11-10-2024

Declaración de Prácticas de Servicios de Confianza (DPC)

CERTIFICADOS Y SELLOS DE TIEMPO

Versión 5.4

OID 1.3.6.1.4.1.501.10.1.1

EADTrust Policy Committee

EADTRUST EUROPEAN AGENCY OF DIGITAL TRUST

Nota sobre derechos de autor

Versiones del documento

Esta publicación podría incluir inexactitudes técnicas o errores tipográficos.

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

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

Aprobado por ***9451** EDUARDO INZA (R ****2624*) el día 09/05/2025 con un certificado emitido por EADTrust RSA 4096 SubCA

Certificación ISO 9001, ISO 27001, ISO 20000-1 y ENS Nivel alto

EADTrust ha superado diversas auditorías, y, en particular las relativas a las normas ISO 9001, ISO 27001, ISO 20000-1 y ENS de nivel alto, 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. Ha superado además las auditorías requeridas como Prestador Cualificado de Servicios de Confianza y figura en la lista TSL correspondiente e España

Certificados:

Los certificados de cumplimiento se identifican con los siguientes números de serie:

Norma	Certificado
ISO 20000-1:2018	STI-0163/22
ISO 27001:2013	SI-0318/20
ISO 9001:2015	EC-9180/20
ENS nivel alto	ENS-0271/22

Prestador de Servicios Electrónicos de Confianza Cualificado
(Acreditación)

EADTrust ha superado la auditoría de acreditación como **Prestador Cualificado de Servicios de Confianza** de acuerdo con el 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 por el que se deroga la Directiva 1999/93/CE, que le habilita para prestar los siguientes servicios:

- Emisión de Certificado Cualificado de Persona Física para Firma Electrónica (Art. 28 del Reglamento eIDAS),
- Emisión de Certificado Cualificado de Persona Jurídica para Sello Electrónico (Art. 38 del Reglamento eIDAS),
- Emisión de Certificado Cualificado de Autenticación de Sitio Web (Art. 45 del Reglamento eIDAS),
- Sellos de Tiempo Electrónicos Cualificados (Art. 42 del Reglamento eIDAS).

CSQA Certificazioni (Conformity Assessment Body que evalúa a EADTrust) ha asignado el número de certificado **58813**.

El Ministerio para la Transformación Digital y de la Función Pública de España mantiene una Lista de Proveedores de Servicios de Confianza (TSL) que corresponde a los proveedores que prestan servicios electrónicos cualificados de confianza y que están establecidos y supervisados en España, en línea con la citada legislación. EADTrust fue incluida en esta lista desde el 7 de octubre de 2020.

Puede consultarse el registro en la TSL en el documento siguiente:

- https://sedediatid.mineco.gob.es/Prestadores/Paginas/Inicio.aspx

También hay una herramienta para consultar los servicios cualificados de diferentes Prestadores de Confianza europeos en:

- EU Trust Services Dashboard (europa.eu)
  https://esignature.ec.europa.eu/efda/tl-browser/#/screen/home

En aplicación del Reglamento de Ejecución (UE) 2015/806 de la Comisión de 22 de mayo de 2015 por el que se establecen especificaciones relativas a la forma de la etiqueta de confianza «UE» para servicios de confianza cualificados, EADTrust puede ostentar del símbolo de Servicios Cualificados:

Tabla de Contenidos

1 Contenido

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	23/09/08	Ninguno	Root EADTrust certification practice statement.
1.2	16/09/09	Versión 1	Aclaraciones sobre la emisión de certificados.
1.3	25/01/10	Versión 1.2	Adaptaciones y aclaraciones sobre los requisitos MITyC.
1.4	30/03/11	Versión 1.3	Inclusión de prácticas y políticas de servicios de confianza.
2.0	12/03/17	Versión 1.4	Sustitución completa debido a cambios regulatorios y cumplimiento con el Reglamento europeo UE 910/2014 (eIDAS).
2.1	12/06/18	Versión 2.0	Adecuación al Reglamento (UE) 679/2016 De Protección de Datos Personales (RGPD).
2.2	21/08/18	Versión 2.1	Inclusión de perfiles de certificados de persona física, representante de persona jurídica y de sello de entidad. Modificación del perfil de persona jurídica para selladde tiempo. Actualización de versiones a las que se hace referencia o de las normas EN 319 401, EN 319 411-1 y EN 319 411-2. Correción de errores tipográficos.
2.3	17/01/2019	Versión 2.2	Adición de CA Root y SubCA para-Web, inclusión de perfiles de certificados cualificados de empleado público, de web domain validated, web organization validated, web extended validation, Persona Jurídica para sello PSD2, Web PSD2. Modificación del perfil de persona jurídica para sello de tiempo. Revisión de OID de políticas. Correción de errores tipográficos.
2.4	05/05/2019	Versión 2.3	Adición de otros servicios no cualificados de comprobación fehaciente de contenidos de páginas web; generación y custodia de claves; custodia documental Cartulario, servicio de notificaciones fehacientes Noticeman y servicio de comprobación de validez de certificados.
2.5	01/07/2019	Versión 2.4	Revisión para incluir los certificados para PSD2 el resultado del Ballot SC 17 de CAB Forum relativo a organizationIdentifier
2.6	02/09/2019	Versión 2.5	Revisión para incluir mejoras identificadas en la auditoría eIDAS
2.7	03/10/2019	Versión 2.6	Revisión para incluir mejoras identificadas en la auditoría eIDAS
3.0	22/11/2019	Versión 2.7	Revisión para consolidar todas las mejoras identificadas en la auditoria interna eIDAS y las versiones internas de este documento.
4.0	23/04/2020	Versión 3.0	Revisión como parte del proceso de mejora continua e inclusión de la videoconferencia como medio de verificación y autenticación de identidad en la RA.
4.1	06 /05/2020	Versión 4.0	Revisión para incluir recomendaciones de auditores eIDAS
4.2	12/06/2020	Versión 4.1	Se introducen los OID`s de test en el servicio de timestamping

4.3	28/10/2020	Version 4.2	Se introducen los perfiles de certificado de sede electrónica y sello de órgano alineados con el documento "Perfiles de Certificados Electrónicos 2.0" de la AAPP. Se ha eliminado la información histórica del arco de OID 19126.
4.4	28/04/2021	Version 4.3	Se introducen las refencias a la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza. Y se eiliminan referencias a normativa derogada, con la aprobación de dicha ley, como la Ley 59/2003 de Firma electrónica.
4.5	16/06/2021	Versión 4.4	Se introducen perfiles DV, OV, EV no cualificados y se quitan de todos los perfiles web los OU informativos del tipo de certificado, el keyusage key encipherment (salta un error con las claves ECDSA en el lint) y los userNotices en todos los de web menos en sede electrónica que viene dado por el documento perfiles electrónicos del Ministerio de hacienda y administraciones públicas.
5.0	27/03/2022	Versión 4.5	Se reestructura el formato y contenidos de la DPC para adecuarla al estándar técnico ETSI EN 319 401. Abarca certificados para firma electrónica y para sello electrónico, incluyendo entidades PSD2. Se unifican en el texto de la DPC las políticas de emisión de certificados de personas físicas y personas jurídicas y la Política de Sello de tiempo. Se publica de forma separada una CPS en idioma inglés para certificados cualificados y no cualificados de web (DV, OV y EV, incluido QWAC PSD2). Se incluye la política QNCP-w para certificados cualificados OV y DV. Se trasladan a una nueva Declaración de Servicios, los servicios societarios y otros servicios no ofrecidos en el marco del Reglamento eIDAS. Se incluye una mención a los certificados emitidos en el contexto del "Pasaporte Verde Digital" frente al COVID19.
5.1	27/06/2023	Versión 5.0	Nuevo logo de la entidad. Se incluye mención a la certificación ENS. Se actualiza la información sobre los certificados de seudónimo de Justicia (en base al documento "CTEAJE - Perfil de Certificado con Seudónimo Justicia V1.0") que en ediciones anteriores estaban incluidos en los certificados de empleado público.Se aclaran aspectos relativos a los certificados PSD2. Se incluye una mención a los certificados EPREL. Se incluye la previsión de identificación para obtener un certificado (y para controlar la firma electrónica de forma remota) mediante la Cartera IDUE (EUDI Wallet). Se amplía la información de identificación del solicitante por Video. Se amplía la información de firma remota.
5.2	27/09/2023	Versión 5.1	Se amplía la información de firma remota, para reflejar mejor el cumplimento de las normas ETSI TS 119 431-1 y ETSI TS 119 431-2. Se introduce en el capítulo 10 por lo que renumera el resto. Reordenación de los certificados del capítulo 17.8
5.3	29/02/2024	Versión 5.2	Se actualizan referencias normativas y denominación del órgano supervisor
5.4	11/10/2024	Versión 5.3	Se actualiza el perfil de empleado público y se completan los OIDs de firma remota para los perfiles de empleado público y sello corporativo

