Política de emisión de certificados PSD2 de Persona Jurídica y de servidor web

Área Documental de Operaciones

Tabla de O.I.D.'s (identificación a distancia ante RA por Videoconferencia)	
Certificado	OID
Certificado cualificado de Persona Jurídica para PSD2 (QsealC) sin QSCD	1.3.6.1.4.1.501.2.1.1.0.41232
Certificado cualificado de Persona Jurídica para PSD2 (QsealC) con QSCD	1.3.6.1.4.1.501.2.1.1.1.41232
Certificado cualificado de sitio web PSD2 (QWAC)	1.3.6.1.4.1.501.2.1.1.0.41243

EADTrust Policy Committee
EADTRUST EUROPEAN AGENCY OF DIGITAL TRUST

abril 2020
Versión 2.0

Nota sobre derechos de autor

Versiones del documento

Esta publicación podría incluir inexactitudes técnicas o errores tipográficos.

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

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

Certificación ISO 9001. ISO 27001 e ISO 20000-1

EADTrust ha superado diversas auditorías, y, en particular las relativas a las normas ISO 9001. ISO 27001 e ISO 20000-1, con el siguiente alcance:

El Sistema Integrado de Gestión de la Información que da soporte a consultoría, auditoría, desarrollo y provisión de los siguientes servicios electrónicos de confianza: Autoridades de Certificación (PKI) que cumplen los requerimientos de las normas EN 319 401 v2.2.1, EN 319 411-1 v1.2.2, EN 319 411-2 v2.2.2, EN 319 421 v1.1.1 para Sellado de Tiempo, Emisión de Certificados, Validación de OCSP, Firma Electrónica Centralizada, Extensión de Firma Electrónica, Notificación Electrónica Fehaciente (Correo Electrónico Certificado), Publicación Electrónica Fehaciente, Comprobación fehaciente de contenidos digitales, Foro Electrónico de Accionistas, Emisión y Gestión de Claves, Cartulario (Custodia Digital de Documentos Electrónicos), Custodia de Evidencias Electrónicas (Retención de Datos), Voto Electrónico, Facturación Electrónica, Digitalización Certificada, Gestión de firma manuscrita digitalizada y Gestión de firma avanzada vocal, para garantizar la validez legal de todo tipo de gestiones que las utilizan, de acuerdo a la declaración de aplicabilidad vigente.

Certificados

Norma	Certificado
ISO 20000-1:2011	10242586 / 10242587
ISO 27001:2013	10242584 / 10242585
ISO 9001:2015	10242588 / 10242589

Tabla de Contenidos

Control Documental

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

TABLA1. HISTORIAL DE VERSIONES.

Versión	Fecha	Documentos sustituidos	Descripción
1.0	25/11/19	Ninguno	Inicio en la prestación del servicio de emisión de certificados cualificados conforme al Reglamento (UE) 910/2014 eIDAS.
2.0	23/04/2020	1.0	Revisión y actualización de la política como parte del proceso de mejora continua e introducción de la videoconferencia como medio de identificación ante la RA.

TABLA2. HISTORIAL DE VERSIONES.

Propiedades del documento.	
Propietario	EADTrust European Agency of Digital Trust, S.L.
Fecha	24 de abril de 2020
Distribución	Público
Nombre / Código	OPR-PC- V2.0-Emisión_certificados_PSD2_EADTrust

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 Electrónicos de Confianza (DPC), basada en parte en la norma RFC 3647 del año 2003, el RFC 6844 (IETF, 2013) y los Requisitos Básicos de la Política de Certificado para la Emisión y la Gestión de los Certificados de Confianza Pública (CA/Browser Fórum, 2019. 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). La versión disponible en la última revisión de esta política es la 1.6.9. Además de lo indicado en dicha versión, se han tenido en cuenta los resultados de la aprobación del Ballot SC 17 en relación con la codificación del campo **organizationIdentifier** para incluir datos identificativos específicos necesarios para el cumplimiento de la normativa PSD2 y en las especificaciones de ETSI (www.etsi.org).

También tiene en cuenta lo dispuesto en las siguientes normas de aplicación en contextos de PSD2 (Segunda Directiva de Pagos):

- Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) no 1093/2010 y se deroga la Directiva 2007/64/CE
- Reglamento Delegado (UE) 2018/389 DE LA COMISIÓN de 27 de noviembre de 2017 por el que se complementa la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo en lo relativo a las normas técnicas de regulación para la autenticación reforzada de clientes y unos estándares de comunicación abiertos comunes y seguros
- Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera.
- ETSI TS 119 495 - Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366
- Opiniones de la EBA (European Banking Authority.) y pautas publicadas por PRETA S.A.S, entidad subsidiaria de EBA Clearing. Y, en particular:
- Opinion of the European Banking Authority on the use of eIDAS certificates under the RTS on SCA and CSC (EBA-Op-2018-7 Date: 10 December 2018) [2]

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

[2] https://eba.europa.eu/documents/10180/2137845/EBA+Opinion+on+the+use+of+eIDAS+certificates+under+the+RTS+on+SCACSC.pdf

En el contexto de la Segunda Directiva de Pagos (PSD2) se gestionan 2 tipos de certificado:

- **QSEALC**. Certificados de persona jurídica para la realización de sellos electrónicos cualificados
- **QWAC**. Certificados cualificados de autenticación de sitios web

Para conocer los aspectos generales relativos a los **Certificados cualificados de persona jurídica** para la realización de sellos electrónicos se debe consultar la política de certificación específica publicada por EADTrust.

Para conocer los aspectos generales relativos a los **Certificados cualificados de autenticación de sitios web** se debe consultar la política de certificación específica publicada por EADTrust.

En esta Política solo se tratan los aspectos especiales de estos tipos de certificados cuando se expiden en cumplimiento de la normativa PSD2.

1.1.- 1.2.-Términos utilizados en el contexto de PSD2

Es frecuente referirse a muchos conceptos relativos a PSD2 en inglés, por sus siglas, ya que se consideran términos acuñados. Seguidamente se indican las siglas y sus significados, en inglés y en español.

