	Crítica	digitalSignature, keyEncipherment

Campos/Extensiones	Crítico	Contenido
CT RFC6962		Certificate Transparency

Este tipo de certificados se expiden bajo las jerarquías cualificadas de web (QWAC) de Extended validation y PSD2 (QWAC) y admite diferentes variantes.

Los certificados EV pueden ser multidominio pero NO se pueden emitir con calificadores de subdominio de tipo "wildcard" (*).

8.2.5.- Perfil de certificado cualificado de sede electrónica administrativa "Organization Validated" (QWAC) con nivel de aseguramiento medio/sustancial

Campos/Extensiones	Crítico	Contenido
version		3
serialNumber		integer positivo, no mayor 20 octetos *
signature		SHA-2 con RSA.
issuer		Mismo Subject que el del certificado emisor. Country Common Name Organization
validity		372 días (maximun 397 days)
subject		
OrganizationalUnit		OU= "SEDE ELECTRONICA"
OrganizationalUnit		El nombre descriptivo de la sede. OU= p. ej: PUNTO DE ACCESO GENERAL
OrganizationName		Denominación (nombre "oficial" de la organización) del suscriptor de servicios de certificación (custodio del certificado)
Common Name		Denominación de nombre de dominio (DNS) donde residirá el certificado. CN= p. ej: administracion.gob.es
LocalityName		Ciudad
StateOrProvinceName		State or province name
CountryName		Estado cuya ley rige el nombre, que será ES ("España") por tratarse de entidades públicas.
serialNumber		El NIF de la entidad responsable. SerialNumber = p. ej: S2833002. Size [RFC 5280] 64
Organization Identifier		Identificador de la organización. Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad) OrganizationIdentifier p. ej: VATES-S2833002.
subjectPublicKeyInfo		RSA 2048 bits minimum
Extensions		
subjectAltName		
dnsName		DNS name(s)
extendedKeyUsage		serverAuth
subjectKeyIdentifier		Identificador de la clave pública del suscriptor o poseedor de claves (derivada de utilizar la función de Hash sobre la clave pública del sujeto). Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.
authorityKeyIdentifier		Medio para identificar la clave pública correspondiente a la clave privada utilizada para firmar un certificado, por ejemplo, en los casos en que el emisor tiene múltiples claves de firma.
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.0.41245
cpsURI		http://policy.eadtrust.eu

Campos/Extensiones	Crítico	Contenido
userNotice		Ej: "Certificado cualificado de sede electrónica, nivel medio/sustancial. Consulte las condiciones de uso en " + URL de la DPC o, en su caso, documento legal de tercero
policyIdentifier		0.4.0.194112.1.4 (ETSI QCP-w)
policyIdentifier		2.23.140.1.2.2 (CAB/FORUM OV)
policyIdentifier		2.16.724.1.3.5.5.2
cRLDistributionPoints		http://crl.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eaddvov<Año>.crl
authorityInfoAccess		
caIssuers		http://ca.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eaddvov<Año>.crt
ocsp		http://ocsp.eadtrust.eu
basicConstraint	Crítica	CA false
qcStatements		
QcCompliance		Indicación de certificado cualificado
QcType		id-etsi-qct-web
QcRetentiodPeriod		Integer:=15 ([ETSI EN 319 412-5] describe el periodo de conservación de toda la información relevante para el uso de un certificado, tras la caducidad de este)
QcPDS		Lugar donde se encuentra la declaración PDS
semnaticsId-Legal		Para indicar semántica de persona jurídica definida por la EN 319 412-1
keyUsage	Crítica	digitalSignature, keyEncipherment
CT RFC6962		Certificate Transparency (cuando estemos en CA/B Forum)

Los certificados OV pueden ser multidominio y se pueden emitir con calificadores de subdominio de tipo “wildcard” (*).