TABLA2. DATOS DEL DOCUMENTO.

Propiedades del documento.	
Propietario	EADTrust European Agency of Digital Trust, S.L.
Fecha	11 de octubre de 2024

Distribución	Público
Nombre / Código	OPR-PG- v5.4 - Declaración_Prácticas_Certificación_DPC_EADTrust

1 Introducción

Este documento recoge la **Declaración de Prácticas del Servicio de Confianza (a partir de ahora, DPC, siglas de la denominación anterior "Declaración de Prácticas de Certificación"),** que describe el conjunto de políticas y las prácticas de los servicios de emisión de certificados de personas físicas y personas jurídicas para la infraestructura de Clave Pública (ICP, en inglés, PKI, Public Key Infraestructure), de EADTrust, European Agency of Digital Trust SL (en Adelante EADTrust). La entidad pertenece al Grupo **Garrigues**.

Los servicios descritos en este documento cumplen 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**); así como, los definidos en la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

El marco de referencia para la redacción y estructura de contenidos de esta Declaración de Prácticas de Certificación es el Estándar Técnico ETSI EN 319 401 (V2.3.1 (2021-05); en consecuencia, se describe cada uno de sus apartados conforme al citado estándar técnico y en su orden. Adicionalmente, se han tomado en consideración los requisitos operacionales definidos en las normas ETSI EN 319 411 1 y 2; ETSI EN 319 412 1 a 5 ETSI EN 319 421, ETSI EN 319 422, etc. También los definidos en RFC 6844 (IETF, 2013) y otras referencias normativas e informativas.

EADTrust CA, es una jerarquía de Certificación gestionada y propiedad de EADTrust que comprende:

- 13 autoridades de certificación raíz o Root
- 18 autoridades de certificación intermedias o Sub CA´s

Existe además una jerarquía (Root CA y Sub-CA) para emitir certificados *no cualificados*, en base a la que emiten certificados de una de las modalidades de sello de tiempo cualificado.

Los certificados digitales amparados en esta DPC pueden emitirse en los siguientes modos o formatos:

- Cuando la clave la genera EADTrust
  - En modo software (formato PKCS#12)
  - En modo token criptográfico (Dispositivo Cualificado de Creación de Firma)
  - En la nube, con claves generadas y gestionadas en un HSM criptográfico (Dispositivo Cualificado de Creación de Firma)

- Cuando la clave la genera el solicitante (y remite el CSR en formato PKCS#10)
  - En formato PEM (base 64 con extensión crt)
  - En formato DER (binario).

En el caso de los certificados de Persona Jurídica, se pueden usar Dispositivos Cualificados de Creación de Sello (DCCS / QSCD / HSM) gestionados por el solicitante o en su nombre.

1.1 Alcance

Este documento describe los servicios cualificados y no cualificados **de emisión, gestión, validación y revocación de Certificados de confianza pública** para:

- Autenticación y firma electrónica de personas físicas,
- Autenticación y firma electrónica de personas físicas, con indicación de entidad en la que trabajan,
- Autenticación y firma electrónica de representantes legales de personas jurídicas,
- Autenticación y firma electrónica de empleados públicos,
- Autenticación y firma electrónica de empleados públicos, en el contexto de la Administración de Justicia
- Autenticación y sello electrónico de personas jurídicas,
- Autenticación y sello electrónico de órganos de la administración pública,
- Autenticación y sello electrónico de personas jurídicas sujetas a la normativa PSD2[1],
- La creación de sellos de tiempo electrónicos cualificados,
- La comprobación y validación de firmas electrónicas, sellos electrónicos, y de sellos de tiempo electrónicos,
- La conservación de firmas electrónicas, sellos o certificados para estos servicios

Entre los servicios de sello electrónico de órgano de la administración pública, se generan certificados para realizar el sellado de Pasaportes COVID de la Unión Europea (**DSC** - Document Signing Certificate), lo que puede conllevar la inclusión de OID específicos en los certificados de entidad final:

- OID 1.3.6.1.4.1.1847.2021.1.1 — válido para certificados que indiquen resultados de test COVID.
- OID 1.3.6.1.4.1.1847.2021.1.2 — válido para certificados que indiquen vacunación COVID
- OID 1.3.6.1.4.1.1847.2021.1.3 — válido para certificados que indiquen que se ha superado la enfermedad

De no incluirse ningún OID de los citados, el Certificado DSC es válido para firmar cualquier tipo de pasaporte COVID.

La Sub-CA de EADTrust ECC 256 SubCA For Qualified Certificates 2019/OU=Legal Person tiene la consideración de **CSCA** (Certificate Signing Certificate Authority) de España, en el contexto de los pasaportes COVID.

Los certificados de Persona Jurídica de EADTRUST son válidos para registrar productos en **EPREL** (Registro Europeo de Productos para el Etiquetado Energético). Responden a los requisitos de la abreviatura QSEAL (Sello Cualificado).

También se prestan servicios de creación de sellos de tiempo electrónicos no cualificados.

Se contempla la posibilidad de identificación remota de solicitantes de certificados de persona física (y, a partir de esa identificación la prestación de otros servicios de confianza) de acuerdo con la Orden

[1]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

Ministerial ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados.[2]

La implementación del procedimiento por EADTRUST está alineada con la norma ETSI TS 119 461 ("Policy and security requirements for trust service components providing identity proofing of trust service subjects).[3]

Estos servicios se brindan al público en general, normalmente a cambio de una remuneración, con las excepciones que EADTrust considere apropiadas y en correspondencia con la legislación vigente.

Este documento **no abarca** los servicios cualificados y no cualificados **de emisión, gestión, validación y revocación de Certificados de confianza pública** para:

- **Autenticación de sitios web**, Domain Validated (DV), Organization Validated (OV), Extended Validation (EV), sede electrónica de la administración pública, QWAC (Qualified Web Authentication Certificate, certificados cualificados basados en certificados EV) y QWAC para entidades PSD2;
- Firmas de aplicación y código,
- Certificados wildcard y multidominos.
- Certificados con políticas QEVCP-w o QNCP-w

Salvo en aspectos básicos en relación con el marco europeo. Este tipo de certificados se recogen en una CPS separada, como se indica a continuación.

