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

Septiembre 2019
Versión 2.3

Tabla de Contenido

1.- Introducción

EADTrust European Agency of Digital Trust, S.L. (en adelante, EADTrust), es un Prestador de Servicios Electrónicos de Confianza radicado en Madrid, España, que opera bajo la supervisión del Ministerio de Economía y Empresa (Secretaría de Estado para el Avance Digital), si bien la denominación del organismo supervisor puede cambiar por criterios políticos e incluso adscribirse a diferente Ministerio. En el ejercicio de su actividad empresarial EADTrust ha definido sus prácticas y políticas según los requisitos del REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y que deroga la Directiva 1999/93/CE (en adelante, eIDAS) y los estándares internacionales establecidos en ETSI.

EADTrust, presta servicios electrónicos de confianza cualificados (definidos en el Reglamento UE 910/2014) y no cualificados (basados en otros enfoques de uso de la criptografía y de la gestión de evidencias digitales). La indicación de servicios "no cualificados" simplemente identifica los servicios de confianza no previstos en el citado Reglamento eIDAS.

El documento principal en el que se recogen los procedimientos de EADTrust en relación con la emisión de certificados y la provisión de otros servicios electrónicos de confianza es la Declaración de Prácticas de Servicios de Confianza (DPC), basada en parte en la norma RFC 3647 del año 2003. Es el documento más completo y se recomienda su lectura.

Este documento de Política de Certificación se limita a indicar la aplicabilidad de ciertos tipos de certificados (agrupados por similitud) a una comunidad o un uso concretos[1]

Su finalidad es detallar para este tipo de certificados lo definido de forma genérica en la DPC de EADTrust, en los documentos específicos del CA/Browser Forum Baseline Requirements (en adelante BR) y EV guidelines (en adelante EVBR) para la emisión de certificados para sitios web) y en las especificaciones de ETSI (www.etsi.org).

EADTrust sigue las siguientes políticas de certificación establecidas por ETSI:

- DVCP (Domain Validation Certificates Policy)
- OVCP (Organizational Validation Certificates Policy)
- EVCP (Extended Validation Certificates Policy)

En relación con la técnica de registro de certificados “Certificate Transparency”, los certificados SSL emitidos se publicarán en el servicio CT de los proveedores de Log Servers a los cuales EADTrust tiene acceso.

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

2.- Participantes en la PKI

2.1.- Autoridades de Certificación

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:

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.

2.2.- Autoridades de Registro

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

Estas RAs son entidades que actúan de acuerdo con esta Política de Certificación, junto con una relación escrita formal y contractual con 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 y se está implementando la posibilidad de inscripción mediante videoconferencia (también descrita como mediante telepresencia) o videograbación ("digital onboarding". La plataforma a utilizar, cumplirá con la normativa española publicada por el Servicio de Prevención de Blanqueo de Capitales (SEPBLAC) para videoidentificación[2] y videoconferencia[3] y la Directiva (UE) 2015/2366 (PSD 2), que se utilizará incluso en los servicios de iniciación de pagos como medio para proporcionar autenticación fuerte de los clientes.

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 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.

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

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:

- Suscriptor del certificado y, como tal, el propietario de la clave.
- El propietario de la clave, en representación de un suscriptor del certificado.
- Representante, con funciones de representación del suscriptor del certificado, que no debe tener acceso a las claves del certificado.

Suscriptores del Certificado

El suscriptor de un certificado es la persona física o 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.

Representante del solicitante

Cualquier persona física o 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 npersona 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 Raiz, y que pueden identificar el punto de consulta de validez de certificados por el servicio OCSP, o, cuando corresponda, por la lista CRL.

En el caso de los certificados cualificados, deben poder identificar las autoridades incluidas en las listas de confianza TSL administradas por el Organismo de Supervisión correspondiente al país, en España la Secretaría de Estado para el Avance Digital adscrita al Ministerio de Economía y Empresa[4] y por el organismo europeo que consolida las TSL nacionales[5].