8.2.4.- Perfil de certificado cualificado de sede electrónica administrativa “Extended Validation” (QWAC) con nivel de aseguramiento Alto

Campos/Extensiones	Crítico	Contenido
version		3
serialNumber		integer positivo, no mayor 20 octetos
signature		SHA-2 con RSA.
issuer		Mismo Subject que el del certificado emisor. Campos Country Common Name Organization
validity		372 días (maximun 397 days)
subject		
OrganizationalUnit		OU= “SEDE ELECTRONICA”
OrganizationalUnit		El nombre descriptivo de la sede. OU= p. ej: PUNTO DE ACCESO GENERAL
businessCategory		businessCategory = “Government Entity”
jurisdictionCountryName		jurisdictionCountryName= “ES”
jurisdictionStOrProvName		State or Province of Jurisdiction of Incorporation or Registration Field
jurisdictionLocalityName		Locality of Jurisdiction of Incorporation or Registration Field
OrganizationName		Denominación (nombre “oficial” de la organización) del suscriptor de servicios de certificación (custodio del certificado)
Common Name		Denominación de nombre de dominio (DNS) donde residirá el certificado. CN= p. ej: administracion.gob.es
LocalityName		Ciudad
StateOrProvinceName		State or province name

Campos/Extensiones	Crítico	Contenido
CountryName		Estado cuya ley rige el nombre, que será ES ("España") por tratarse de entidades públicas.
serialNumber		El NIF de la entidad responsable. SerialNumber = p. ej: S2833002. Size [RFC 5280] 64
Organization Identifier		Identificador de la organización. Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad) OrganizationIdentifier p. ej: VATES-S2833002.
subjectPublicKeyInfo		RSA 2048 bits
Extensions		
subjectAltName		
dnsName		DNS name(s)
extendedKeyUsage		serverAuth
subjectKeyIdentifier		Identificador de la clave pública del suscriptor o poseedor de claves (derivada de utilizar la función de Hash sobre la clave pública del sujeto). Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.
authorityKeyIdentifier		Medio para identificar la clave pública correspondiente a la clave privada utilizada para firmar un certificado, por ejemplo en los casos en que el emisor tiene múltiples claves de firma.
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.0.41246
cpsURI		http://policy.eadtrust.eu
userNotice		P. ej: "Certificado cualificado de sede electrónica, nivel alto. Consulte las condiciones de uso en " + URL de la DPC o, en su caso, documento legal de tercero
policyIdentifier		0.4.0.194112.1.4 (ETSI QCP-w)
policyIdentifier		2.23.140.1.1 (CAB/FORUM EV)
policyIdentifier		2.16.724.1.3.5.5.1
cRLDistributionPoints		http://crl.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadevpsd2<Año>.crl
authorityInfoAccess		
caIssuers		http://ca.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadevpsd2<Año>.crt
ocsp		http://ocsp.eadtrust.eu
basicConstraint	Crítica	CA false
qcStatements		
QcCompliance		Indicación de certificado cualificado
QcType		id-etsi-qct-web
QcRetentiodPeriod		Integer:=15 ([ETSI EN 319 412-5] describe el periodo de conservación de toda la información relevante para el uso de un certificado, tras la caducidad de este) OID 0.4.0.1862.1.3
QcPDS		Lugar donde se encuentra la declaración PDS
semanticsId-Legal		Para indicar semántica de persona jurídica definida por la EN 319 412-1
keyUsage	Crítica	digitalSignature, keyEncipherment
CT RFC6962		Certificate Transparency (cuando estemos en CA/B Forum)
cabfOrganizationIdentifier		(OID: 2.23.140.3.1) If the subject:organizationIdentifier is present, this field MUST be present.

Los certificados EV pueden ser multidominio pero NO se pueden emitir con calificadores de subdominio de tipo “wildcard” (*).

9.- Requisitos Empresariales y Legales

9.1.- Tarifas

EADTrust recibirá las contraprestaciones económicas correspondientes, de acuerdo con las tarifas aprobadas por su Órgano de Dirección.

Las tarifas se recogen en el documento de términos y condiciones para cada tipo de certificado o servicio.

En el caso de concursos y licitaciones podrán establecerse otros precios en cumplimiento de los pliegos publicados por el poder adjudicador.

9.2.- Consideraciones de protección de datos de carácter personal

Todos los datos correspondientes a las personas físicas están sujetos a la normativa sobre protección de datos de carácter personal. De conformidad con lo establecido en el Reglamento (UE) 679/2016 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (Texto pertinente a efectos del EEE), también conocido como RGPD.