Las políticas y prácticas de los certificados de **sitio web** de EADTrust se definen en el documento "Publicly-Trusted-Certificates-EADTrust (CPS)". Dicho documento cumple la normativa técnica y jurídica desarrollada en el marco del Reglamento eIDAS, el marco de la norma RFC 3647 del IETF y los requisitos denominados "Baseline Requirements"[4] y "EV TLS Certificate Guidelines"[5] para la emisión y la gestión de certificados confiables publicados por la entidad CA/B fórum y disponibles en su sitio web: http://www.cabforum.org

Puede consultarse la "Publicly-Trusted-Certificates-EADTrust (CPS)" en:

- https://eadtrust.eu/download/6993/

1.2 Nombre e identificación del documento

El nombre de este documento es "Declaración de Prácticas de Servicios de Confianza (DPC). Se le ha asignado el siguiente **OID a este documento: 1.3.6.1.4.1.501.10.1.1**

[2] Modificada por la Orden ETD/743/2022, de 26 de julio, por la que se modifica la Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados.

[3] https://www.etsi.org/deliver/etsi_ts/119400_119499/119461/01.01.01_60/ts_119461v010101p.pdf

[4] https://cabforum.org/working-groups/server/baseline-requirements/documents/

[5] https://cabforum.org/working-groups/server/extended-validation/documents/

2 Participantes de la PKI

2.1 Autoridades de certificación

Las Autoridades de Certificación (CAs) de EADTrust para la emisión de certificados cualificados y no cualificados de persona física y de entidad jurídica incluidos los de órganos de las AAPP (con perfiles específicos para la Administración de Justicia) y entidades PSD2, están organizadas en jerarquías de dos niveles, con varias CAs raíz offline, adaptadas a las normas y prácticas actuales del sector, desde el punto de vista tecnológico.

Se contemplan algoritmos criptográficos de tipo RSA con tamaños de clave de 2048 bits, 4196 bits y 8192 bits y algoritmos criptográficos de tipo ECC (Criptografía de Curva Elíptica) con tamaños de clave de 256 bits y 384 bits.

Los diferentes niveles de robustez de criptografía permiten el cumplimiento de los niveles medios y altos del ENS (Esquema Nacional de Seguridad) de España, tal como se describen en el documento "Guía de Seguridad de las TIC - CCN-STIC 807 - Criptología de empleo en el Esquema Nacional de Seguridad" [6]según las necesidades de las Administraciones Públicas.

Los tamaños de clave para los certificados cualificados son:

- RSA Root CA 2048-bit key 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.
- ECC Root CA P-384 with SHA384 digest algorithm para certificados cualificados.

Para certificados no cualificados

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

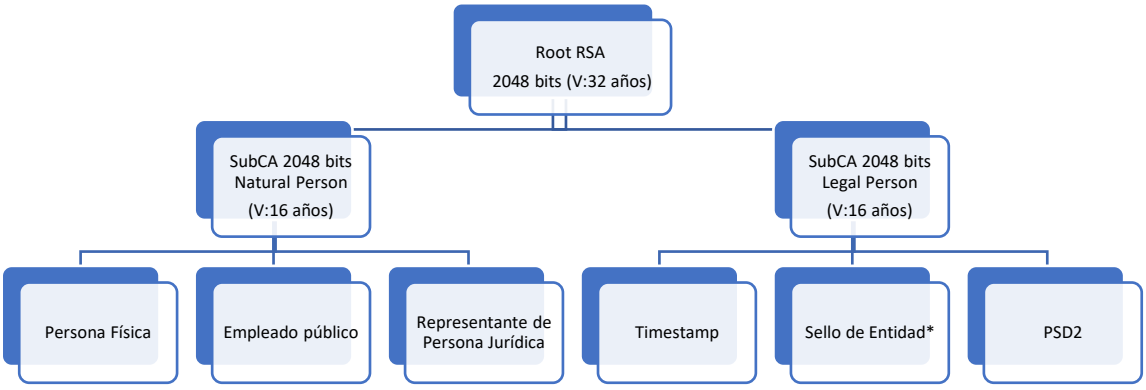
Esta jerarquía emite certificados no cualificados para sello de tiempo cualificado.

[6] https://www.ccn-cert.cni.es/es/series-ccn-stic/guias/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/513-ccn-stic-807-criptologia-de-empleo-en-el-ens/file.html

Gráficamente:

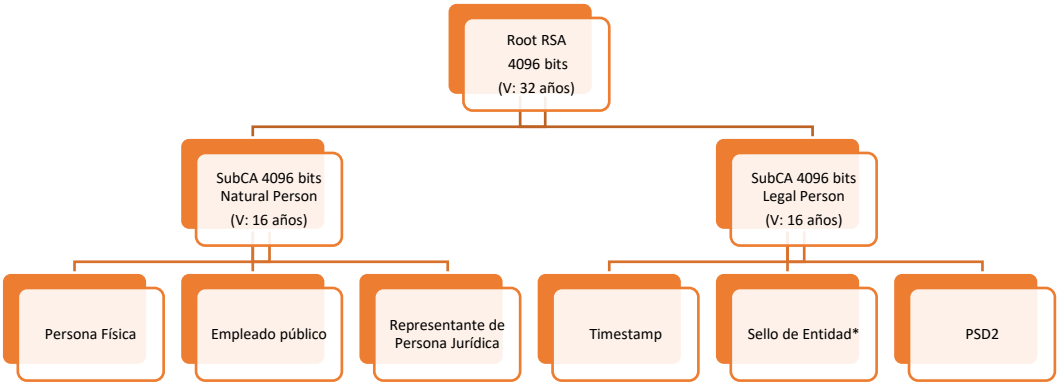
Root's Cualificadas para Certificados:

- Algoritmo RSA, tamaño 2048 bits



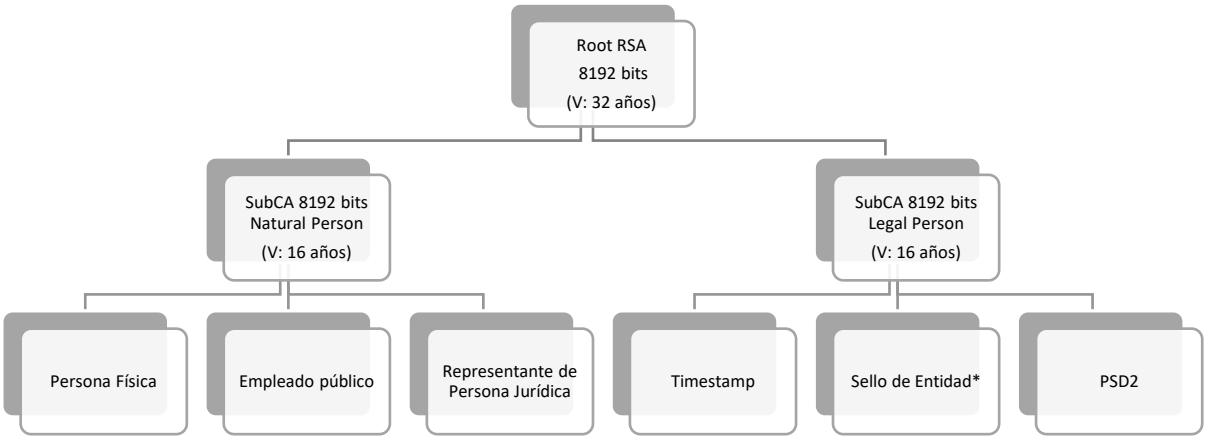
(*) Entre los sellos de entidad se incluyen los sellos de órgano con perfil de las AAPP.

