European Agency of Digital Trust

Política de emisión de certificados de persona física

Área Documental de Operaciones

Tabla de O.I.D.'s		
Certificado	Sin dispositivo Cualificado	Con Dispositivo Cualificado
Persona Física	1.3.6.1.4.1.501.2.1.1.0.41221	1.3.6.1.4.1.501.2.1.1.1.41221
Representante de Persona Jurídica	1.3.6.1.4.1.501.2.1.1.0.41222	1.3.6.1.4.1.501.2.1.1.1.41222
Empleado público aseguramiento sustancial/Medio	1.3.6.1.4.1.501.2.1.1.0.41223	1.3.6.1.4.1.501.2.1.1.1.41223
Empleado público Seudónimo Firma (aseguramiento alto)	N/A	1.3.6.1.4.1.501.2.1.1.1.41224
Empleado público Seudónimo Autenticación (aseguramiento alto)	N/A	1.3.6.1.4.1.501.2.1.1.1.41225

Septiembre 2019
Versión 2.2

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 de2014 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, basada en parte en la norma RFC 3647 del año 2003. Es el documento más completo y se recomienda su lectura.

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

2.- Participantes en la PKI

2.1.- Autoridades de Certificación

Las CAs de EADTrust están organizadas en una jerarquía de dos niveles, con diferentes CA's raíz- root- y CA's subordinadas –SubCA's- adaptadas a las normas actuales y las mejores prácticas del sector.

Se diferencian por algoritmo de clave pública-RSA y ECC, tamaño de la clave y por diferentes usos de los certificados de entidad final, cualificados y no cualificados. Las jerarquías destinadas a emitir certificados de sitio web no emiten certificados de otro tipo para favorecer la interoperabilidad con los requisitos de CAB Forum.

Para certificados cualificados

- RSA Root CA 2048-bit key size size with SHA256 digest algorithm para certificados cualificados.
- RSA Root CA 4096-bit key size with SHA256 digest algorithm para certificados cualificados.
- RSA Root CA 8192-bit key size with SHA512 digest algorithm para certificados cualificados.
- ECC Root CA P-256 with SHA256 digest algorithm para certificados cualificados.
- ECCRoot CA P-384 with SHA384 digest algorithm para certificados 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.

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

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, 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 en un dispositivo cualificado de creación de firma (si es el caso) o mediante fichero cuando no se requiera dispositivo cualificado de creación de firma.
- Conservación de cualquier documentación relevante y relacionada con la emisión del certificado 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 personas físicas que reciban servicios de emisión de certificado, gestión y uso de certificados digitales. Entre otros se incluyen:

- 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.

[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

Suscriptores del Certificado

El suscriptor de un certificado es la persona física que posee el certificado que se vincula con una clave privada.

En los certificados individuales, el suscriptor y el propietario de la clave coinciden. En los certificados en los que ambas figuras no coinciden, (como las entidades y los certificados de las organizaciones), el suscriptor suele ser una persona jurídica y el propietario de la clave es una persona física, representante o empleado autorizado por la organización para recibir y utilizar el certificado.

Propietarios de la clave

El propietario de la clave es una persona física que tiene y puede utilizar exclusivamente las claves criptográficas del certificado.

Incluso si el propietario de la clave suele ser identificado como el firmante en la regulación de la firma electrónica, se designa por su clasificación más genérica, para incluir cualquier otro uso del certificado (como la autenticación o el descifrado).

En caso de que el propietario de la clave y el suscriptor no sean la misma persona, ambos se identificarán correctamente en el certificado, por su nombre legal completo o, si fuera necesario, pseudónimos.

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 pueden o no ser suscriptores dentro de esta PKI, pero, en cualquier caso, se proporcionarán diferentes canales de comunicación, para que puedan (como 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 indentificar 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/

[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

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 firma electrónica cualificados garantizan la identidad del suscriptor y del titular de la clave privada. Cuando se utilizan con dispositivos cualificados de creación de firmas, son adecuados para ofrecer soporte a la firma electrónica cualificada; en otras palabras, una firma electrónica avanzada respaldada en un certificado cualificado y basada en un dispositivo cualificado equivale a una firma manuscrita sin necesidad de satisfacer requisitos adicionales.