Término	Descripción
AIS	Account Information Services. Servicios de Información de Cuentas. Servicios accesibles mediante API (Application Program Interface) para los TPP (Third Party Provider) Prestadores Financieros en los que obtener información de los usuarios de servicios de pago.
AISP	Account Information Service Provider. Proveedor de servicios de información sobre cuenta. Prestador Financiero que obtiene información de varias entidades en nombre de un usuario de servicios de pago y se las presenta de forma consolidada.
API	Application Programming Interface. Interfaz de Programación de Aplicación. Una API proporciona a una entidad una forma sistemática de obtener información o iniciar acciones en otra entidad. Mediante parámetros y opciones pueden programarse diferentes servicios a terceros. La denominación acuñada para la API es XS2A.
ASPSP	Account Servicing Payment Service Provider. Proveedor de servicios de pago gestor de cuenta. Una entidad financiera en la que un usuario de servicios de pago tiene cuentas a cuya información un Prestador Financiero puede acceder en su nombre o en la puede iniciar una transferencia.
Autenticacion	El proceso de confirmar la identidad de un Prestador Financiero o de un usuario de servicios de pago. Existen pautas como SCA – Strong Customer Authentication (Autenticación Reforzada de Cliente) o mecanismos como los certificados eIdAS para garantizar la correcta identificación.
Autorización	El proceso de confirmar la funcionalidad permitida según las credenciales de un Prestador Financiero o de un usuario de servicios de pago. Inicialmente la funcionalidad se limita a acceder a información de cuentas o iniciar transferencias, según el tipo de prestador (AISP o PISP).
Consentimiento	El acuerdo por el que el usuario de servicios de pago otorga al Prestador la posibilidad de acceder a su información bancaria o iniciar transferencias.
eIdAS	Reglamento UE 910/2014 que regula, entre otros aspectos los requisitos de expedición de certificados cualificados QWAC para sitios web y certificados cualificados para sello electrónico de los diferentes Prestadores. Los certificados los expiden QTSPs – Qualified Trust Service providers, Prestadores cualificados de servicios electrónicos de confianza
NCA	National Competent Authority. Autoridad Nacional Competente. Organismo regulador o supervisor de entidades financieras que autoriza a un Prestador Financiero a operar en el nuevo marco de servicios financieros PSD2 cuando cumpla ciertos requisitos. En España, es el Banco de España.
PIS	Payment Initiation Services. Servicios de iniciación del pagos. Servicios de transferencia bancaria gestionados por un Prestador Financiero en nombre de un usuario de servicios de pago a través de una API ofrecida por su Proveedor de servicios de pago gestor de cuenta.
PIIS	Payment Issuer Instrument Service. Servicio asociado a medio de pago para solicitar por API la autorización de pago con tarjeta indicando el importe (comprueba la validez de la tarjeta y la disponibilidad del importe).

PISP	Payment Initiation Service Provider. Proveedor de servicios de iniciación de pago. Prestador Financiero de servicios de transferencia bancaria gestionados en nombre de un usuario de servicios de pago a través de una API ofrecida por su Proveedor de servicios de pago gestor de cuenta. Puede requerirse por parte del ASPSP la confirmación del usuario.
PSU	Payment Service User. Usuario de servicios de pago.
QTSP	Qualified Trust Service Provider. Prestadores cualificados de servicios electrónicos de confianza. Expiden certificados cualificados QWAC para sitios web y certificados cualificados para sello electrónico de los diferentes Prestadores Financieros. Los certificados permiten identificar a los Prestadores Financieros cuando usan las APIs de otras entidades en entornos de Producción.
SCA	Strong Customer Authentication. Autenticación Reforzada de Cliente. Proceso de confirmar la identidad del usuario. Normalmente se usan dos o más factores de autenticación: • "Algo que sabes" • "Algo que tienes" • "Algo que te caracteriza"
Sandbox	Experimentos con gaseosa. Zona de pruebas. El término en inglés Sandbox se refiere a una zona de juegos para niños en la que no estropean nada ni se hacen daño. Se amplía a usos profesionales en los que se prueban desarrollos con funcionalidades similares a las del entorno real antes del paso a producción.
TPP	Third Party Provider. Prestador Financiero. AISP o PISP. Actúa en nombre de un usuario de servicios de pago accediendo a su información bancaria en otra entidad o iniciando una transferencia. Requiere una licencia por parte de una NCA y puede operar en otros países en virtud del concepto de "pasaporte" haciendo uso de certificados eIdAS.
XS2A	Access to account. Interfaz de acceso a la cuenta por el ASPSP para facilitar las consultas de información, inicio de pagos y otros servicios proporcionados por los TPP.

2.- Definición

Los certificados definidos en esta política son expedidos en correspondencia con los requisitos del REGLAMENTO (UE) No 910/2014, tomando en consideración, además, los estándares internacionales establecidos en ETSI e IETF, en particular el IETF RFC 3647.

Dentro de las políticas de certificación definidas en ETSI EN 319 411-2 para los certificados cualificados conforme al Reglamento (UE) No 910/2014, EADTrust adopta como políticas de base para sus certificados PSD2, las siguientes:

Para QSEAL:

- Una política para los certificados calificados de la UE emitidos a personas jurídicas (QCP-l) que ofrecen el nivel de calidad definido en Reglamento (UE) Nº 910/2014 para los certificados reconocidos por la UE. Los requisitos para el QCP-l incluyen todos los requisitos de la política de NCP, además de los requisitos adicionales adecuados para apoyar la emisión y gestión de certificados cualificados de la UE, tal como se especifica en el Reglamento (UE) No 910/2014

- Una política (QCP-l-qscd) para los certificados calificados de la UE emitidos a personas jurídicas que ofrecen el nivel de calidad definido en el Reglamento (UE) Nº 910/2014 para los certificados reconocidos por la UE y que requiere el uso de un sello reconocido y un Dispositivo de creación (QSCD). Dicha política requiere que la clave privada relacionada con la clave pública certificada resida en el QSCD: - Los requisitos para el QCP-l-qscd incluyen todos los requisitos del QCP-l (incluyendo todos los requisitos de la NCP+), además de disposiciones adicionales adecuadas para apoyar la emisión de certificados cualificados de la UE y gestión según se especifica en el Reglamento (UE) Nº 910/2014 [i.1], incluidas las específicas del QSCD.

Para QWAC:

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

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

2.1.- Soporte y nivel de seguridad

Tipo	Certificado	Policy Identifier	Policy OID	Formato	Nivel de seguridad
Entidad Legal PSD2	Sello Corporativo (QSeal)	0.4.0.194112.1.1 (OID ETSI QCP-l) 0.4.0.194112.1.3 (OID ETSI QCP-l-QSCD)	1.3.6.1.4.1.501.2.1.1.0.41232 1.3.6.1.4.1.501.2.1.1.1.41232	Software Disposition*	Sustancial Alto
Autenticación de sitio web	SSL PSD2 (QWAC)	0.4.0.194112.1.4 (ETSI QCP-w) 2.23.140.1.1 (CAB/FORUM EV)	1.3.6.1.4.1.501.2.1.1.0.41243	Software	Sustancial

(*) Los dispositivos habituales son HSM (Hardware Security Module), token seguro y tarjeta chip. Los tokens USB se consideran equivalentes al uso de tarjetas inteligentes contando con que incorporan el lector de tarjeta en el mismo encapsulado.

3.- Administración de políticas

3.1.- 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.