- Algoritmo RSA, tamaño 4096 bits



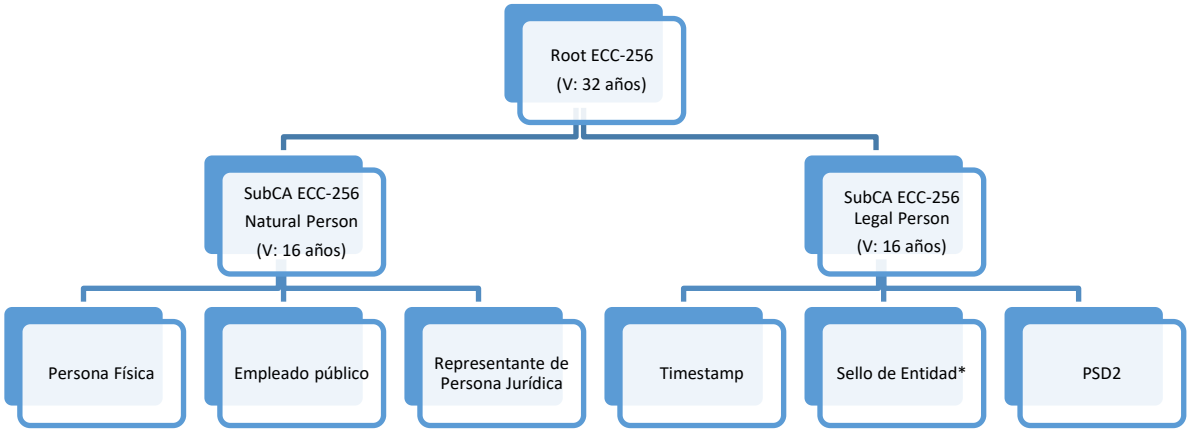
(*) Entre los sellos de entidad se incluyen los sellos de órgano con perfil de las AAPP.

- Algoritmo RSA, tamaño 8192 bits



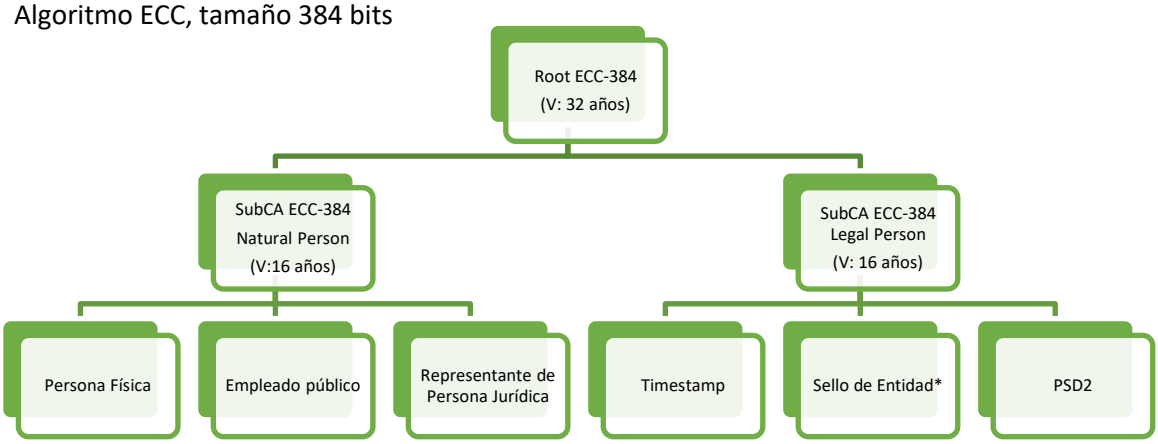
(*) Entre los sellos de entidad se incluyen los sellos de órgano con perfil de las AAPP.

- Algoritmo ECC, tamaño 256 bits



(*) Entre los sellos de entidad se incluyen los sellos de órgano con perfil de las AAPP.

- Algoritmo ECC, tamaño 384 bits



(*) Entre los sellos de entidad se incluyen los sellos de órgano con perfil de las AAPP.

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 (Issuing CA).

Normalmente, cada raíz de EADTrust cuenta con una o dos CAs intermedias para emisión de certificados de entidad final para suscriptores.

Además, como prestador de servicios, EADTrust opera una RSA Root CA de 2048 bits con algoritmo de función compendio o resúmen (hash) SHA256 offline, dedicada a emitir certificados "internos". Estos certificados sólo se proporcionan a los participantes de la PKI que acceden a los servicios prestados por EADTrust, con el fin de identificarlos y autenticarlos en ese contexto.

Cada CA firma su propia CRL y las respuestas OCSP se firman por la SubCA correspondiente. El propio certificado de entidad final contiene la información del endpoint en el que se obtiene la CRL o al que se puede consultar el servicio OCSP. Existe un perfil de certificado OCSP de uso opcional para servidores OCSP externos.

Existe un perfil de certificado OCSP para su emisión a entidades externas que ofrezcan servicios de validación independientes del prestador que emitió los certificados (OCSP multi-CA o Proxy) que se consultan.

Se incluye a continuación una tabla que recoge por cada certificado de la jerarquía su hash, en base al algoritmo SHA-256 y su denominación (CN, common name).

Denominación	Fingerprint SHA1	Tipo
CN=EADTrust ECC 256 Root CA For Qualified Certificates 2019	1FBE6EC155A781C727BC529B533EDA2A0627C567	Root
CN=EADTrust ECC 384 Root CA For Qualified Certificates 2019	FB20B3C5541E4C97DDD31F0B5D71CCD190D14BA8	Root
CN=EADTrust RSA 2048 Root CA For Non-Qualified Certificates 2019	F258783EC7D95A600073AAD59C5B8AD71CC507DC	Root
CN=EADTrust RSA 2048 Root CA For Qualified Certificates 2019	9D8D83379B08367CA1CE04B6A131AB27CFD43844	Root
CN=EADTrust RSA 4096 Root CA For Qualified Certificates 2019	B591E1174767810CC783E5CB07BA1F235FE31560	Root
CN=EADTrust RSA 8192 Root CA For Qualified Certificates 2019	BDABBA2FA168ADD556BDAB8379B7444C2C187859	Root
CN=EADTrust ECC 256 SubCA For Qualified Certificates 2019/OU=Legal Person	E68E26F21DCEB4F4E0D6AE1D30D46C98F2ACBC53	SubCA
CN=EADTrust ECC 256 SubCA For Qualified Certificates 2019/OU=Natural Person	D6CC5E28482FB5B75E8BA4EC78ABE9BFAB40C134	SubCA
CN=EADTrust ECC 384 SubCA For Qualified Certificates 2019/OU=Legal Person	296DC314845CBB7F3582575822DD54C744921C75	SubCA
CN=EADTrust ECC 384 SubCA For Qualified Certificates 2019/OU=Natural Person	9F36AA7F22F51E94EF265910A2F4429C2152B8DB	SubCA
CN=EADTrust RSA 2048 SubCA For Qualified Certificates 2019/OU=Legal Person	B799FC1C931E5EA8EF3117474CEBD3DCC9EFDE3D	SubCA
CN=EADTrust RSA 2048 SubCA For Qualified Certificates 2019/OU=Natural Person	E3FC4D9713E082BD55D69EA6F210BA77619197A9	SubCA
CN=EADTrust RSA 2048 SubCA For Non-Qualified Certificates 2019	3A5282560B9594300C6DB67A259766F5403BDF5A	SubCA
CN=EADTrust RSA 4096 SubCA For Qualified Certificates 2019/OU=Legal Person	6CFD78D91F9B1839A1A54F72609EDFC893E0DE89	SubCA

Denominación	Fingerprint SHA1	Tipo
CN=EADTrust RSA 4096 SubCA For Qualified Certificates 2019/OU=Natural Person	FADAF7FA8B9FBF505CCD82A75DDBFCB04C8A480B	SubCA
CN=EADTrust RSA 8192 SubCA For Qualified Certificates 2019/OU=Legal Person	0B46B3C789350D1C4BA3A941A18C78B165D4B5D6	SubCA
CN=EADTrust RSA 8192 SubCA For Qualified Certificates 2019//OU=Natural Person	B0CEC5130FB3A8A0559A560D33D643BEFEF50B34	SubCA

Pueden emitir Certificados bajo la jerarquía EADtrust las Autoridades de Certificación operadas por organizaciones externas cuyas Políticas o DPC estén conformes con las Política de Certificación contempladas en en esta DPC y en la CPS para certificados de web y hayan sido previamente autorizadas.