Las partes que confían deben conocer y sujetarse a las garantías, límites y responsabilidades aplicables en la aceptación y uso de los certificados en los que confían, y aceptar sujetarse a las mismas. 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.

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 sito 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] https://sede.minetur.gob.es/es-ES/datosabiertos/catalogo/lista-prestadores-tsl
[5] https://ec.europa.eu/digital-single-market/en/eu-trusted-lists-trust-service-providers

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
Dirección de email para PSD2	CA-request@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-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 caducados y revocados, accediendo por puertos diferentes:

Certificados revocados:

- https://dominio.eadtrust.eu: 8443

Certificados caducados:

- https://dominio.eadtrust.eu: 9443

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.

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

Todos los certificados de usuario de entidad final contienen un nombre dado en el campo **Subject Name**. Los atributos especificados en el nombre diferenciado en el campo de Sujeto están contenidos en la sección correspondiente al perfil de certificado. El valor autenticado en el campo **Common Name** es el nombre del propietario de la clave. El campo **subjectAltName** también se utiliza ocasionalmente para situar un nombre que se puede utilizar para identificar el sujeto, pero que es diferente del nombre que aparece en el campo **Subject Name**.

En relación con los Subject (sujeto al que se emite el certificado) se considera los siguientes campos:

- Country: ES (corresponde al código ISO de país, correspondiente al Estado Español).
- Organizational Unit Name: El nombre del tipo de servicio de certificación que se presta.
- Surname: Los apellidos del suscriptor, autorizado por la Entidad de Registro.
- Given Name: El nombre del suscriptor, autorizado por la Entidad de Registro.
- Serial Number: DNI/NIE, del suscriptor, autorizado por la Entidad de Registro, u otro número descrito en la norma EN 319 412-1.
- Common Name: El nombre en texto libre del suscriptor, autorizado por la Entidad de Registro.

La estructura sintáctica y el contenido de los campos de cada certificado emitido por EADTrust, así como su significado semántico, se encuentran descritos en cada uno de los perfiles de certificados, definidos en función de los requerimientos especificados en las normas ETSI correspondientes (412-1 a 5; 411-1 y 2), así como 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.

6.1.2.- Necesidad de que los nombres sean significativos

El nombre del sujeto y el emisor contenidos en un certificado, deben ser significativos en el sentido de que la CA tenga evidencia de la asociación existente entre estos nombres y las entidades a las cuales pertenecen.

Cada certificado digital contiene un conjunto único de atributos de nombre único. Estos atributos incluyen una recopilación del nombre de la persona, nombre de la compañía, unidad organizacional e identificador único. Un sujeto o suscriptor puede tener dos o más certificados con el mismo Nombre Único del Suscriptor.

6.1.3.- Normas para interpretar diferentes formas de nombres

EADTrust atiende a lo estipulado por el estándar X.500 de referencia en la ISO/IEC 9594 **Informationtechnology – Open SystemsInterconnection – TheDirectory: Public-key and attribute certificate frameworks**

- X.509 - ISO/IEC 9594-813
- X.520 -ISO/IEC 9594-614

6.1.4.- Singularidad de los nombres

Los nombres de suscriptores y, en su caso, los nombres de los propietarios de claves son únicos para cada tipo de certificado dentro de la Declaración de prácticas de certificación de EADTrust.

6.2.- Validación inicial 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.

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 de persona física representante, de persona jurídica y 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).

En el caso de certificados expedidos a servidores web, 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.

Si la entidad hace uso en su DNS de las extensiones[6] 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.

En el caso de certificados emitidos a Prestadores de Servicios contemplados en las Directivas de Pagos, se constatará su existencia en el Registro administrado por el Órgano Supervisor (National Competent Authorities).

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.
- Por la Autoridad Competente en los casos previstos en la normativa PSD2.

[6] 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.