3.2.- Contacto

Nombre del PSC	European Agency of digital Trust, S. L.
Dirección	C/ Alba,15, 28043 Madrid - Spain
Dirección de email (en relación con la política)	policy@eadtrust.eu
Dirección de email para PSD2 (para uso de las **Autoridades Nacionales Competentes**)	CA-request@eadtrust.eu
Teléfono	(+34) 902365612 / (+34) 917160555

En el contexto del sector financiero, EADTrust dispone de **Código LEI** (Legal Entity Identifier, en español, Identificador de Entidad Jurídica) así como otros códigos identificadores:

Código LEI	9598009UB0L0E8XB2R35

Código D-U-N-S	461509305
CIF	B85626240

4.- Participantes en la PKI

4.1.- 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. Se diferencian por algoritmo de clave pública, tamaño de la clave y por diferentes usos de los certificados de entidad final, cualificados y no cualificados.

Para certificados cualificados de persona física o jurídica:

- 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 certificados cualificados web:

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

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

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

4.2.- Autoridad de Registro

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

Estas RAs son entidades que actúan de acuerdo con esta Política de Certificación y las prácticas descritas en la Declaración de Prácticas de Certificación (DPC), junto con una relación escrita formal y contractual con EADTrust. Su objetivo principal es la gestión de relaciones con los titulares y suscriptores de los certificados, que incluye la identificación y registro de los titulares de los certificados, 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.

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

Hay dos formas principales que la RA puede adoptar en la estructura de EADTrust respecto a la verificación de identidad de los solicitantes: inscripción en persona con personación ante una agente de RA en persona, o mediante la verificación de la identidad a distancia (identificación remota) mediante videoconferencia (también descrita como mediante telepresencia) o videograbación ("digital onboarding"). A la fecha de esta versión de esta Política, sólo está disponibles las variantes de servicio que requieren personación y telepresencia por videoconferencia o mediante firma electrónica cualificada conforme se indica en la política específica.

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

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

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

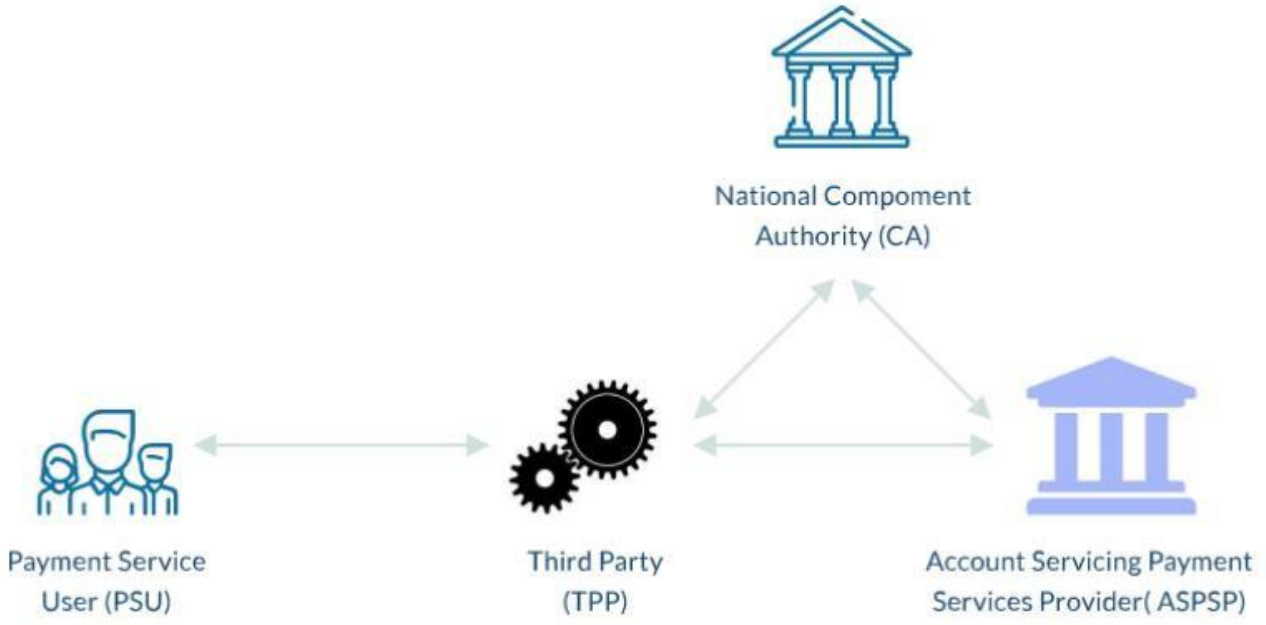
- Identificación y autenticación de los titulares y suscriptores de certificados.
- Desarrollo de una relación contractual para la emisión de certificados con la entidad final o el suscriptor.
- Generación de certificado (por medio de comunicación autenticada con la CA online) y la entrega del certificado de forma que se pueda instalar en el servidor web o con la relación del titular del certificado y/o 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.
- Conservación de cualquier documentación relevante y relacionada con la emisión del certificado o con la relación del suscriptor con la RA.

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.

4.3.- Titulares de certificados y terceros que confían

Al nivel de uso de los certificados considerados en este documento, son participantes de la PKI las entidades proveedoras de servicios de pago (third party payment service provider - TPP) y gestores de cuenta (ASPSP) que usan los certificados o confían en ellos.

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



Los certificados de usuario final se emiten a TPP (AISP, PISP y PIISP).

Un TPP utiliza su certificado para identificarse en la interfaz XS2A (access to account , acceso a la cuenta) proporcionada por un ASPSP según lo requerido por los artículos 65, 66 y 67 de la Directiva (UE) 2015/2366 y los artículos 34, 35 y 36 del Reglamento Delegado (UE) 2018/389.

El TPP firma sus solicitudes utilizando la clave privada correspondiente e incluye su certificado en el mensaje de solicitud.

Un ASPSP participa como tercero que confía en el certificado. El ASPSP debe verificar el sello electrónico firma electrónica y el certificado que forman parte de un mensaje entrante en la interfaz XS2A proporcionada por el ASPSP de acuerdo con el artículo 35 del Reglamento Delegado (UE) 2018/389.

El ASPSP tiene que decidir en base a su propio análisis y gestión de riesgos sobre los pasos detallados que se deben realizar para la verificación de un certificado (verificar con una lista blanca de certificados administrados por el ASPSP, verificar con una CRL proporcionada por EADTrust o a través de consultas al servicio OCSP proporcionado por EADTrust.

Por otro lado, se debe comprobar la cadena de confianza hasta la autoridad raíz verificando la inclusión del prestador en la lista de confianza (TSL).

5.- Expedición de certificados

5.1.- Limitaciones a la expedición de certificados PSD2

Solo se expiden certificados PSD2 a entidades proveedoras de servicios de pago (third party payment service provider - TPP) que actúen en uno o más de estos roles:

- Gestor de cuenta (Account Servicing Payment Service Provider (ASPSP)
- Proveedor de servicios de iniciación de pagos (Payment Initiation Service Provider - PISP),
- Proveedor de información sobre cuentas (Account Information Service Provider - AISP)
- Emisor de instrumentos de pago basados en tarjetas (Payment Instrument Issuer Payment Service Provider - PIISP).