Existirá una relación escrita formal y contractual entre las organizaciones externas y EADTrust para dar cobertura a los compromisos mutuos.

2.2 Autoridades de registro

La emisión de certificados de EADTrust requiere la verificación de identidad previa del Solicitante/ Suscriptor del servicio. Esta se lleva a cabo a través de la Autoridad de Registro (AR, en inglés, RA, Registration Authorities) propia o de Autoridades de registro delegadas o externas.

Las RA´s externas que cooperan en la jerarquía PKI de EADTrust, actúan de acuerdo con las Políticas y prácticas del servicio, y otros documentos relativos al ciclo de vida del certificado. Adicionalmente, están obligadas a superar la evaluación anual de cumplimiento obligatoria realizada por EADTrust o cualquier tercero evaluador o auditor designado por este. La colaboración de las RAs se instrumenta a partir de una relación escrita formal y contractual con EADTrust.

Los acuerdos con asociaciones o colectivos se instrumentarán en base a acuerdos marco a los que se podrán adherir los profesionales o despachos participantes en la red de RAs de EADTrust.

La entidad que actúe como Autoridad de Registro de EADTrust podrá autorizar a una o varias personas como operador de la RA para operar con el sistema de emisión de certificados de EADTrust en nombre de la Autoridad de Registro.

También podrán ser Autoridades de Registro sujetas a esta Declaración de Prácticas de Certificación, las unidades designadas para esta función por los suscriptores de los certificados, como un departamento de personal, dado que disponen de los registros auténticos acerca de la vinculación de los firmantes con el suscriptor.

En el contexto de los certificados emitidos para personas relacionadas con el sector público, administraciones públicas y administración de Justicia se tendrán en consideración los requerimientos específicos de cada organismo público.

Las RA´s internas y externas son autoridades delegadas de la CA, aunque es la CA, en última instancia, la responsable del servicio,

EADTrust ha estructurado el servicio de verificación de identidad mediante RAs de la manera siguiente:

- Verificación de identidad presencial: con personación en las instalaciones de EADTrust o de la RA colaboradora.
- Verificación de identidad en presencia notarial haciendo constar en el documento notarial la legitimación de firma y, cuando corresponda, las atribuciones del firmante, por ejemplo, en relación con una entidad.
- Verificación de identidad a distancia mediante:
  - Firma electrónica avanzada basada en un certificado cualificado, que se haya emitido en base a una identificación presencial de la persona física o de un representante autorizado de la persona jurídica, o distancia, utilizando medios de identificación electrónica, para los cuales se haya garantizado la presencia de la persona física o de un representante autorizado de la persona jurídica previamente a la expedición del certificado cualificado, y que cumplan los requisitos establecidos con el artículo 8 del Reglamento UE 910/2014 con respecto a los niveles de seguridad «sustancial» o «alto».
  - Videoconferencia o videoidentificación (videonboarding) basada en la norma ETD/465/2021 (y Orden ETD/743/2022, de 26 de julio) según autorización del Organismo Supervisor[7].

Cuando la verificación de identidad se realice por firma electrónica avanzada basada en certificado cualificado y el certificado no incluya información sobre el número de documento de identidad, EADTrust podrá realizar comprobaciones adicionales para validar la identidad declarada, por lo que la Autoridad de registro de EADTrust podrá utilizar la videoconferencia como medio complementario de verificación de identidad. En estos casos se solicitará, previamente, el consentimiento del titular.

EADTrust podrá utilizar servicios externos de RA que realicen identificación a distancia basada en medios de identificación electrónica, para los cuales se haya garantizado la presencia de la persona física o de un representante autorizado de la persona jurídica previamente a la expedición del certificado cualificado, y que cumplan los requisitos establecidos con el artículo 8 con respecto a los niveles de seguridad

[7] Durante el estado de alarma decretado por el Real Decreto 463/2020, de 14 de marzo, ante la situación sanitaria de pandemia generada por el Covid-19, el órgano supervisor admitió, de manera provisional, métodos de identificación por videoconferencia basados en los procedimientos autorizados por el Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias o reconocidos para la expedición de certificados cualificados por otro Estado miembro de la Unión Europea. Así lo estableció la Disposición adicional undécima del Real Decreto-ley 11/2020, de 31 de marzo por el que se adoptan medidas urgentes complementarias en el ámbito social y económico, como medidas provisionales para la expedición de certificados electrónicos cualificados. En este marco, EADTrust notificó al Supervisor su método de verificación de identidad por videoconferencia. Al finalizar el estado de alarma estas autorizaciones provisionales decayeron. Actualmente, EADTrust ha adaptado su servicio de identificación remota a los requisitos establecidos en la Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados para ofrecer nuevamente el servicio. Este servicio se presta una vez superada la evaluación de conformidad y recibida la autorización del Organismo Supervisor.

«sustancial» o «alto». Estos servicios de terceros podrán complementar la modalidad de identificación indicada con mecanismos adicionales que utilicen otros métodos de identificación reconocidos a escala nacional que aporten una seguridad equivalente en términos de fiabilidad a la presencia física. La seguridad equivalente será confirmada por un organismo de evaluación de la conformidad. Si los servicios de RA los prestara un Proveedor de Servicios de Confianza de un tercer país, se requerirá la autorización por el Organismo Supervisor de Servicios Electrónicos de Confianza Cualificados de su país.

En atención a la norma ETSI TS 119 461 EADTrust podrá definir una Política específica para la gestión de identidades en la emisión y revocación de todos sus certificados. El documento contempla las pautas a seguir para la identificación y validación de la identidad declarada, la documentación a aportar y la operativa en cada tipo de solicitud. Mas detalles en:

- https://eadtrust.eu/documentos-vigentes/

Aparte de las RAs, EADTrust ha considerado la posibilidad de que otras empresas puedan prestarle otros servicios técnicos, lo cual no afectará al usuario.

2.3 Suscriptores

Se denominan como tal, en sentido genérico, a los usuarios de los servicios de emisión de certificados de EADTrust. En apartados precedentes se indican matices a este concepto.

Cuando en este documento, se utilice el término “suscriptores” en plural, se está haciendo referencia a todos los posibles usuarios del servicio: solicitante y suscriptor

Cuando en este documento se utilice el término “suscriptor” en singular se hace referencia al concepto definido en el apartado 2.3.2 de esta DPC.

2.3.1 Solicitante

Las personas físicas que, actuando en su propio nombre o de una persona jurídica (empresa, administración pública etc.), solicita el certificado y una vez lo ha obtenido, se erige titular de las claves privadas del certificado y lo utiliza.