También pueden utilizarse certificados de firma electrónica cualificados, si así se definen en el tipo de certificado correspondiente, para firmar mensajes de autenticación, en particular desafíos de cliente SSL o TLS, correo electrónico seguro S/MIME, cifrado sin recuperación de claves y otros. 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.

En el caso de los sellos de tiempo cualificados, es requisito del Reglamento eIDAS que se creen haciendo uso de firmas avanzadas lo que permite que estas estén basadas o no en certificados cualificados. EADTrust contempla en su servicio de sello de tiempo cualificado la posibilidad de usar ambos tipos de certificados.

3.2.- Usos Prohibidos del Certificado

Los certificados deberán utilizarse para el fin específico para el que fueron creados. Asimismo, los certificados sólo deben utilizarse de conformidad con la legislación aplicable.

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 que corresponden a esta Política de Certificación.

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

5.- 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 actuales se encuentran publicadas en https://www.eadtrust.eu.

6.- Publicación de información y repositorio de certificados

6.1.- 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.

6.2.- 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.

6.3.- 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

7.- Identificación y Autenticación

7.1.- Nombre

7.1.1.- 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.

El perfil de los certificados se puede solicitar a través del servicio de soporte al cliente de EADTrust aunque estarán disponibles en la sección de políticas:

- policy.eadtrust.eu

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.

- **Persona física:** En certificados correspondientes a personas físicas la identificación del signatario estará formada por su nombre y apellidos, más su número de identificación de los admitidos en la norma EN 319 412-1.

- **Persona física - representante persona jurídica**: Determina la relación de representación legal o de apoderado general entre la persona física (titular del certificado/Sujeto/Firmante) y una entidad con personalidad jurídica.

7.1.2.- 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.

7.1.3.- Anonimidad o pseudonimidad de los suscriptores

Se podrán emitir certificados de seudónimo en los casos previstos en la normativa. Por ejemplo, en relación con el perfil de “certificado electrónico de empleado público con seudónimo”.

En este caso el certificado se identificará como de seudónimo de manera inequívoca.

Cuando se consigne un seudónimo en un certificado electrónico, en el proceso de registro se constatará la verdadera identidad del firmante o titular del certificado y se conservará la documentación que la acredite.

EADTrust se compromete a revelar la citada identidad asociada a los certificados de seudónimo cuando lo soliciten los órganos judiciales y otras autoridades públicas para el ejercicio de las funciones que tienen atribuidas con sujeción a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

7.1.4.- Tratamientos de datos excluidos en los certificados

No se harán constar en los certificados datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física, salvo cuando alguno de los datos sea de consignación obligatoria por una normativa aplicable.

Cuando sean de aplicación las excepciones previstas en el artículo 9.2 del Reglamento (UE) 2016/679 del Parlamento europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, se actualizará la presente Política, para especificar de manera clara la excepción aplicada y la razón por la que se lleva a cabo.

7.1.5.- 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

7.1.6.- 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.

7.2.- Validación inicial de la identidad

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

Cuando se genera un par de claves:

- Por una Autoridad de Registro y si las claves se almacenan en un token o una tarjeta criptográfica, la prueba de posesión de la clave privada se demuestra en virtud del procedimiento confiable de entrega y aceptación del token o de la tarjeta criptográfica y del correspondiente certificado y el par de claves almacenados en su interior. De no ser preciso el uso de Dispositivo, los ficheros que contienen el certificado y la clave los entrega la Autoridad de registro de forma separada a la contraseña que permite su uso.

7.2.2.- 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).

7.2.3.- Autenticación de la identidad individual

La identificación de los suscriptores se llevará a cabo mediante Entidades de Registro propias o afiliadas, comprobando los documentos de identidad.