Solo se expiden certificados PSD2 a entidades (proveedores de servicios de pago) que figuren inscritas en un registro de una Autoridad Nacional Competente de la que conste una dirección de correo electrónico a los efectos de informar sobre la expedición de certificados de su ámbito de competencia o recibir solicitudes de revocación.

En la expedición de certificados la RA comprueba que la entidad consta en el registro de una Autoridad Nacional Competente

La lista de Autoridades Nacionales Competentes que se consideran en esta Política de certificación se incluye en el **Anexo I.** Esta información podrá actualizarse conforme esté disponible por parte de las Autoridades Nacionales Competentes.

Para codificar correctamente los atributos del certificado se tendrá en cuenta:

- El número de autorización del TPP (PSP identifier)
- El rol o roles con los que opera
- La denominación de la Autoridad Nacional Competente en cuyo registro consta.

El número de identificación y su estructura depende del país y de la Autoridad Nacional Competente. Se describe en el **Anexo II.**

El número de autorización del TPP (PSP identifier) puede incluir un prefijo seguido de dos puntos ":" seguido del tipo de entidad según se indica en el artículo 1.1 de la Directiva (UE) 2015/2366 por si fuera necesario para garantizar la unicidad de identificación (en el caso de que se asignen códigos diferenciados por cada tipo de entidad de modo que pudiera darse que dos entidades de distinto tipo pudieran tener un mismo código). Los tipos de entidad admitidos son:

- "Credit institution" – **CI**
- "Payment institution" – **PI**
- "Electronic money institution (or e-money institution)" – **EMI**
- "Account information service provider "exento en aplicación del artículo 33 de la Directiva (UE) 2015/2366 – **RAISP**

La codificación de los roles se incluye en el **Anexo III.**

Las abreviaturas oficiales de las denominaciones de las Autoridades Nacionales Competentes se incluyen en el **Anexo IV**.

5.2.- Limitaciones de uso de los certificados PSD2

Un PIISP, PISP or AISP deberá usar estos certificados según se indica en los artículos 65 2. (c) (para el PIISP), 66 3. (d) (para el PISP) y 67 2. (c) (para el AISP) para identificarse en la interfaz XS2A ofrecida por un ASPSP.

5.3.- Obligaciones de los titulares de certificados PSD2

Los titulares de certificados PSD2 deben dejar de usar las claves privadas asociadas a ellos en las siguientes circunstancias:

- Cuando la autorización del PSP haya sido retirada por la autoridad competente de su estado miembro de origen,
- Cuando el PSP interrumpa sus servicios o su negocio,
- Cuando cualquier atributo contenido en su certificado haya cambiado,
- Cuando se sospeche que la clave privada del PSP se haya comprometido.

El suscriptor (PSP) debe notificar a EADTrust sin demoras indebidas cuando se den algunas de las circunstancias anteriores.

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.

La CA destinada a la emisión de certificados para 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.

Los perfiles y la política de certificación se ajustan a lo definido en la norma ETSI TS 119 495.

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 PSD2 para TLS son los siguientes

- https://ecc-256-psd2-tst.eadtrust.eu/
- https://ecc-384-psd2-tst.eadtrust.eu/
- https://rsa-2048-psd2-tst.eadtrust.eu/
- https://rsa-4096-psd2-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**

6.2.- Validación inicial de la identidad

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

Para los certificados **QWAC**, el solicitante aporta una solicitud de certificado PKCS#10 generada en su servidor web, lo que implica la posesión de la clave privada.

Los certificados **QsealC** se entregarán en formato PKCS#12 lo que incluye la clave privada. Si EADTrust o sus Entidades de Registro tienen constancia de que una solicitud de certificado PKCS#10 se ha generado en un HSM, se podrán entregar certificados cualificados con la indicación de Dispositivo Cualificado de Creación de Sello.

6.2.2.- Autenticación de la organización e identidad del dominio

Como parte del proceso de autenticación de EADTrust, en el caso de expedición o-revocación de certificados de PSD2, (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. EADTrust también podrá utilizar otros medios para llevar a cabo esta comprobación.

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

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

En el caso de certificados emitidos a Prestadores de Servicios contemplados en las Directivas de Pagos (PSD2), se constatará su existencia en el Registro administrado por el Órgano Supervisor (National Competent Authorities) y su rol.

Si la NCA proporciona reglas de validación relativas al registro de actividades de servicios de pago, y las comunica a EADTrust, serán tenidas en cuenta.

Los registros identificados que se consultarán se señalan en el **Anexo II**.

Una vez que se expida un certificado PSD2, EADTrust notificará a la Autoridad Nacional Competente en el mail que consta en el **Anexo I** acerca de los datos contenidos en el certificado, en un formato fácilmente legible:

- Número de serie del certificado en hexadecimal
- Nombre distinguido del sujeto (la entidad PSP) que figura en el certificado
- Nombre distinguido del emisor (EADTrust) que figura en el certificado
- Período de validez del certificado
- Información de contacto e instrucciones para la solicitud de revocación
- Copia del archivo de certificado en formato Base64
- URL de la política de certificados PSD2 (en inglés)
- URL de la Declaración de práctica de Certificación (en inglés)
- URL de los certificados de CA intermedia y root aplicables
- URL de los repositorios de CRL
- URL deservicio OCSP.

En el caso de solicitudes de nuevos certificados antes de la expiración del vigente, se vuelve a comprobar que la entidad sigue figurando en los registros correspondientes como PSP.

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 o del certificado de sello.
- Por el titular, por compromiso de sus claves o por cualquier otra razón que lo requiera.

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

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

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 Nacional 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.

El TSP tramitará dicha solicitud de revocación y validará su autenticidad. Si no está claramente indicado o implícita la razón por la que se solicita la revocación, o si la razón no es de la competencia de la ANC, EADTrust puede decidir no tomar medidas. Sobre la base de una solicitud auténtica de una ANC, EADTrust revocará el certificado a su debido tiempo si se cumple alguna de las siguientes condiciones:

- la autorización de la PSP ha sido revocada;
- se ha revocado cualquier función de PSP incluida en el certificado.

EADTrust podrá realizar la revocación de oficio en el caso de certificados PSD2 si detecta que la entidad titular de los certificados ha dejado de figurar en los registros que le permiten ejercer la actividad de PSP (indicados en el Anexo II). En ese caso contactará con la entidad y la Autoridad Nacional Competente para ratificar que esa circunstancia se ha producido antes de proceder a la revocación. La investigación de oficio se activa por indicios, incluso una solicitud de revocación por la Autoridad Nacional Competente insuficientemente autenticada o que no haya seguido el procedimiento.
La Autoridad Nacional Competente se podrá autenticar con una firma electrónica en el documento con el que solicita la revocación o mediante un procedimiento que se describe más adelante.