En España, es de aplicación lo dispuesto en la Ley Orgánica 3/2018, de 5 de diciembre de 2018, de protección de datos personales y garantía de derechos digitales, también conocida como LOPD-GDD.

Conforme establece la citada legislación de protección de datos, se consideran datos de carácter personal cualquier información relativa a personas físicas identificadas o identificables.

La información personal que no haya de ser incluida en los certificados y en el mecanismo indicado de comprobación del estado de los certificados, es considerada información personal de carácter privado.

Los siguientes datos son considerados información privada:

- Solicitudes de certificados, aprobadas o denegadas, así como toda otra información personal obtenida para la expedición y mantenimiento de certificados, excepto las informaciones indicadas en la sección correspondiente.
- Claves privadas generadas y/o almacenadas por la Entidad de Certificación.
- Cualquier otra información que pudiera identificarse como “Información privada”.

Los datos recabados por el prestador de servicios electrónicos de confianza tendrán la consideración legal que corresponda a su naturaleza, siendo normalmente datos de nivel básico. La información confidencial de acuerdo con la normativa de protección de datos es protegida de su pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizado. A estos efectos EADTrust considera pública y no confidencial la siguiente información:

- Los certificados expedidos.
- Los usos y límites económicos reseñados en el certificado.
- El periodo de validez del certificado, así como la fecha de emisión del certificado y la fecha de caducidad.
- El número de serie del certificado.
- Los diferentes estados o situaciones del certificado y la fecha del inicio de cada uno de ellos, en concreto: pendiente de generación o entrega, válido, revocado, suspendido o caducado y el motivo que provocó el cambio de estado.
- Las listas de revocación de certificados, así como el resto de informaciones de estado de revocación.

Los certificados de sitio web publicados en el registro de “Certificate Transparency” pueden ser descargados y analizados por terceros, normalmente en contextos de gestión de debida diligencia en la expedición de certificados y control de calidad.

9.2.1.- Consentimiento para usar datos de carácter personal

EADTrust S.L informa que los datos personales a los que tenga acceso en el marco de la prestación de sus servicios serán incorporados al registro de actividades de tratamiento del que es Responsable. EADTrust fundamenta el tratamiento de datos concretamente dependiendo de la finalidad para la cual los solicite en: el interés legítimo que tiene en responder solicitudes de información sobre sus servicios, la ejecución de un contrato o en el consentimiento expreso del titular del dato en los casos en que este sea requerido. Los titulares de datos pueden retirar ese consentimiento en cualquier momento.

Los datos recabados son los mínimos necesarios para la prestación de los servicios y se conservan por los períodos que establece la Ley. No se ceden a terceros, salvo obligación legal; ni se realizan perfiles o se toman decisiones automatizadas en base a estos datos.

EADTrust le informa igualmente que, en caso de solicitar los servicios amparados en esta DPC por vía telefónica, su voz podrá ser grabada durante las conversaciones telefónicas que mantenga con la Autoridad de Registro (AR) o la Autoridad de Certificación (AC), con el fin de permitir una tramitación segura de la solicitud de emisión o revocación de certificados. Previo a la grabación se le ofrecerá la información básica de protección de datos estipulada en el RGPD y se le recabará su consentimiento expreso. Los datos personales recabados por esta vía se incorporarán al registro de actividades de tratamiento del que es responsable EADTrust.

Cuando el servicio de emisión o revocación de certificados se provea en la modalidad de verificación y autenticación de identidad mediante video conferencia o videograbación, EADTrust requerirá captar la imagen y la voz del Solicitante. La base legal para este tratamiento es la ejecución del contrato de prestación de servicios en esta modalidad conforme dispone el artículo 6.1 b) del Reglamento General de Protección de Datos. Estos datos son necesarios para la adecuada prestación del servicio y se incorporarán al registro de actividades de tratamiento de EADTrust.
Para más información sobre el ejercicio de los derechos al amparo del RGPD y sobre el tratamiento de sus datos personales por EADTrust consulte la nota legal más extensa, incluida en:ww.eadtrust.rgpd.de

9.2.2.- Comunicación a terceros de datos de carácter personal

Los datos de carácter personal solo podrán ser comunicados a terceros, siempre que el titular del derecho lo consienta expresamente o por obligación legal de EADTrust.