Aunque todavía no está disponible, al ponerse en marcha el servicio mediante identificación a distancia, se dará cumplimiento a los controles definidos en las siguientes normas de SEPBLAC:

- Autorización de procedimientos de vídeo-identificación
- Autorización de procedimientos de identificación no presencial mediante videoconferencia
- Autorización de procedimiento de identificación no presencial

Además, se tomará en consideración las normas equivalentes publicadas en otros países, tales como:

- BAFIN (Alemania) - Circular 3/2017 (GW) - video identification procedures
- Gabinete Nacional de Segurança (Portugal) - Despacho 154/2017 da Entidade Supervisora nacional, de 5 de dezembro Relativo à Identificação de pessoas físicas através de procedimentos de identificação à distânciacom recurso a videoconferência.

7.3.- 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 en la que prestaba servicios el titular del certificado, si el certificado es de Representante, de Persona Jurídica o de sitio web.
- Por el titular, por compromiso de sus claves o por cualquier otra razón que lo requiera.

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.

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

8.1.- 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).

8.1.1.- Quién puede enviar una solicitud del certificado

Pueden solicitar un certificado las personas que necesiten:

- Autenticar la identidad de un usuario, de forma electrónica, ante terceros
- Firmar documentos o transacciones digitalmente de forma que se garantice la integridad de los datos trasmitidos y su procedencia.
- Cifrar datos para que solo el destinatario del documento pueda acceder a su contenido. En este caso, es

recomendable contar con un procedimiento de respaldo de claves privadas, dado que, si se produjera alguna incidencia con ellas, EADTrust no tiene posibilidad de proporcionarlas.

8.1.2.- 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 propias y de la Autoridades de Registro.

Las Oficinas de Registro Propias de EADTrust o de las entidades usuarias con las que EADTrust firme un 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.
- 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).

8.2.- 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.

8.2.1.- Realización de funciones de identificación y autenticación

Es responsabilidad de EADTrust llevar a cabo correctamente la identificación del suscriptor. Este proceso se lleva a cabo antes de la emisión del certificado.

En todos los casos, los usuarios deben consultar la documentación específica de cada certificado para obtener detalles sobre cada uno de ellos.

En relación con las medidas de seguridad adoptadas por los diferentes países miembros de la unión europea en relación con los documentos de identidad, se toman en consideración los datos recogidos en la plataforma PRADO[6] (Registro Público de Documentos Auténticos de Identidad y de Viaje en Red)[7].

[6] http://www.consilium.europa.eu/prado/es/prado-start-page.html
[7] https://www.consilium.europa.eu/prado/ES/prado-glossary/prado-glossary.pdf

Características difractivas:

- Hologramas
- Identigramas
- Estructuras cinemáticas (Kinegramas)

Técnicas de personalización:

- Imagen láser cambiante
- Tipografía

Material:

- Ventanas (por ejemplo, personalizadas)
- Sombras de seguridad (personalizadas)
- Colores cambiantes ópticamente

Impresión de seguridad:

- Microimpresión
- Estructuras de guilloché

Se puede considerar que existe conformidad, cuando se cumplen los criterios de prueba de al menos tres características de seguridad seleccionadas al azar para la identificación de diferentes categorías de la lista anterior contenidas en el documento de identificación presentado.

En el proceso de verificación de identidad es preciso que confirmar las características del documento utilizado específicamente para la verificación de identidad, sean reconocibles y controlables y que estas coincidan (como el diseño, el número de caracteres, el tamaño, el espaciado y la tipografía) con las características predeterminadas de este tipo de documentos.

Se comprueba que las características de seguridad ópticas son visualmente reconocibles en forma y contenido y que coinciden con las características individuales contenidas en el documento de identificación (por ejemplo, coincidencia de las imágenes primaria y secundaria en el documento como identigramas, imágenes de láser cambiante, etc.) o que coinciden con referencias de una base de datos de documentos de identificación.

También se verifica que el documento de identidad utilizado no está dañado y no está manipulado y, en particular, que no contiene una imagen adherida.

8.2.2.- 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.

8.2.3.- 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.

8.3.- 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.