6.4.- Requisitos operacionales del ciclo de vida de los certificados

El interesado en un certificado emitido por la CA de EADTrust podrá de los definidos en esta política, deberá cumplimentar el formulario de solicitud de emisión de certificados disponible en la página web: www.eadtrust.eu

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

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

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

- Documento Identificación: DNI, NIE, PAS
- Poder que acredita la Representación vigente
- Debe conocer además la siguiente información:
    a) deberá identificar además la categoría de la entidad
        i. Organización privada.
        ii. Entidad gubernamental.
        iii. Entidad comercial.
        iv. Entidad no comercial.
    b) Indicar el tipo de certificado web que se desea adquirir:
        i. Certificado cualificado de web extended validación (EV).
- Indicar el nombre del dominio/dominios que desea autenticar (DNS/CSR).

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

6.4.1.- Emisión del Certificado

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

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

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.

6.4.2.- Quién puede enviar una solicitud del certificado

Pueden solicitar un certificado de entidad PSD2:

- Gestor de cuenta (Account Servicing Payment Service Provider (ASPSP)
- Proveedor de servicios de iniciación de pagos (Payment Initiation Service Provider - PISP),
- Proveedor de información sobre cuentas (Account Information Service Provider - AISP)
- Emisor de instrumentos de pago basados en tarjetas (Payment Instrument Issuer Payment Service Provider - PIISP).

6.4.3.- 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 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.
- Mantener toda la información y documentación relativa a los certificados, y gestionar su emisión o revocación.
- 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, o revocación, 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).

6.4.4.- 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.

Tras comprobar la identidad del solicitante por su DNI o documento de identificación, los operadores de la RA deberán leer y valorar la copia de los estatutos de la sociedad, de los poderes de representación y la declaración de que se encuentran vigentes, para confirmar que procede la emisión del certificado, considerando, entre otros aspectos que la solicitud de certificados se encuentra dentro de las potestades del solicitante.

Además, se comprueba que la entidad figura inscrita en alguno de los registros mantenidos por las Autoridades Competentes del país en el que se realiza la supervisión. Una vez realizada la verificación EADTrust informará por email a las Autoridades Competentes que hubieran proporcionado ese dato de contacto sobre la emisión de un certificado a entidades de su ámbito de competencia.

Para los certificados QWAC PSD2 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.

6.4.5.- 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 de la suficiencia de poderes de representación.

Si la información no es correcta, la RA denegará la solicitud y se pondrá en contacto con el solicitante para explicar la razón. Si la información es correcta, se emitirá el certificado.

En el proceso de expedición de certificados de EADTrust, se aplican controles duales, de modo que la decisión de expedición del certificado no la pueda tomar la misma persona que comprueba la información asociada a la solicitud.

En el proceso de expedición de los certificados QWAC PSD2 definidos en esta Política, además, se aplica un tercer control para la comprobación de que el dominio esté bajo el control exclusivo del solicitante del certificado.

6.4.6.- 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.

6.4.7.- 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 remitida por el solicitante.
- Después de recibir la documentación, EADTrust emite el certificado, que se deberá insertar en el dispositivo en el que se generó la solicitud.

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

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

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

6.5.- 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.

6.5.1.- Conducta que constituye la aceptación del certificado

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

6.5.2.- 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.

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

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

Cuando se emite un certificado de PSD2 se notifica mediante el email designado a la Autoridad Nacional Competente en cuyo registro consta el TPP.

6.6.- Par de Claves y Uso del Certificado

6.6.1.- 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.
- 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 titulares 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

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

vinculado, siempre que se utilice un dispositivo criptográfico (dispositivo cualificado de creación de sello electrónico), según las disposiciones del Reglamento eIDAS.
- Abonar las tarifas por los servicios de certificación solicitados en los términos y condiciones previstos por la CA, cuando el titular coincida con el suscriptor.
- Autorizar a la CA a que, a través de la RA, utilice los datos personales aportados por el titular para validar, comprobar y autenticar la identidad declarada por este.
- Solicitar la revocación del Certificado cuando se cumpla alguno de los supuestos previstos en esta política y en las prácticas específicas y en la legislación vigente para los diferentes status del ciclo de vida de los certificados
- Comprender y aceptar los términos y condiciones de uso del certificado, y cualquier modificación que se realice a estos
- No comprometer intencionalmente la seguridad de los servicios de certificación
- Todas las que se deriven de la DPC, de esta política de certificado específica y de la legislación vigente

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

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

- 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.

6.7.- Renovación del Certificado

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

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

6.7.1.- Circunstancias para la renovación del certificado

No Aplica.

6.7.2.- Quién puede solicitar la renovación

No Aplica.

6.7.3.- Procesamiento de solicitudes de renovación de certificados

No Aplica.

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

No Aplica.

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

No Aplica.

6.7.6.- Publicación del certificado de renovación por la CA

No Aplica.

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

No Aplica.

6.8.- 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.

6.8.1.- Circunstancias para la modificación del certificado

No Aplica.

6.8.2.- Quién puede solicitar la modificación del certificado

No Aplica.

6.8.3.- Procesamiento de las solicitudes de modificación del certificado

No Aplica.

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

No Aplica.

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

No Aplica.

6.8.6.- Publicación del certificado modificado por la CA

No Aplica.

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

No Aplica.

6.9.- Revocación 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.

6.9.1.- Circunstancias para la revocación

Además de las circunstancias para la revocación indicadas en las políticas de certificación con las que se relaciona la presente política, en relación con los certificados PSD2 se consideran las siguientes:

- Que una Autoridad Nacional Competente indique la necesidad de revocar un certificado PSD2.
- Que se detecte por parte de EADTrust que la entidad ha perdido la condición de TPP autorizada en el registro nacional correspondiente a su país.
- Que el titular del certificado EADTrust que la entidad ha perdido la condición de TPP autorizada en el registro nacional correspondiente a su país.
- 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.
- Otras definidas en la Declaración de Practicas de Certificación que sean aplicables.

6.9.2.- Quién puede solicitar la revocación

La revocación de un certificado podrá solicitarse por

- El titular del certificado.
- El Solicitante o Suscriptor cuando no coincide con el Titular.
- La RA o la CA.
- Los organismos supervisores (Autoridades Nacionales Competentes).

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

6.9.3.- Procedimiento para la solicitud de revocación

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

- En línea, cumplimentando el formulario de solicitud de revocación disponible en la dirección www.eadtrust.eu
- Por correo electrónico con solicitud firmada electrónicamente utilizando un certificado cualificado.
- Por correo postal dirigido al domicilio de EADTrust, 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.
- Los organismos supervisores (Autoridades Competentes) pueden solicitar la revocación mediante el uso de una dirección de e-mail designada para ello, sin perjuicio de las comprobaciones adicionales que realice EADTrust para verificar la legitimidad de la solicitud.