La Autoridad Competente podrá iniciar la revocación de certificados PSD2 por e-mail cuando se remita la solicitud desde la dirección designada, sin perjuicio de que se adopten medidas adicionales para comprobar la legitimidad de la solicitud de revocación.

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

7.1.- Solicitud del Certificado

La solicitud de los certificados puede llevarse a cabo on site (personación); no obstante, el servicio podrá ofrecerse también accediendo desde un ordenador o app a la plataforma que está implementando EADTrust para la emisión de certificados (identificación remota).

7.1.1.- Quién puede enviar una solicitud del certificado

- Pueden solicitar un certificado las personas 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.

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, revocación y renovación 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, renovación, reactivación y 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, el operador de la RA mediante el acceso a la plataforma de gestión verifica 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.

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 "Extended Validation" se aplicarán 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.

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 token criptográfico, en una tarjeta inteligente, en HSM o en un soporte de software.

I. **Procedimiento de emisión de certificados expedidos en un HSM:**

- La Autoridad de Registro autentica la validez de la documentación presentada por el solicitante, y audita la generación de la solicitud de certificado en HSM y la solicitud de certificado con formato PKCS#10.
- Tras la autenticación, la Autoridad de Registro solicita el certificado de EADTrust, aportando el fichero en formato PKCS#10.
- Después de comprobar que la solicitud procede de una Autoridad de Registro autorizada, EADTrust emite el certificado según los procedimientos establecidos y lo envía a la Autoridad de Registro
- Después de que la Autoridad de Registro haya comprobado que la solicitud proviene de EADTrust, esta descarga el certificado y lo pone a disposición del solicitante que deberá insertarlos en el dispositivo criptográfico en el que se generó la solicitud.
- Si EADTrust decide no emitir el certificado (incluso cuando los procedimientos de autenticación sean correctos), se notificarán al solicitante los motivos de la decisión.

II. **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 presentada 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.

III. 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 presentada 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

EADTrust notifica al suscriptor sobre la emisión del certificado mediante correo electrónico o SMS, indicando la emisión del certificado.

También podrá notificarse la emisión a través de una App de teléfono móvil si el suscriptor se ha instalado esta App y configura sus preferencias sobre esta forma de notificación.

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

Dependiendo del documento de solicitud del certificado, se especifica tanto la aceptación de las condiciones de uso y como el contrato del suscriptor, a los que se debe dar cumplimiento. Como evidencia, el suscriptor debe firmar una hoja de recepción y aceptación, si bien serán válidas las diferentes formas de prestar consentimiento admitidas en derecho, siempre que generen evidencias digitales de forma semejante para todos los intervinientes. El uso del certificado determina su aceptación.

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"[9]

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.
- Transferirá obligaciones específicas a los propietarios de la clave.
- 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.

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.

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

- Comprobar la validez, suspensión 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[10].
- 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:

- 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

7.6.1.- Circunstancias para la renovación del certificado

El certificado se puede renovar si el certificado no ha expirado o si han transcurrido menos de **2 años** desde su última personación e identificación ante la RA. EADTrust realiza las renovaciones de certificados emitiendo nuevas claves, por lo tanto, el proceso técnico de emisión es igual al que se sigue cuando se realiza una solicitud por primera vez.

7.6.2.- Quién puede solicitar la renovación

Para solicitar la renovación de un certificado, se deben cumplir los requisitos exigidos en la primera expedición.

7.6.3.- Procesamiento de solicitudes de renovación de certificados

El suscriptor puede ponerse en contacto con EADTrust y solicitar su renovación. EADTrust informa en su página web sobre la forma de realizar la solicitud.

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

Se tomarán las siguientes medidas:

- EADTrust podrá comprobar que un certificado está a punto de expirar.
- El suscriptor será informado de que puede renovar su certificado.
- El suscriptor solicitará una cita con la RA por teléfono o por medio del sitio web e incluso podrá firmar la solicitud utilizando su certificado, firmando la renovación de su certificado.
- El certificado se generará siguiendo el procedimiento habitual de emisión.