8.3.1.- 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 token criptográfico o en una tarjeta inteligente:

- La Autoridad de Registro autentica la validez de la documentación presentada por el solicitante.
- Tras la autenticación, la Autoridad de Registro solicita un certificado de EADTrust.
- Después de comprobar que la solicitud procede de una Autoridad de Registro autorizada, EADTrust emite el certificado de acuerdo con 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, descarga el certificado al dispositivo de creación de firmas usando un proceso seguro de administración de dispositivos criptográficos. En caso de que EADTrust provea un servicio de firma electrónica remota en nombre del firmante la inserción del material criptográfico se realizará en el dispositivo administrado por EADTrust y se entregarán al solicitante los medios de identificación que permiten su uso.
- Si EADTrust decide no emitir el certificado (incluso cuando los procedimientos de autenticación sean correctos), se notificarán al solicitante las razones de la decisión.

II. 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. También podrá admitirse un informe de auditoría de un especialista certificando que la solicitud se ha generado en un HSM.
- 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.

III. 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.

IV. 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.

8.3.2.- 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.

En el futuro, 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.

8.4.- 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 de emisión de Certificados 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.

8.4.1.- 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.

8.4.2.- Publicación del certificado por la CA

No se publican en directorios LDAP ni en otros repositorios los certificados expedidos a personas físicas para firma digital y autenticación ni a personas jurídicas para sello digital y autenticación.

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

No aplica en el caso de personas físicas.

8.5.- Par de Claves y Uso del Certificado

8.5.1.- 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.

8.5.2.- 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, 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[8].
- 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.

[8] 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

- 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.

8.6.- Renovación del Certificado

8.6.1.- Circunstancias para la renovación del certificado

El certificado se puede renovar si el certificado no ha expirado o si han transcurrido menos de 5 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.

8.6.2.- Quién puede solicitar la renovación

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

8.6.3.- 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.

8.6.4.- 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.

8.6.5.- 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.

8.6.6.- Publicación del certificado de renovación por la CA

Los nuevos certificados de autenticación, firma y sello no se publican en repositorios de certificados.

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

No aplica en el caso de personas físicas.

8.7.- 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.

8.7.1.- Circunstancias para la modificación del certificado

Puede ser necesario modificar un certificado cuando se detecte un error o cuando haya cambiado algún dato de los que se hacen constar en el certificado.

El Proceso de sustitución de certificados se considera una renovación y así computa a la hora del cálculo de los años de renovación sin presencia física tal como marca la normativa aplicable.

8.7.2.- Quién puede solicitar la modificación del certificado

Cualquier suscriptor podrá solicitar la modificación de su certificado si reúne las circunstancias descritas para la renovación.

8.7.3.- Procesamiento de las solicitudes de modificación del certificado

La parte que detecte el error o la necesidad de hacer constar en el certificado datos distintos, comunica a la otra parte la necesidad de proceder a la modificación.

El resto del procedimiento se ajusta al proceso de renovación.

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

EADTrust notifica al suscriptor sobre la emisión de un nuevo certificado mediante los mismos procedimientos previstos en la emisión convencional de certificados.

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

Se aplican las mismas consideraciones que las relativas a la renovación de certificados.

8.7.6.- Publicación del certificado modificado por la CA

Se aplican las mismas consideraciones que las relativas a la renovación de certificados.

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

Se aplican las mismas consideraciones que las relativas a la renovación de certificados.

8.8.- 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.

8.8.1.- 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.
- 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 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.

8.8.2.- 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 AC.
- Podrá realizarse de oficio si a EADTrust le consta por otra vía que se han producido circunstancias que hagan necesaria la revocación.

8.8.3.- 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 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.

8.8.4.- 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.

En caso de que sea de aplicación una política **de firma** concreta, es responsabilidad del tercero que confía en los certificados expedidos por EADTrust la comprobación de que la Política de Firma aplicable es compatible con la Política de Certificación de EADTrust. Dos de las posibles políticas a aplicar, en España, son la de la Administración General del Estado[9] y la de la Administración de Justicia[10].

8.8.5.- 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 donde se alimenta el respondedor OCSP.

[9] https://www.boe.es/boe/dias/2016/11/03/pdfs/BOE-A-2016-10146.pdf
[10] https://www.cteaje.gob.es/cteaje/PA_WebAppSGNTJCTEAJE/descarga/CTEAJE-GIS-707-Autenticaci%C3%B3n,%20Certificados%20y%20Firma%20electr%C3%B3nica.pdf?idFile=53f9d618-467b-4993-a7bd- 7d5ef69ab654

8.8.6.- 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".