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

Cuando la revocación la solicita la NCA:

EADTrust informará a las NCA respecto a las que tenga constancia de la existencia de una dirección de mail de contacto para relacionarse con Prestadores de Servicios de Confianza Digital acerca de los procedimientos de autenticación y mantendrá el contacto que facilite su labor.

Resumidamente, los procedimientos son los siguientes:

- En el caso de los certificados para PSD2, los organismos supervisores (Autoridades Nacionales Competentes) pueden solicitar la revocación mediante el uso de la dirección de e-mail designada para ello por la NCA (incluida en el **Anexo I**), dirigida a la dirección de mail reservada para este uso designada en la sección "**Contact**o" de esta política, sin perjuicio de las comprobaciones adicionales que realice EADTrust para verificar la legitimidad de la solicitud.
- Para realizar la solicitud de revocación deberán indicar los datos de la entidad cuyos certificados se revocan:
    - Nombre de la entidad
    - Número de registro de la entidad tal como se codifica en el campo "**organizationIdentifier**"
    - Número de identificación fiscal.
    - Número LEI, si le consta
    - Rol para el que el certificado debe ser revocado
    - Razón de la revocación en términos descriptivos
- Si la NCA posee certificado de firma o sello, la petición se deberá incluir en un fichero PDF firmado. Si la NCA no posee certificado de firma o sello, la petición se deberá acompañar de un valor de autenticación calculado como la función SHA-256 aplicada a la concatenación del código único asignado al NCA por EADTrust (y remitido a su dirección de contacto indicada en el **Anexo I**) y la fecha del día en formato AAAAMMDD (por ejemplo: CODCODCODCODCODAAAAMMDD). Este procedimiento se ilustra con un ejemplo en la notificación enviada a cada NCA.

Una vez comprobado que la solicitud de revocación cumple con los requisitos definidos en esta Política y en la Declaración de Prácticas de EADTrust, se procederá a la revocación del certificado. La revocación se procesará en un tiempo menor de 24 horas.

Luego de realizada la revocación EADTrust informará al titular del certificado y a la Autoridad Nacional Competente, indicando que se ha completado la revocación, independientemente de que la solicitud de revocación proceda de uno o de la otra o haya sido realizada de oficio por EADTrust si detecta que una entidad ha dejado de figurar en el registro que le permite ejercer la actividad de PSP (indicados en el Anexo II).

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.

6.9.1.- Periodo de gracia para comprobar certificados revocados

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

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.

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[7] y la de la Administración de Justicia[8].

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

6.9.2.- 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, generándose una nueva CRL y en la base de datos de la plataforma de gestión que consulta el respondedor OCSP.

6.9.3.- 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”.

6.9.4.- 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 como máximo 10 minutos más tarde desde que se confirma una revocación.

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

[7] https://www.boe.es/boe/dias/2016/11/03/pdfs/BOE-A-2016-10146.pdf
[8] 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

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

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

6.9.5.- Actualización de la CRLs

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 la base de datos desde la que se ofrece el servicio OCSP y desde la que se genera la lista CRL se establece en un máximo de 10 minutos.

6.9.6.- 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)[9].

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.

6.9.7.- Recuperación de Certificados

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

7.- 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.

7.1.- Extensiones de certificado

Las extensiones utilizadas dependiendo del perfil en cada caso son:

- Authority key Identifier.
- subjectKeyIdentifier.
- basicConstraints.
- keyUsage.

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

- certificatePolicies.
- subjectAltName.
- issuerAltName.
- extKeyUsage.
- cRLDistributionPoint.
- Authority Information Access.
- **qcStatements**
- **organizationIdentifier**
- **cabfOrganizationIdentifier**

7.2.- Perfil de certificado cualificado de web PSD2 (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		
OrganizationIdentifier		ETSI EN 319 412-1 and CA/B Forum format
OrganizationalUnit		Type of web certificate
OrganizationName		Organization Name
LocalityName		Locality Name
StateOrProvinceName		State or province name
CountryName		CountryName
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
serialNumber		Registration Number
subjectPublicKeyInfo		RSA 2048 bits minimum or ECDSA 256 bits (prime256v1) or 384 bits (secpr384r1)
extensions		
subjectAltName		
dnsName		DNS name(s)
extendedKeyUsage		serverAuth, clientAuth
subjectKeyIdentifier		Derived from the result of applying the hash to the public key of the subject
authorityKeyIdentifier		Derived from the result of applying the hash to the Public key of the issuing CA
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.0.41243
cpsURI		http://policy.eadtrust.eu
userNotice		European Agency of Digital Trust, S.L. EU qualified website authentication certificate for payment service provider.
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
qcStatement-2		0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)
PSD2QcType		ETSI TS 119 495 Format
keyUsage	Crítica	digitalSignature, keyEncipherment
CT RFC6962		Certificate Transparency
cabfOrganizationIdentifier		Effective January 31, 2020, if the subject:organizationIdentifier field is present, this field MUST be present

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

La cumplimentación de **cabfOrganizationIdentifier** se realizará en versiones posteriores del certificado y como muy tarde el 31 de enero de 2020.

7.2.1.- Perfil de certificado cualificado PSD2 de persona jurídica para sello electrónico

Campos/Extensiones	Crítico	Contenido
version		3
serialNumber		Número positivo único
signature		Sha256WithRSAEncryption ó ecdsa-with-SHA256 ó ecdsa-with-SHA384
issuer		Igual al campo Subject del certificado de la CA emisora
validity		4 años
subject		
serialNumber	Opcional	DNI/NIE en formato ETSI EN 412-1
Surname	Opcional	Apellidos
Givenname	Opcional	Nombre
CommonName		Nombre común
organizationIdentifier		<3 caracteres de tipo de identidad><país>- <identificador>. Ejemplo: VATES-B12312312
Organization Name		Nombre registrado completo
Country		País
OrganizationalUnit		Certificado de Sello de Entidad
subjectPublicKeyInfo		RSA mínimo 2048 bits ECDSA 256 bits (prime256v1) ó 384 bits (secpr384r1)
extensions		
issuerAltName		Igual al campo SubjectAlternativeNames de la CA Emisora
extendedKeyUsage		clientAuth, emailProtection
subjectKeyIdentifier		Derivada del resultado de aplicar el hash a la clave pública del sujeto
authorityKeyIdentifier		Derivada del resultado de aplicar el hash a la Clave pública de la AC emisora
certificatePolicies*		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.0.41232
cpsURI		http://policy.eadtrust.eu
userNotice		"European Agency of Digital Trust, S.L. Legal Person Qualified Certificate for Qualified Payment Service Provider."
policyIdentifier		0.4.0.194112.1.1 (OID ETSI QCP-l)
userNotice		European Telecommunications Standards Institute. eIDAS European Regulation Compliant
cRLDistributionPoints		http://crl.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadlp<Año>.crl
authorityInfoAccess		
calssuers		http://ca.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadlp<Año>.crt
ocsp		http://ocsp.eadtrust.eu
basicConstraint	Crítica	CA false
qcStatements**		
QcCompliance		Presente
QcType		id-etsi-qct-eseal
QcRetentiodPeriod		15
qcStatement-2		0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)
PSD2QcType		ETSI TS 119 495 Format
keyUsage	Crítica	digitalSignature, nonRepudiation, keyEncipherment