El certificado generado se entregará al suscriptor.

[10] 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

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

El certificado se considera aceptado si se firmó la solicitud de renovación electrónicamente (en el caso de que se haga de esta manera) o firmando el formulario de entrega y la aceptación ante la RA. También serán válidas las diferentes formas de prestar consentimiento admitidas en derecho, siempre que generen evidencias digitales de forma semejante para todos los intervinientes. El uso del certificado determina su aceptación.

7.6.6.- Publicación del certificado de renovación por la CA

Los nuevos certificados de sitio web pueden ser registrados en repositorios de control de seguridad: Certificate Transparency.

7.6.7.- 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 SSl o TLS) según la normativa "CertificateTransparency"[11].

7.7.- Revocación y suspensión 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.

La suspensión, por su parte, técnicamente se trata como una revocación en la que se indica una causa de suspensión (es decir, es un caso particular de revocación). Sin embargo, la revocación no sería definitiva y podría decidirse finalmente que el certificado se reactiva y se elimina de la lista de certificados revocados.

EADTrust no realiza suspensiones. En caso de que se produzca una circunstancia que pudiera resolverse con la reactivación del certificado, en su lugar se expedirá un nuevo certificado.

7.7.1.- 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.
- Que una Autoridad Competente indique la necesidad de revocar un certificado PSD2.
- 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

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

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.
- Que hayan transcurrido 3 meses desde el momento en que se solicita la certificación sin que se recoja el certificado.
- 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.

7.7.2.- 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 AC.
- En el caso de los certificados para PSD2, los organismos supervisores (Autoridades Competentes).
- Podrá realizarse de oficio si a EADTrust le consta por otra vía que se han producido circunstancias que hagan necesaria la revocación.

7.7.3.- 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 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 revocar el certificado a través de los siguientes canales:

- En línea, en la dirección www.eadtrust.eu o por correo electrónico con solicitud firmada electrónicamente utilizando un certificado cualificado.
- Por correo, enviando la solicitud de revocación de certificado firmada y validada ante notario.
- 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.
- En el caso de los certificados para PSD2, los organismos supervisores (Autoridades Nacionales Competentes) pueden solicitar la revocación mediante el uso de una dirección de e-mail designada para ello, s perjuicio de las comprobaciones adicionales que realice EADTrust para verificar la legitimidad de la solicitud.

7.7.4.- Periodo de gracia para comprobar certificados revocados

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

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)

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, si bien la disponibilidad de la información de revocación a través del servicio OCSP de EADTrust es de como máximo 10 minutos tras la finalización de la comunicación que da noticias de las razones de la revocación.

7.7.5.- 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 donde se alimenta el respondedor OCSP.

7.7.6.- 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".

7.7.7.- 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 una CRL puede ser emitida antes del tiempo indicado en la CRL 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 cuando se produce una revocación.

La CRL para los certificados CA (ARL) se emite cada 12 meses o cuando se produce una revocación.

Los certificados revocados que caducan se eliminan de la CRL. No obstante, se conservan en el registro interno de EADTrust por un período de 10 años adicionales.

7.7.8.- Latencia máxima para 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.

7.7.9.- 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)[14].

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.

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

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

8.3.1.- 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 254 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		1.3.6.1.4.1.501.2.1.1.0.41241
cpsURI		http://policy.eadtrust.eu
userNotice		European Agency of Digital Trust, S.L.

Campos/Extensiones	Crítico	Contenido
		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		
caIssuers		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

8.3.3.- 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 254 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		
caIssuers		http://ca.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eaddvov<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
CT RFC6962		Certificate Transparency

8.3.2.-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 254 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
CT RFC6962		Certificate Transparency

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.

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 fundamentalmente 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. 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.

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:http://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 de la extinción o suspensión de la vigencia del certificado electrónico.

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**)[21]

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

[21] 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.

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.