8.8.7.- 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 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.

8.8.8.- 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.

8.8.9.- 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)[11].

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.

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

9.- Perfiles de Certificado

9.1.- Perfiles de Certificados de Entidad Final

9.1.1.- Perfil de certificado cualificado de persona física

Campo	Crítico	Contenido
version		3
serialNumber		Número positivo único
signature		Sha256WithRSAEncryption o ecdsa-with-SHA256 o ecdsa-with-SHA384
issuer		Igual al campo Subject del certificado de la CA emisora
validity		4 años
subject		
Country		País (ISO 3166-1 alpha 2 code)
Common Name		Nombre y Apellidos
Given Name		Nombre
Surname		Apellidos
serial number		<3 caracteres de tipo de identidad><país>- <identificador>. Ejemplo: IDCES-012345678R
Organizational Unit		Certificado de persona física
subjectPublicKeyInfo		RSA mínimo 2048 bits ECDSA 254 bits (prime256v1) ó 384 bits (secpr384r1)
Extensiones		
authorityKeyIdentifier		Derivada del resultado de aplicar el hash a la Clave pública de la AC emisora
subjectKeyIdentifier		Derivada del resultado de aplicar el hash a la clave pública del sujeto
issuerAltName		Igual al campo Subject Alternative Names de la CA Emisora
subjectAltName		rfc822 Name Correo electrónico del titular opcional DirectoryName 1.3.6.1.4.1.501.1.1 Nombre 1.3.6.1.4.1.501.1.2 Primer Apellido 1.3.6.1.4.1.501.1.3 Segundo Apellido 1.3.6.1.4.1.501.1.4 DNI/NIE/NIF/ PASS
certificatePolicies*		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.0.41221
cpsURI		http://policy.eadtrust.eu/cps
userNotice		European Agency of Digital Trust, S.L. Natural Person Qualified Certificate
policyIdentifier		0.4.0.194112.1.0 (QCP-n)
qcStatements**		
QcCompliance		Presente
QcType		id-etsi-qct-esign
QcRetentionPeriod		15 años
qcStatement-2		0.4.0.194121.1.1 (id-etsi-qcs-SemanticsId-Natural)
cRLDistributionPoints		
distributionPoint		http://crl.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadnp<Año>.crl
authorityInfoAccess		
calssuers		http://ca.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadnp<Año>.crt
ocsp		http://ocsp.eadtrust.eu
extendedKeyUsage		clientAuth, emailProtection
keyUsage	**Crítica**	digitalSignature, nonRepudiation, keyEncipherment

* En caso de que la clave privada del certificado se encuentre en un **dispositivo cualificado de creación de firma** se cambia el OID 1.3.6.1.4.1.501.2.1.1.0.41221 por 1.3.6.1.4.1.501.2.1.1.1.41221 y el OID 0.4.0.194112.1.0 por 0.4.0.194112.1.2

** En caso de que la clave privada del certificado se encuentre en un **dispositivo cualificado de creación de firma** se añade el campo QSCD