* En caso de que la clave privada del certificado se encuentre en un **dispositivo cualificado de creación de sello** se cambia el OID 1.3.6.1.4.1.501.2.1.1.0.41232 por 1.3.6.1.4.1.501.2.1.1.1.41232 y el OID 0.4.0.194112.1.1 por 0.4.0.194112.1.3
** En caso de que la clave privada del certificado se encuentre en un **dispositivo cualificado de creación de sello** se añade el campo QSCD

Este tipo de certificados se expiden bajo las jerarquías cualificadas no web de persona jurídica y admite diferentes variantes.

8.- Requisitos Empresariales y Legales

8.1.- 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.

8.2.- 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.

8.2.1.- 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.

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

Cuando el servicio de emisión o revocación de certificados se provea en la modalidad de verificación y autenticación de identidad mediante video conferencia o videograbación, EADTrust requerirá captar la imagen y la voz del Solicitante. La base legal para este tratamiento es la ejecución del contrato de prestación de servicios en esta modalidad conforme dispone el artículo 6.1 b) del Reglamento General de Protección de Datos. Estos datos son necesarios para la adecuada prestación del servicio y se incorporarán al registro de actividades de tratamiento de EADTrust.

Para más información sobre el ejercicio de los derechos al amparo del RGPD y sobre el tratamiento de sus datos personales por EADTrust consulte la nota legal más extensa, incluida en: http://eadtrust.rgpd.de/

8.2.2.- 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.

8.3.- Responsabilidad contractual y extracontractual

8.3.1.- 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.

8.3.2.- 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.

8.3.3.- 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.

8.3.4.- 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.

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.

8.3.5.- 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 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.

8.3.6.- 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.

8.3.7.- 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.

8.3.8.- Quejas. Reclamaciones y jurisdicción

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

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

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

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

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

Las reclamaciones dirigidas a EADTrust se gestionarán de forma directa para intentar llegar a un acuerdo que resuelva el incidente o, en su caso, comprobar si es una cobertura incluida en el seguro.

La actividad de EADTrust se rige por la Ley española y por los Tribunales de Madrid, salvo que el usuario ostente la condición de consumidor, lo que redundará en que se aplique la normativa de protección de consumidores.

9.- Anexo I

List of email addresses of the national competent authorities that will follow the process for requesting revocation of eIDAS certificates as set out in the EBA Opinion on the use of eIDAS certificates (EBA-OP-2018-7).

Version 2, published on 13th September 2019[10].

EU MS	Name of Authority	Email address
Austria	Austrian Financial Market Authority	PSD2@fma.gv.at
Belgium	National Bank of Belgium	psd@nbb.be
Bulgaria	Bulgarian National Bank	Payment_Supervision@bnbank.org
Croatia	Croatian National Bank	psd2.certificate@hnb.hr
Cyprus	Central Bank of Cyprus (1)	
Czech	Czech National Bank (1)	
Denmark	Danish Financial Supervisory Authority (1)	
Estonia	Estonia Financial Supervisory Authority (1)	
Finland	Finnish Financial Supervisory Authority	PSD2@finanssivalvonta.fi
France	Prudential Supervisory and Resolution Authority (2)	2788-EXEMPTION-API-UT@acpr.banquefrance.fr
Germany	Federal Financial Supervisory Authority (1)	
Greece	Bank of Greece	sec.PaymentEmoneyIns@bankofgreece.gr
Hungary	Central Bank of Hungary (1)	
Ireland	Central Bank of Ireland (1)	
Italy	Bank of Italy (1)	
Latvia	Financial and Capital Markets Commission	fktk@fktk.lv

[10] https://eba.europa.eu/documents/10180/2882455/Email+addresses+of+CAs+for+the+notification+exchange+with+QTSPs.pdf.

Lithuania	Bank of Lithuania	PSD2-eIDAS-certificates@lb.lt
Luxembourg	Commission for the Supervision of Financial Sector	eidas@cssf.lu
Malta	Malta Financial Services Authority	aubankingfis@mfsa.com.mt
Netherlands	The Netherlands Bank	infobetaalinstellingen@dnb.nl
Poland	Polish Financial Supervision Authority	pspcert@knf.gov.pl
Portugal	Bank of Portugal	sp.psd2@bportugal.pt
Romania	National Bank of Romania (1)	
Slovakia	National Bank of Slovakia	eIDAS.psd2@nbs.sk
Slovenia	Bank of Slovenia	PSD2.porocanje@bsi.si
Spain	Bank of Spain	pspsupervision@bde.es
Sweden	Swedish Financial Supervisory Authority	finansinspektionen@fi.se

(1) Autoridad Nacional Competente que no ha comunicado su dirección de email y que no autoriza la emisión de certificados a las entidades que se encuentran bajo su supervisión)

(2) Autoridad Nacional Competente que no desea recibir comunicaciones de Prestadores de Servicios de Confianza (QTSPs) salvo en los siguientes supuestos:

- Notificación de que el QTSP ha emitido un certificado a un proveedor de servicios de pago autorizado por dicha Autoridad,
- Información de como remitir una petición de revocación autenticada para certificados emitidos por el QTSP .

10.- Anexo II

Type of identification numbers used in the EBA PSD2 Register and the EBA Credit Institutions Register

Version 1, published on 31st July 2019. [11]

Country	Type of national identification numbers used in the EBA registers for:			
	Payment institutions	E-money institutions	Exempted AISPs (Article 33 of PSD2)	Credit institutions*
Austria	**Trade register number** (Firmenbuchnummer)	**Trade register number**	**Trade register number**	**Registration number –** BLZ (Bank code assigned by the CA)
Belgium	**Tax identification number:** KBO/BCE number (Kruispuntbank van Ondernemingen/Banque-Carrefour des Entreprises) - "0" + the VAT-Number	**Tax identification number:** KBO/BCE number - "0" + the VAT-Number	**Tax identification number:** KBO/BCE number - "0" + the VAT-Number	**Tax identification number:** KBO/BCE number - "0" + the VAT-Number
Bulgaria	**Trade register number** - ЕИК (UIC)	**Trade register number** - ЕИК (UIC)	N/A	**Trade register number** - ЕИК (UIC)
Croatia	**Registration number** (Assigned by the CA)	**Registration number** (Assigned by the CA)	**Registration number** (Assigned by the CA)	**Tax identification number** – Personal Identification Number (Osobni identifikacijski broj - OIB).
Cyprus	**Authorisation number** (Assigned by the CA)	**Authorisation number**	**Authorisation number**	**Trade register number** – Company registration number
Czech Republic	**Trade register number** - Personal identification number (Identifikační číslo osoby - IČO)	**Trade register number** - IČO	**Trade register number** - IČO	**Trade register number** - IČO
Denmark	**Trade register number** - CVR number (Central Business Register number) and a VAT number	**Trade register number** - CVR number and a VAT number	**Trade register number** - CVR number and a VAT number	Not yet available. Expected to be the CVR number.
Estonia	**Trade register number** – legal entity identifier	**Trade register number**	**Trade register number**	**Trade register number**
Finland	**Trade register number** - Business ID	**Trade register number** - Business ID	**Trade register number** - Business ID	**Trade register number** - Business ID
France	**Trade register number** - SIREN	**Trade register number** - SIREN	**Trade register number** - SIREN	**Authorisation number** - CIB – code interbancaire (assigned by the CA)
Germany	**Authorisation number**	**Authorisation number**	**Authorisation number**	**Authorisation number**