El Solicitante puede ser a su vez Suscriptor del certificado cuando lo solicita para sí mismo.

Cuando solicita el certificado para una persona jurídica, la persona física se denominará Solicitante o Titular de las claves y la persona jurídica el Suscriptor.

Cuando EADTrust expida certificados para sus propios dominios, su propio personal, o sus servicios de sello de tiempo, se mantendrán las exigencias que apliquen a otros solicitantes; conservando los documentos que acrediten la identidad y la representación, según aplique. En todo momento, se garantizará la independencia e imparcialidad.

2.3.2 Suscriptor

La persona jurídica en cuyo nombre y representación una persona física ha solicitado el certificado electrónico. EADTrust no emite certificados en los que una persona física actúe como representante de otra persona física.

Durante el proceso de gestión de identidades desplegado por EADTrust se debe identificar tanto al Solicitante como al Suscriptor del certificado.

El documento de términos y condiciones generales y particulares del servicio de EADTrust obliga tanto al suscriptor como al solicitante del certificado.

2.3.3 Partes que confían

Persona física o jurídica que confía en una identificación electrónica o en un servicio de emitido bajo esta PKI.

Un resumen de lo que deben conocer los terceros que confían se encuentra disponible en el documento PDS (PKI Disclosure Statement), disponible en:

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

2.3.4 Titulares de certificados y terceros que confían en contextos PSD2

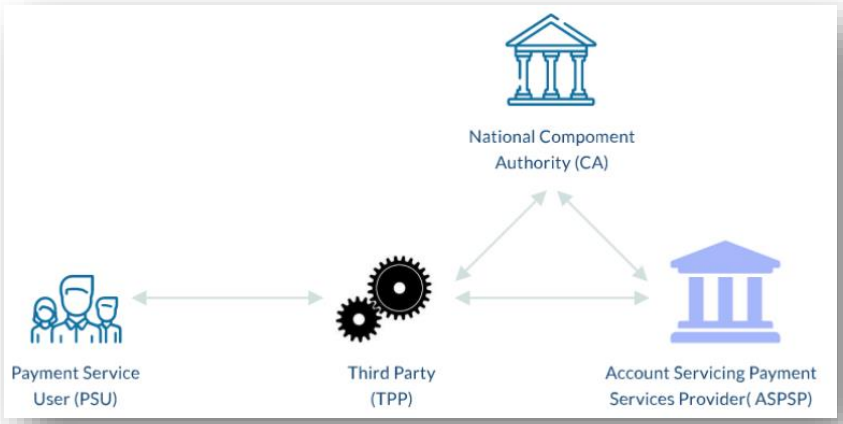
Al nivel de uso de los certificados considerados en este documento, son participantes de la PKI de EADTrust en contextos PSD2, las entidades proveedoras de servicios de pago (third party payment service provider - TPP) y gestores de cuenta (ASPSP) que usan los certificados o confían en ellos.

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

- **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.
- **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.
- **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.

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).

2.4 Usos del certificado

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

2.4.1 Usos adecuados del certificado

Los certificados garantizan la identidad del suscriptor y del titular de la clave privada; tambien permiten la generación de la “firma electrónica avanzada basada en certificado electrónico cualificado” y pueden utilizarse en aplicaciones como las que se indican a continuación:

a) Autenticación en sistemas de control de acceso.
b) Firma de correo electrónico seguro.
c) Otras aplicaciones de firma electrónica, de acuerdo con lo que acuerden las partes o con las normas jurídicas aplicables en cada caso.

Cuando se utilizan con dispositivos cualificados de creación de firmas, son adecuados para ofrecer soporte a la firma electrónica cualificada; en otras palabras, una firma electrónica avanzada respaldada en un certificado cualificado y basada en un dispositivo cualificado equivale a una firma manuscrita sin necesidad de satisfacer requisitos adicionales, según se establece en el Reglamento UE 910/2014.

También pueden utilizarse certificados de firma electrónica cualificados, si así se definen en el tipo de certificado correspondiente, para firmar mensajes de autenticación, en particular desafíos de cliente SSL o TLS, correo electrónico seguro S/MIME, cifrado sin recuperación de claves y otros. Esta firma digital de carácter técnico se utiliza para garantizar la identidad del suscriptor del certificado, pero no expresan conformidad con lo firmado. Los certificados cualificados se ajustan a la norma técnica EN 319 412 (documentos 1 a 5) del Instituto Europeo de Normas de Telecomunicaciones ETSI. Este uso de los certificados se entiende como “Autenticación”.

Si los certificados se emiten a personas jurídicas o entidades sin personalidad jurídica al objeto de crear sellos electrónicos se establecen consideraciones equivalentes a las de las firmas electrónicas, lo que da lugar a los sellos electrónicos avanzados basados en certificados cualificados y cuando estos se gestionan haciendo uso de dispositivos cualificados de creación de sello, a los sellos electrónicos cualificados.

El Reglamento Delegado (UE) 2018/389 de la Comisión, por el que se complementa la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo (PSD 2), sobre las normas técnicas de regulación para la autenticación reforzada de clientes contempla el uso de certificados cualificados para las comunicaciones entre entidades. Un PIISP, PISP o AISP deberá usar los 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.

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

2.4.2 Usos prohibidos del certificado

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

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

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

EADTrust no tiene acceso a los datos sobre los que se puede aplicar el uso de un certificado. Por lo tanto, y como consecuencia de esta imposibilidad técnica de acceder al contenido del mensaje, no es posible por parte de EADTrust emitir valoración alguna sobre dicho contenido, asumiendo por tanto el suscriptor, el firmante o la persona responsable de la custodia, cualquier responsabilidad dimanante del contenido aparejado al uso del certificado.

Así mismo le será imputable al suscriptor, al firmante o a la persona responsable de la custodia, cualquier responsabilidad que pudiese derivarse de la utilización del certificado fuera de los límites y condiciones de uso recogidas en esta Declaración de Prácticas de Certificación, los documentos jurídicos vinculantes con cada certificado, o los contratos o convenios con las entidades de registro o con sus suscriptores, así como de cualquier otro uso indebido del mismo derivado de este apartado o que pueda ser interpretado como tal en función de la legislación vigente.

3 Referencias

3.1 Referencias normativas

En el momento de revisar esta Declaración de Prácticas de Certificación, estaban vigentes las siguientes normas relativas a los servicios electrónicos de confianza:

- Reglamento (UE) 2016/679 del Parlamento europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.[8]
- 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 por el que se deroga la Directiva 1999/93/CE.[9]
- Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) nº 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital[10].
- Decisión de Ejecución (UE) 2015/296 de la Comisión de 24 de febrero de 2015. Por la que se establecen las modalidades de procedimiento para la cooperación entre los Estados miembros en materia de identificación electrónica con arreglo al artículo 12, apartado 7, del Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.[11]
- Reglamento de Ejecución (UE) 2015/806 de la Comisión de 22 de mayo de 2015. Por el que se establecen especificaciones relativas a la forma de la etiqueta de confianza «UE» para servicios de confianza cualificados.[12]
- Reglamento de Ejecución (UE) 2015/1501 de la Comisión de 8 de septiembre de 2015. Sobre el marco de interoperabilidad de conformidad con el artículo 12, apartado 8, del Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.[13]
- Reglamento de Ejecución (UE) 2015/1502 de la Comisión de 8 de septiembre de 2015. Sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica con arreglo a lo dispuesto en el artículo 8, apartado 3, del Reglamento (UE)