9.1.2.- Perfil de certificado cualificado de representante de persona jurídica

Campo	Crítico	Contenido
version		3
serialNumber		Número positivo único
signature		Sha256WithRSAEncryption o ecdsa-with-SHA256 o ecdsa-with-SHA384
issuer		Igual al campo Subject del certificado de la CA emisora
validity		4 años
subject		
Country		País (ISO 3166-1 alpha 2 code)
Common Name		NIF, nombre y primer apellido del representante y (R: NIF de la Entidad representada)
Given Name		Nombre
Surname		Apellidos
serial number		DNI / NIE
organizationName		Razón Social, tal como figura en los registros oficiales.
organizationIdentifier		3 caracteres tipo -identidad + Country + - + identificador. Ejemplo VATES-B1234567
description		Codificación del documento público que acredita las facultades del firmante o los datos registrales
subjectPublicKeyInfo		RSA mínimo 2048 bits ó ECDSA 254 bits (prime256v1) ó 384 bits (secpr384r1)
Extensiones		
authorityKeyIdentifier		Derivada del resultado de aplicar el hash a la Clave pública de la AC emisora
subjectKeyIdentifier		Derivada del resultado de aplicar el hash a la clave pública del sujeto
issuerAltName		Igual al campo Subject Alternative Names de la CA Emisora
subjectAltName		rfc822 Name Correo electrónico del titular DirectoryName 1.3.6.1.4.1.501.1.1 Nombre del representante 1.3.6.1.4.1.501.1.2 Primer Apellido del representante 1.3.6.1.4.1.501.1.3 Segundo Apellido del representante 1.3.6.1.4.1.501.1.4 NIF del Representante 1.3.6.1.4.1.501.1.6 Razón Social de la Entidad 1.3.6.1.4.1.501.1.7 NIF de la Entidad Representada
certificatePolicies*		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.0.41222
cpsURI		http://policy.eadtrust.eu/cps
userNotice		European Agency of Digital Trust, S.L. Power of Attorney Qualified Certificate
policyIdentifier		0.4.0.194112.1.0 (QCP-n)
PolicyIdentifier		2.16.724.1.3.5.8 (OID MPR)
qcStatements**		
QcCompliance		Presente
QcType		id-etsi-qct-esign
QcRetentionPeriod		15 años
qcStatement-2		0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)
cRLDistributionPoints		
distributionPoint		http://crl.eadtrust.eu/eadtrust-subca<algoritmo><tamañoclave>eadnp<Año>.crl
authorityInfoAccess		
calssuers		http://ca.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadnp<Año>.crt
ocsp		http://ocsp.eadtrust.eu
extendedKeyUsage		clientAuth, emailProtection
keyUsage	**Crítica**	digitalSignature, nonRepudiation, keyEncipherment

* En caso de que la clave privada del certificado se encuentre en un **dispositivo cualificado de creación de firma** se cambia el OID 1.3.6.1.4.1.501.2.1.1.0.41222 por 1.3.6.1.4.1.501.2.1.1.1.41222 y el OID 0.4.0.194112.1.0 por 0.4.0.194112.1.2
** En caso de que la clave privada del certificado se encuentre en un **dispositivo cualificado de creación de firma** se añade el campo QSCD

9.1.3.- Perfil de certificado cualificado de empleado público con nivel de aseguramiento sustancial/medio

Campos/Extensiones	Crítico	Contenido
Versión		3
serialNumber		Número positive único
signature		Sha256WithRSAEncryption ó ecdsa-with-SHA256 ó ecdsa-with-SHA384
Issuer		Igual que el subject de la CA C O OU OI CN
Validity		4 años
Subject		
CommonName		Nombre Apellido1 Apellido2 – DNI/NIE (DNI/NIE)
Title	Opcional	Cargo
OrganizationalUnit	Opcional	Unidad dentro de la administración
OrganizationalUnit	Opcional	Código DIR3 de la unidad
OrganizationalUnit	Opcional	Número de identificación. (NRP o NIP)
OrganizationalUnit		CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO
OrganizationName		Organization Name
serialNumber		DNI/NIE semántica ETSI EN 319 412-1
Surname		Apellidos – DNI/NIE (DNI/NIE)
Given Name		Nombre
CountryName		CountryName
subjectPublicKeyInfo		RSA 2048 bits
extensions		
subjectAltName		
rfc822Name	Opcional	Email del responsable
directoryName		
2.16.724.1.3.5.7.2.1		CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO
2.16.724.1.3.5.7.2.2		Entidad suscriptora
2.16.724.1.3.5.7.2.3		Número único de identificación de la entidad
2.16.724.1.3.5.7.2.4		DNI o NIE del firmante
2.16.724.1.3.5.7.2.5	Opcional	Número de identificación del firmante
2.16.724.1.3.5.7.2.6		Nombre (40 caracteres)
2.16.724.1.3.5.7.2.7		Apellido1 (40 caracteres)
2.16.724.1.3.5.7.2.8		Apellido2 (40 caracteres)
2.16.724.1.3.5.7.2.9	Opcional	Correo electrónico del firmante
2.16.724.1.3.5.7.2.10	Opcional	Unidad, dentro de la Administración, en la que está incluida el firmante
2.16.724.1.3.5.7.2.11	Opcional	Puesto desempeñado por el firmante dentro de la administración.
Othername: UPN	Opcional	UPN para smart card logon
extendedKeyUsage		clientAuth, emailProtection
subjectKeyIdentifier		Derivado de aplicar el hash a la clave del suscriptor
authorityKeyIdentifier		Derivado de aplicar el hash a la clave del emisor
certificatePolicies*		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.0.41223
cpsURI		http://policy.eadtrust.eu
userNotice		European Agency of Digital Trust, S.L. Certificado cualificado de empleado público
policyIdentifier		0.4.0.194112.1.0 (ETSI QCP-n)
policyIdentifier		2.16.724.1.3.5.7.2
cRLDistributionPoints		http://crl.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadnp<Año>.crl