[11] https://eba.europa.eu/documents/10180/2882455/Identification+numbers+in+the+EBA+registers.pdf

Greece	**Tax Identification Number**	**Tax Identification Number**	**Tax Identification Number**	**Tax Identification Number**
Hungary	**Registration number** (Assigned by the CA)	**Registration number**	**Registration number**	**Registration number**
Iceland				
Ireland	**Authorisation number**	**Authorisation number**	**Authorisation number**	Not yet available. Will investigate providing an authorisation number.
Italy	**Tax Identification Number**	**Tax Identification Number**	**Tax Identification Number**	**Authorisation number** – national credit register number (assigned by the CA)
Liechtenstein				
Latvia	**Registration number** (Assigned by the CA)	**Registration number**	**Registration number**	**Tax Identification Number** – VAT numbers
Lithuania	**Trade register number** - Legal entity's code	**Trade register number**	**Trade register number**	**Trade register number**
Luxembourg	**Authorisation number**	**Authorisation number**	**Authorisation number**	**Authorisation number**
Norway	**Trade register number**	**Trade register number**	**Trade register number**	**Trade register number**
Malta	**Trade register number**	**Trade register number**	**Trade register number**	**Trade register number**
Netherlands	**Authorisation number** - Relation number DNB (Relatienummer DNB)	**Authorisation number**	**Authorisation number**	**Authorisation number**
Poland	**Tax Identification Number**	**Tax Identification Number**	**Tax Identification Number**	**Tax Identification Number**
Portugal	**Authorisation number**	**Authorisation number**	**Authorisation number**	**Authorisation number**
Romania	**Tax Identification Number** – to be used following the transposition of PSD2	**Tax Identification Number** – to be used following the transposition of PSD2	**Tax Identification Number** – to be used following the transposition of PSD2	**Registration number** (Assigned by the CA)
Slovakia	**Trade register number** - IČO	**Trade register number** - IČO	**Trade register number** - IČO	**Trade register number** - IČO
Slovenia	**Trade register number**	**Trade register number**	**Trade register number**	N/A (LEI Code only)
Spain	**Authorisation number** (referred to as a registration number by the CA)	**Authorisation number** (referred to as a registration number by the CA)	**Authorisation number** (referred to as a registration number by the CA)	**Authorisation number** (referred to as a registration number by the CA)
Sweden	**Authorisation number** - FI identification number (Institutsnummer hos FI)	**Authorisation number** - FI identification number (Institutsnummer hos FI)	**Authorisation number** - FI identification number (Institutsnummer hos FI)	**Trade register number** - Corporate ID number (Organisationsnummer)
United Kingdom	**Authorisation number**	**Authorisation number**	**Authorisation number**	**Authorisation number**

* Para las entidades de crédito, este es el tipo de número de identificación nacional insertado en el campo “National Reference Code” (Código de referencia nacional) en el EBA CIR, que es adicional al código del Identificador de entidad legal (LEI).

Cuando no conste que la NCA a cargo del registro haya establecido otro procedimiento, se hará uso del registro consolidado de la EBA

- https://euclid.eba.europa.eu/register/pir/search

11.- Anexo III

Codificación normalizada de roles para incluir en los certificados

Los roles se identifican con las siguientes siglas:

- account servicing (PSP_AS);
- payment initiation (PSP_PI);
- account information (PSP_AI);
- issuing of card-based payment instruments (PSP_IC).

12.- Anexo IV

National identification codes to be used by qualified trust service providers for identification of competent authorities in an eIDAS certificate for PSD2 purposes

Version 1, published on 31st July 2019. [12]

Code	Country	Authority Title
AT-FMA	Austria	Austrian Financial Market Authority
BE-NBB	Belgium	National Bank of Belgium
BG-BNB	Bulgaria	Bulgarian National Bank
HR-HNB	Croatia	Croatian National Bank
CY-CBC	Cyprus	Central Bank of Cyprus
CZ-CNB	Czech	Czech National Bank
DK-DFSA	Denmark	Danish Financial Supervisory Authority
EE-FI	Estonia	Estonia Financial Supervisory Authority
FI-FINFSA	Finland	Finnish Financial Supervisory Authority
FR-ACPR	France	Prudential Supervisory and Resolution Authority
DE-BAFIN	Germany	Federal Financial Supervisory Authority
GR-BOG	Greece	Bank of Greece
HU-CBH	Hungary	Central Bank of Hungary
IS-FME	Iceland	Financial Supervisory Authority
IE-CBI	Ireland	Central Bank of Ireland
IT-BI	Italy	Bank of Italy
LI-FMA	Liechtenstein	Financial Market Authority Liechtenstein
LV-FCMC	Latvia	Financial and Capital Markets Commission
LT-BL	Lithuania	Bank of Lithuania
LU-CSSF	Luxembourg	Commission for the Supervision of Financial Sector
NO-FSA	Norway	The Financial Supervisory Authority of Norway
MT-MFSA	Malta	Malta Financial Services Authority
NL-DNB	Netherlands	The Netherlands Bank
PL-PFSA	Poland	Polish Financial Supervision Authority
PT-BP	Portugal	Bank of Portugal
RO-NBR	Romania	National Bank of Romania
SK-NBS	Slovakia	National Bank of Slovakia
SI-BS	Slovenia	Bank of Slovenia
ES-BE	Spain	Bank of Spain
SE-FINA	Sweden	Swedish Financial Supervisory Authority
GB-FCA	United Kingdom	Financial Conduct Authority

Otros registros pueden usar guión bajo ("_") en lugar de guión menos ("-"), pero en el contexto del presente documento se requiere guión menos cuando se vincula el código de país con un identificador NCA

[12] https://eba.europa.eu/documents/10180/2882455/NCA+abbreviations+for+inclusion+in+eIDAS+certificates.pdf