[8] http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679

[9] http://data.europa.eu/eli/reg/2014/910/oj

[10] https://eur-lex.europa.eu/eli/reg/2024/1183/oj

[11] http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:JOL_2015_053_R_0006&from=EN

[12] http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:JOL_2015_128_R_0006&from=ES

[13] http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:JOL_2015_235_R_0001&qid=1441792087678&from=ES

Nº 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.[14]

- Decisión de Ejecución (UE) 2015/1506 de la Comisión de 8 de septiembre de 2015. Por la que se establecen las especificaciones relativas a los formatos de las firmas electrónicas avanzadas y los sellos avanzados que deben reconocer los organismos del sector público de conformidad con los artículos 27, apartado 5, y 37, apartado 5, del Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.[15]
- Decisión de Ejecución (UE) 2015/1984 de la Comisión, de 3 de noviembre de 2015. Por la que se definen las circunstancias, formatos y procedimientos de notificación con arreglo al artículo 9, apartado 5, del Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior [notificada con el número C (2015) 7369].[16]
- Decisión de Ejecución (UE) 2016/650 de la Comisión, de 25 de abril de 2016. Por la que se fijan las normas para la evaluación de la seguridad de los dispositivos cualificados de creación de firmas y sellos con arreglo al artículo 30, apartado 3, y al artículo 39, apartado 2, del Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.[17]
- 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[18]
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.[19]
- Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados.[20]

En relación con los certificados de seudónimo y certificados de empleados públicos:

- Real Decreto 668/2015, de 17 de julio, por el que se modifica el Real Decreto 1671/2009 de 6 de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.[21]
- Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.[22]

[14] http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:JOL_2015_235_R_0002&qid=1441792087678&from=ES

[15] http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:JOL_2015_235_R_0006&qid=1441792087678&from=ESEnlaces-Legislacion

[16] http://www.boe.es/doue/2015/289/L00018-00025.pdf

[17] http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016D0650&from=EN

[18] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32015L2366

[19] https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-14046

[20] https://www.boe.es/eli/es/o/2021/05/06/etd465

[21] https://www.boe.es/buscar/doc.php?id=BOE-A-2015-8048

[22] https://www.boe.es/buscar/act.php?id=BOE-A-2021-5032

En relación con la información de fuente de tiempo:

- Real Decreto 1308/1992, de 23 de octubre, por el que se declara al Laboratorio del Real Instituto y Observatorio de la Armada como laboratorio depositario del Patrón Nacional de Tiempo y laboratorio asociado al Centro Español de Metrología.[23]
- Ley 32/2014, de 22 de diciembre, de Metrología.[24]

3.2 Referencias técnicas

- ETSI TS 119 612, Electronic Signatures and Infrastructures (ESI); Trusted Lists
- 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
- ETSI EN 319 403 V2.2.2 (2015-08), Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers.
- ETSI EN 319 401 V2.3.1 (2021-05)- Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- ETSI EN 319 411-1 V1.3.1 (2021-05)- Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- ETSI EN 319 411-2 V2.4.1 (2021-11) - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.
- ETSI EN 319 421 V1.1.1 (2016-03) - Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.
- ETSI TS 119 431-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev
- ETSI TS 119 431-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation
- ETSI TS 119 461 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects.
- FIPS 140 - 2, Federal Information Processing Standards Publication - Security Requirements for Cryptographic Modules, Information Technology Laboratory, National Institute of Standards and Technology, May 25, 2001.
- ISO 21188:2006, Public key infrastructure for financial services - Practices and policy framework. Network and Certificate System Security Requirements, v.1.0, 1/1/2013.
- NIST SP 800 - 89, Recommendation for Obtaining Assurances for Digital Signature Applications (URL).
- RFC2119, Request for Comments: 2119, Key words for use in RFCs to Indicate Requirement Levels, Bradner, March 1997.
- RFC2527, Request for Comments: 2527, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, March 1999.
- RFC3647, Request for Comments: 3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, November 2003.
- RFC4366, Request for Comments: 4366, Transport Layer Security (TLS) Extensions, Blake - Wilson, et al, April 2006.

[23] https://www.boe.es/diario_boe/txt.php?id=BOE-A-1992-26093

[24] https://www.boe.es/buscar/doc.php?id=BOE-A-2014-13359

- RFC5019, Request for Comments: 5019, The Lightweight Online Certificate Status Protocol (OCSP) Profile for High - Volume Environments, A. Deacon, et al, September 2007
- RFC5280, Request for Comments: 5280, Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile, Cooper et al, May 2008.
- RFC6960, Request for Comments: 6960, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. Santesson, Myers, Ankney, Malpani, Galperin, Adams, June 2013.
- WebTrust for Certification Authorities, SSL Baseline with Network Security, Version 2.1[25].
- CAB Forum - Baseline Requirements[26]. Última version consultada: BR2.0.8.
- CAB Forum - Guidelines for The Issuance and Management of Extended Validation Certificates[28]. Última version consultada EV2.0.1.
- X.509, Recommendation ITU - T X.509 (10/2012) | ISO/IEC 9594 - 8:2014 (E), Information technology - Open Systems Interconnection - The Directory: Public - key and attribute certificate frameworks.
- X.520, Recommendation ITU-T X.520 (10/2016) | ISO/IEC 9594-6:2017, Information technology - Open Systems Interconnection - The Directory: Selected attribute types
- *"Article 19 Incident reporting (Incident reporting framework for eIDAS Article 19",* ENISA, December 2016.[29]
- "Guidelines on termination of qualified trust services", ENISA, December 2017. [30]
- Perfil de certificados 2.0 en el marco de la Leyes españolas 39/2015 y 40/2015. [31]
- Perfil de certificados del ámbito judicial aprobado por el CTEAJE en el marco de la Ley 18/2011 española.[32]
- Remote Identity Proofing - Attacks & Countermeasures[33]
- CEN EN 419 221-5 CEN EN 419 241-2, CEN TS 419 221-6, ETSI TS 119 431-1, ETSI TS 119 431-2.
- Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market
- CEN EN 419 241-2: Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing,
- CEN EN 419 221-5:2018 – Protection Profiles for TSP Cryptographic Modules - Part 5 - Cryptographic Module for Trust Services
- CEN EN 419 241-1: Trustworthy Systems Supporting Server Signing Part 1: General System Security Requirements,

3.3 Referencias informativas

En el contexto de España se han publicado diferentes normas legales conectadas con el uso de los servicios de confianza digital. Entre ellas, cabe destacar las siguientes:

[25] http://www.webtrust.org/principles-and-criteria/item83172.aspx

[26] https://cabforum.org/baseline-requirements/

[28] https://cabforum.org/extended-validation/

[29] https://www.enisa.europa.eu/publications/article19-incident-reporting-framework

[30] https://www.enisa.europa.eu/publications/tsp-termination

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

[32] https://www.cteaje.gob.es/documents/185545/299892/CTEAJE-Perfil+Certificado+Seudonimo+Justicia_v1.0.pdf

[33] https://www.enisa.europa.eu/publications/remote-identity-proofing-attacks-countermeasures

- Real Decreto-ley 6/2023, de 19 de diciembre, por el que se aprueban medidas urgentes para la ejecución del Plan de Recuperación, Transformación y Resiliencia en materia de servicio público de justicia, función pública, régimen local y mecenazgo.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.
- Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (entrada en vigor: 2 de octubre de 2016).
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (entrada en vigor: 2 de octubre de 2016).
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de Derechos Digitales.
- Real Decreto-Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
-

4 Definición de términos y abreviaturas

4.1 Términos

Infraestructura de Clave Pública: Conjunto de hardware, software, personas, procedimientos, reglas, políticas y obligaciones utilizados para facilitar la creación, emisión, administración y uso confiables de Certificados y claves basados en Criptografía de Clave Pública.