Campos/Extensiones	Crítico	Contenido
authorityInfoAccess		
caIssuers		http://ca.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadnp<Año>.crt
ocsp		http://ocsp.eadtrust.eu
qcStatements**		
QcCompliance		Present
QcType		id-etsi-qct-esign
QcRetentiodPeriod		15
qcStatement-2		0.4.0.194121.1.1 (id-etsi-qcs-SemanticsId-Natural)
keyUsage	Crítica	digitalSignature, keyEncipherment,contentcommitment

* En caso de que la clave privada del certificado se encuentre en un **dispositivo cualificado de creación de firma** se cambia el OID 1.3.6.1.4.1.501.2.1.1.0.41223 por 1.3.6.1.4.1.501.2.1.1.1.41223 y el OID 0.4.0.194112.1.0 por 0.4.0.194112.1.2
** En caso de que la clave privada del certificado se encuentre en un **dispositivo cualificado de creación de firma** se añade el campo QSCD

9.1.4.- Perfil de certificado cualificado de empleado público con seudónimo con nivel de aseguramiento Alto (Firma)

Campos/Extensiones	Crítico	Contenido
Versión		3
serialNumber		Número positive único
signature		Sha256WithRSAEncryption
Issuer		Igual que el subject de la CA C O OU OI CN
Validity		4 años
Subject		
CommonName		(PUESTO o CARGO o literal SEUDONIMO) – SEUDONIMO – NOMBRE OFICIAL DEL ORGANISMO
Pseudonym		seudónimo
Title	Opcional	Nombre del puesto o cargo
OrganizationalUnit	Opcional	Unidad dentro de la administración
OrganizationalUnit	Opcional	Código DIR3 de la unidad
OrganizationalUnit		CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO
OrganizationName		Organization Name
CountryName		CountryName
subjectPublicKeyInfo		RSA 2048
extensions		
subjectAltName		
rfc822Name	Opcional	Email del responsable
directoryName		
2.16.724.1.3.5.4.1.1		CERTIFICADO CUALIFICADO DE FIRMA ELECTRONICA DE EMPLEADO PUBLICO CON SEUDONIMO, DE NIVEL ALTO
2.16.724.1.3.5.4.1.2		Entidad suscriptora
2.16.724.1.3.5.4.1.3		NIF suscriptora
2.16.724.1.3.5.4.1.9	Opcional	Correo electrónico de contacto
2.16.724.1.3.5.4.1.10	Opcional	Unidad
2.16.724.1.3.5.4.1.11	Opcional	Puesto
2.16.724.1.3.5.4.1.12		Seudónimo
subjectKeyIdentifier		Derivado de aplicar el hash a la clave del suscriptor
authorityKeyIdentifier		Derivado de aplicar el hash a la clave del emisor
certificatePolicies*		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.1.41224
cpsURI		http://policy.eadtrust.eu
userNotice		European Agency of Digital Trust, S.L. Certificado cualificado de empleado público con seudónimo nivel alto
policyIdentifier		0.4.0.194112.1.2 (ETSI QCP-n-qscd)
policyIdentifier		2.16.724.1.3.5.4.1