9.3.- Responsabilidad contractual y extracontractual

9.3.1.- Limitación de responsabilidad

EADTrust no asumirá responsabilidad alguna por los daños derivados o relacionados con la no ejecución o la ejecución defectuosa de las obligaciones del titular de un certificado.

EADTrust no será responsable de la utilización incorrecta de los Certificados ni de las claves, ni de cualquier daño indirecto que pueda resultar de la utilización de los Certificados.

EADTrust no será responsable de los daños que puedan derivarse de aquellas operaciones en que se hayan incumplido las limitaciones de uso del Certificado.

EADTrust no asumirá responsabilidad alguna por la no ejecución o el retraso en la ejecución de cualquiera de las obligaciones contenidas en esta Política si tal falta de ejecución o retraso fuera consecuencia de un supuesto de fuerza mayor, caso fortuito o, en general, cualquier circunstancia en la que no se pueda tener un control directo.

EADTrust no será responsable del contenido de aquellos documentos firmados electrónicamente por los titulares de certificados.

EADTrust no garantiza los algoritmos criptográficos ni responderá de los daños causados por ataques exitosos externos a los algoritmos criptográficos usados, si guardó la diligencia debida de acuerdo al estado actual de la técnica, y procedió conforme a lo dispuesto en esta Política y en la normativa de aplicación.

9.3.2.- Responsabilidades

EADTrust responderá en el caso de incumplimiento de sus obligaciones según se indica en el Reglamento (UE) 910/2014 del Parlamento europeo y del Consejo, de 23 de julio de 2014, y en la normativa reguladora de los servicios electrónicos de confianza, así como en la presente Política.

EADTrust responderá por los daños y perjuicios que causen al firmante o terceros de buena fe cuando incumpla las obligaciones que impone el Reglamento (UE) 910/2014 del Parlamento europeo y del Consejo, de 23 de julio de 2014 y la próxima Ley reguladora de determinados aspectos de los servicios electrónicos de confianza.

La responsabilidad del prestador de servicios de confianza regulada en la ley será exigible conforme a las normas generales sobre la culpa contractual o extracontractual, según proceda, si bien corresponderá al prestador de servicios de confianza demostrar que actuó con la diligencia profesional que le es exigible siendo responsable de los perjuicios causados de forma deliberada o por negligencia a cualquier persona física o jurídica en razón del incumplimiento de las obligaciones establecidas en el Reglamento 910/2014.

Se presumirá la intencionalidad o la negligencia de un prestador cualificado de servicios de confianza salvo cuando el prestador cualificado de servicios de confianza demuestre que los perjuicios a que se refiere el párrafo primero del artículo 13 del Reglamento 910/2014 se produjeron sin intención ni negligencia por su parte.

Cuando EADTrust, como prestador cualificado de servicios de confianza, informe debidamente a los suscriptores con antelación sobre las limitaciones de la utilización de los servicios que presta y estas limitaciones sean reconocibles para un tercero, el prestador de servicios de confianza no será responsable de los perjuicios producidos por una utilización de los servicios que vaya más allá de las limitaciones indicadas.

De manera particular, EADTrust como prestador de servicios de confianza responderá de los perjuicios que se causen al firmante o a terceros de buena fe por la falta o el retraso en la inclusión en el servicio de consulta sobre la vigencia de los certificados

EADTrust como prestador de servicios de certificación asumirá toda la responsabilidad frente a terceros por la actuación de las personas en las que deleguen la ejecución de alguna o algunas de las funciones necesarias para la prestación de servicios de confianza.

9.3.3.- Entidad de registro

La Autoridad de Registro asumirá toda la responsabilidad sobre la correcta identificación de los solicitantes y la comprobación de sus datos, con las mismas limitaciones que se establecen para la Autoridad de Certificación.

9.3.4.- Responsabilidades del titular de los certificados

El titular de los certificados asumirá toda la responsabilidad y riesgos derivados de la fiabilidad y seguridad del puesto de trabajo, equipo informático o medio desde el cual emplee su certificado.

Así mismo el titular de los certificados se responsabilizará de los riesgos derivados de la aceptación de una conexión segura sin haber realizado previamente la preceptiva verificación de la validez del certificado exhibido por el prestador de servicios.

