European Agency of Digital Trust

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

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

Octubre 2019
Versión 1.3

Tabla de Contenido

1.- Introducción

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

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

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

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

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

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]

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

[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

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.

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.

3.- Administración de políticas

3.1.- Organización que administra el documento

EADTrust 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:

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.

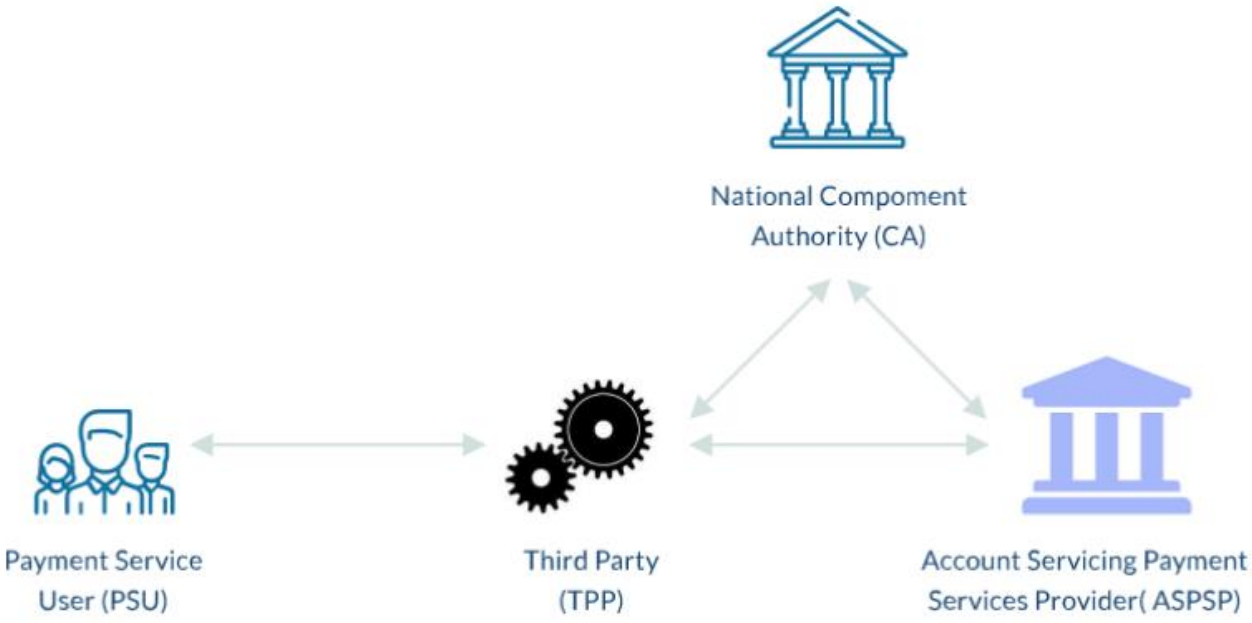
Para certificados cualificados web:

- 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 CA's raíz siempre se mantienen offline, emitiéndose los certificados para los subscriptores, desde las Sub-CA's correspondientes.

4.2.- 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 gestoes de cuenta (ASPSP) que usan los certificados o confían en ellos.



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 de 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 renovación de certificados de persona física representante (lo que no es de aplicación en los certificados PD2), de persona jurídica y de certificados para servidor web, se valida el nombre de la organización introducido durante la inscripción, que se hace constar en el campo apropiado del certificado.

La organización a la que se atribuye un certificado debe ser una entidad activa, confirmada por una autoridad oficial responsable del registro de empresas dentro de la jurisdicción específica (localidad, estado, país) indicada en la solicitud del certificado. El nombre de la organización inscrita y el nombre alegado deben coincidir literalmente. En caso de existir abreviaturas, solo se aplicarán a las partes que identifican el tipo legal de sociedad o entidad (S.A., S.L., S. COOP., LLC, Ltd).

En el caso de certificados expedidos a servidores web, se comprobará que la titularidad del nombre de dominio corresponde a la organización, y se solicitará confirmación a las direcciones de correo que figuran asociadas al dominio a través del servicio WHOIS.

Si la entidad hace uso en su DNS de las extensiones[3] 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.

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

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 renovación de certificados, 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.
- 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.

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.

Ver apartado **6.6.3.**

6.4.- Emisión del Certificado

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

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

Los certificados se pueden emitir en un token criptográfico, en una tarjeta inteligente, en HSM o en un soporte de software.

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

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

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

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

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

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

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

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

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

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

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

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”[4]

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.- Revocación y suspensión del certificado

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

6.6.1.- 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.
- Que hayan transcurrido 3 meses desde el momento en que se solicita la certificación sin que se recoja el certificado.
- Si EADTrust recibe una solicitud para la emisión del certificado y ya existe un certificado válido de la misma clase y unicidad, el certificado válido será revocado a petición del solicitante.

6.6.2.- Quién puede solicitar la revocación

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

Entre otros solicitantes indicados en las políticas de certificación con las que se relaciona la presente política, pueden solicitar la revocación de certificados PSD2 organismos supervisores (Autoridades Nacionales Competentes).

6.6.3.- Procedimiento para la solicitud de revocación

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.

La revocación se procesará en un tiempo menor de 24 horas.

Una vez 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.

Ver el apartado **6.3** en relación con otros aspectos de la revocación de certificados.

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.
- 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 254 bits (prime256v1) or 384 bits (secpr384r1)
extensions		
subjectAltName		
dnsName		DNS name(s)
extendedKeyUsage		serverAuth, clientAuth
subjectKeyIdentifier		Derived from the result of applying the hash to the public key of the subject
authorityKeyIdentifier		Derived from the result of applying the hash to the Public key of the issuing CA
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.0.41243
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

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 254 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		
caIssuers		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

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.

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[5].

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

[5] 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. [6]

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**

[6] 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. [7]

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

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