Campos/Extensiones	Crítico	Contenido
cRLDistributionPoints		http://crl.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadnp<Año>.crl
authorityInfoAccess		
caIssuers		http://ca.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadnp<Año>.crt
ocsp		http://ocsp.eadtrust.eu
qcStatements**		
QcCompliance		Present
QcType		id-etsi-qct-esign
QcRetentiodPeriod		15
QcSSCD		Presente
qcStatement-2		0.4.0.194121.1.1 (id-etsi-qcs-SemanticsId-Natural)
keyUsage	Crítica	contentCommitment

Contempla el uso de dispositivo cualificado de creación de firma

9.1.5.- Perfil de certificado cualificado de empleado público con seudónimo con nivel de aseguramiento Alto (Autenticación)

Campos/Extensiones	Crítico	Contenido
Versión		3
serialNumber		Número positive único
signature		Sha256WithRSAEncryption
Issuer		Igual que el subject de la CA C O OU OI CN
Validity		4 años
Subject		
CommonName		(PUESTO o CARGO o literal SEUDONIMO) – SEUDONIMO – NOMBRE OFICIAL DEL ORGANISMO
Pseudonym		seudónimo
Title	Opcional	Nombre del puesto o cargo
OrganizationalUnit	Opcional	Unidad dentro de la administración
OrganizationalUnit	Opcional	Código DIR3 de la unidad
OrganizationalUnit		CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO
OrganizationName		Organization Name
CountryName		CountryName
subjectPublicKeyInfo		RSA 2048
extensions		
subjectAltName		
rfc822Name	Opcional	Email del responsable
directoryName		
2.16.724.1.3.5.4.1.1		CERTIFICADO CUALIFICADO DE FIRMA ELECTRONICA DE EMPLEADO PUBLICO CON SEUDONIMO, DE NIVEL ALTO
2.16.724.1.3.5.4.1.2		Entidad suscriptora
2.16.724.1.3.5.4.1.3		NIF suscriptora
2.16.724.1.3.5.4.1.9	Opcional	Correo electrónico de contacto
2.16.724.1.3.5.4.1.10	Opcional	Unidad
2.16.724.1.3.5.4.1.11	Opcional	Puesto
Othername: UPN	Opcional	UPN para smart card logon
subjectKeyIdentifier		Derivado de aplicar el hash a la clave del suscriptor
authorityKeyIdentifier		Derivado de aplicar el hash a la clave del emisor
certificatePolicies*		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.1.41225
cpsURI		http://policy.eadtrust.eu
userNotice		European Agency of Digital Trust, S.L. Certificado cualificado de empleado público con seudónimo nivel alto
policyIdentifier		0.4.0.194112.1.2 (ETSI QCP-n-qscd)
policyIdentifier		2.16.724.1.3.5.4.1

Campos/Extensiones	Crítico	Contenido
cRLDistributionPoints		http://crl.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadnp<Año>.crl
authorityInfoAccess		
calssuers		http://ca.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadnp<Año>.crt
ocsp		http://ocsp.eadtrust.eu
qcStatements**		
QcCompliance		Present
QcType		id-etsi-qct-esign
QcRetentiodPeriod		15
QcSSCD		Presente
qcStatement-2		0.4.0.194121.1.1 (id-etsi-qcs-SemanticsId-Natural)
extendedKeyUsage		serverAuth, emailprotection
keyUsage	Crítica	digitalSignature

Contempla el uso de dispositivo cualificado de creación de firma

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

10.- Requisitos Empresariales y Legales

10.1.- Tarifas

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

10.2.- Tarifas de emisión de certificados

Las tarifas que los usuarios deben abonar en contraprestación al servicio, se recogen en el documento términos y condiciones de emisión para cada tipo de certificado.

10.3.- 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.

10.3.1.- Consentimiento para usar datos de carácter personal

EADTrust S.L informa de 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/

10.3.2.- 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.

La información de identidad real de los titulares de certificados de seudónimos se aportará a instancia de los órganos judiciales en el marco de un proceso jurisdiccional.

10.4.- Responsabilidad contractual y extracontractual

10.4.1.- 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.

10.4.2.- 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.

10.4.3.- 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.

10.4.4.- 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.

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.

10.4.5.- 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 EADTrust.
- 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.

10.4.6.- 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.

10.4.7.- 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.