Los procedimientos para contrastar la seguridad de la conexión con dicho prestador de servicios deberán ser proporcionados por éste al titular del certificado, por ejemplo, mediante técnicas de OCSPStapling (es decir haciendo uso de la extensión “TLS CertificateStatusRequest” descrita en la sección 8 de la norma **RFC 6066**)[8]

[8] La norma RFC 6961 “The Transport Layer Security (TLS) – Multiple Certificate Status Request Extension” contempla múltipes respuestas, en el establecimiento de sesiones TLS, lo que permite validar los certificados de las CAs intermedias de la cadena de confianza.

Un certificado (en el sentido de instrumento que contempla la gestión de una clave privada) es un documento personal e intransferible emitido por EADTrust. Su titular está obligado a su custodia y la del código PIN o clave que habilita su uso, y es responsable de la conservación del mismo. No puede cederlos a otras personas.

9.3.5.- Exención de responsabilidades de EADTrust

EADTrust no asume ninguna responsabilidad por perjuicios ocasionados en las siguientes circunstancias:

- En caso de guerra, catástrofes naturales o cualquier otro supuesto de caso fortuito o de fuerza mayor: alteraciones de orden público, huelga en los transportes, corte de suministro eléctrico y/o telefónico, virus informáticos, deficiencias en los servicios de telecomunicaciones o el compromiso de las claves asimétricas derivado de un riesgo tecnológico imprevisible.
- Ocasionados durante el periodo comprendido entre la solicitud de un certificado y su entrega al usuario.
- Ocasionados durante el periodo comprendido entre la revocación de un certificado y el momento de publicación de la siguiente CRL.
- Ocasionados por el uso de certificados que exceda los límites establecidos por los mismos y esta Política.
- Ocasionado por el uso indebido o fraudulento de los certificados o CRLs emitidos por la infraestructura de Certificación de EADTrut.
- Ocasionados por el mal uso de la información contenida en el certificado.
- La Autoridad de Certificación no será responsable del contenido de aquellos documentos firmados electrónicamente ni de cualquier otra información que se utilice en un proceso de autenticación en la que esté involucrado un certificado emitido por ella.

9.3.6.- Perjuicios derivados del uso de servicios y certificados

A excepción de lo establecido por las disposiciones de la presente Política, y lo determinado por Ley, EADTrust no asume ningún otro compromiso ni brinda ninguna otra garantía, así como tampoco asume ninguna otra responsabilidad ante titulares de certificados o terceros que confían en los certificados.

9.3.7.- Seguro de responsabilidad civil

EADTrust cuenta con un Seguro de Responsabilidad Civil adecuado a sus actividades, según lo dispuesto en la normativa reguladora de los servicios electrónicos de confianza.

9.3.8.- Quejas. Reclamaciones y jurisdicción

En caso de una queja del usuario o de un tercero interesado, este podrá dirigir su queja al mail: info@eadtrust.eu o por correo postal; aportando copia de su identificación; así como todos los documentos y toda la información que considere oportuna para fundamentar su queja.

La CA de EADTrust en un plazo de 48 horas le remitirá por la misma vía de comunicación utilizada por el solicitante, un informe fundamentado de respuesta.

El plazo definido anteriormente podrá ser extendido en caso de que la resolución de la queja revista complejidad para su solución. Esta ampliación será comunicada al usuario.

En caso de que el usuario no esté conforme con la resolución de la queja. Este podrá presentar una solicitud de recurso de apelación ante la Dirección General de EADTrust. Para ello solo deberá comunicarse vía e mail a info@eadtrust.eu , indicando en el asunto que se trata de un recurso de apelación, también podrá emplearse la vía del correo postal.

Para la resolución de apelaciones se seguirá el procedimiento descrito anteriormente.

Las reclamaciones dirigidas a EADTrust se gestionarán de forma directa para intentar llegar a un acuerdo que resuelva el incidente o, en su caso, comprobar si es una cobertura incluida en el seguro. La actividad de EADTrust se rige por la Ley española y por los Tribunales de Madrid, salvo que el usuario ostente la condición de consumidor, lo que redundará en que se aplique la normativa de protección de consumidores.