Certificado de confianza pública: Certificado que es de confianza en virtud del hecho de que su Certificado Raíz correspondiente se distribuye como un ancla de confianza en el software de aplicación ampliamente disponible.

Autoridad de Certificación: Organización responsable de la creación, emisión, revocación y gestión de los certificados. El término aplica igualmente tanto a las CAs raíz como a las CAs subordinadas.

Autoridad de Certificación (AC) EADtrust: es un Prestador Cualificado de Servicios de Confianza (Trust Service Provider o TSP por sus siglas en inglés) constituido al amparo de la legislación española, con CIF B-85626240, domicilio social físico en Calle Alba 15, 28043, Madrid, y dirección electrónica a efectos de notificaciones: info@eadtrust.eu, en virtud de escritura de poder otorgada ante el notario Rafael de la Fuente García, el 29 de enero de 2009, con el número 187 de su protocolo. Inscrita debidamente en el Registro Mercantil de Madrid en el Tomo 26.403, Folio 63, Hoja M-475828. En la prestación del servicio solicitado, EADTrust actúa como Autoridad de Certificación (en adelante la "AC") relacionando una determinada clave pública con una persona o entidad concreta a través de la emisión de un Certificado Electrónico.

CA Emisora: En relación con un Certificado particular, la CA que emitió el Certificado. Puede ser tanto una CA Raíz como una CA subordinada.

CA Raíz: Autoridad de Certificación de nivel superior, cuyo Certificado Raíz es distribuido por Proveedores de Software de Aplicación y que emite Certificados de CA Subordinados.

Certificado Raíz: Certificado autofirmado emitido por la CA Raíz para identificarse y facilitar la comprobación de Certificados emitidos a sus CAs Subordinadas.

CA Subordinada: Una CA cuyo Certificado es firmado por la CA Raíz, u otra CA Subordinada.

Certificado de CA Subordinada Técnicamente Restringido: Certificado de CA subordinada que utiliza un conjunto de Valores de Uso de Clave Extendida y de Restricción de Nombre para limitar el ámbito dentro del cual el certificado de entidad emisora subordinada puede emitir certificados de CA de Suscriptor o Subordinados adicionales.

Solicitante: La persona física o jurídica que solicita la emisión o revocación del certificado.

Suscriptor: Persona física o jurídica a la que solicita la emisión/revocación de un Certificado y que está legalmente obligada por un Acuerdo de Suscriptor o Términos de Uso.

En los Certificados de persona física la figura del Solicitante y el Suscriptor recaen en la misma persona física. En los Certificados para personas jurídicas, el solicitante es la persona física que utilizará las claves del certificado y el Suscriptor, es la entidad jurídica que contrata los servicios.

Persona jurídica: Asociación, corporación, sociedad, alianza, propiedad, entidad gubernamental u otra entidad con personalidad jurídica en el sistema legal de un país.

Entidad de Gobierno: Entidad legal, agencia, departamento, ministerio, rama o elemento similar del gobierno de un país o una subdivisión política dentro de ese país (tal como un estado, provincia, ciudad, condado, etc.).

Representante del Solicitante: Persona física que actúa en nombre y en representación de una persona jurídica o de una entidad sin personalidad jurídica. A la fecha de estas prácticas EADTrust no emite certificados de representante de persona física

Autoridad de Registro (RA): Un departamento del prestador de servicios electrónicos de confianza o una persona Jurídica separada que sea responsable de la identificación y autenticación de los sujetos de Certificados. Una RA puede ayudar en el proceso de solicitud de certificado, en el proceso de revocación o en ambos. Cuando "RA" se usa como adjetivo para describir un papel o función, no implica necesariamente un cuerpo separado, sino que puede ser parte de la CA.

RA de Empresa: Empleado o agente de una organización no afiliada a la CA que autoriza la emisión de Certificados a dicha organización.

Rol de confianza: Un rol que califica a una persona para acceder o modificar los sistemas, la infraestructura y la información confidencial de ISRG PKI.

Tercero de Confianza: Cualquier persona física o jurídica que se base en un Certificado Válido. Un Proveedor de Software de Aplicación no se considera una Parte de Confianza cuando el software distribuido por dicho Proveedor simplemente muestra información relacionada con un Certificado.

Declaración de Prácticas de Certificación o DPC (en inglés, Certificate Practice Statement o CPS): conjunto de prácticas adoptadas por una Autoridad de Certificación de EADTrust para la emisión de certificados cualificados y no cualificados donde se encuentra información detallada sobre su sistema de seguridad, soporte, administración y emisión de los certificados, y sobre la relación de confianza entre las Partes.

Política de Certificado: Conjunto de reglas que indican la aplicabilidad de un Certificado designado a una comunidad en particular y/o la implementación de PKI con requisitos de seguridad comunes.

Términos y Condiciones del Servicio: Acuerdo entre la CA y el Solicitante/Suscriptor que especifica los derechos y responsabilidades de las partes.

Términos de Uso del certificado: Disposiciones relativas a la custodia y usos aceptables de un Certificado emitido según estos Requisitos cuando el Solicitante / Suscriptor es Afiliado de la CA o es la CA.

Repositorio: Base de datos en línea que contiene documentos de gobierno de PKI divulgados públicamente (tales como PDS (Plicy Disclosure Statement), Políticas de Certificado y Declaraciones de Prácticas de Certificación) e información de estado de Certificado, ya sea en forma de CRL o de respuesta de OCSP.

Certificado: Documento electrónico que utiliza una firma digital para vincular una clave pública y una identidad.

Certificado cualificado: Certificado expedido por un Prestador Cualificado de Servicios de Confianza de conformidad con los requisitos del Reglamento UE 910/2014 de 23 de julio de 2014 (Reglamento "e IDAS") y emitido con una autoridad de certificación que figura en las Listas de confianza (TSL).

Datos del Certificado: Solicitudes de Certificado y datos relacionados con el mismo (ya sean obtenido del Solicitante o de otro modo) en posesión o control de la CA o al cual la CA tiene acceso.

Proceso de Gestión del Certificado: Procesos, prácticas y procedimientos asociados con el uso de claves, software y hardware, mediante los cuales la CA verifica los Datos de Certificado, emite Certificados, mantiene un Repositorio y revoca Certificados.

Lista de Revocación del Certificado: Lista con sello de fecha y hora actualizada con regularidad de los Certificados revocados que se crea y firma digitalmente por la CA que emitió los Certificados.

Certificado de Prueba: Certificado con un período de validez máximo de 30 días y que: (i) incluye una extensión crítica con el Certificado de Prueba especificado CABF OID, o (ii) se emite bajo una CA donde no hay rutas / cadenas de certificado a un Certificado raíz sujeto a estos Requisitos.

Fecha de vencimiento: La fecha "No después" en un certificado que define el final del período de validez de un certificado.

Certificado Válido: Certificado que ha pasado el procedimiento de validación especificado en RFC5280.

Período de Validez: Periodo de tiempo medido desde la fecha en la que se emite el Certificado hasta la Fecha de Expiración.

Par de Claves: La Clave Privada y su Clave Pública asociada.

Clave Privada: La clave de un Par de Claves que se mantiene en secreto por el titular del par de claves y que se utiliza para crear firmas digitales y / o descifrar registros o archivos electrónicos que se cifraron con la clave pública correspondiente.

Clave pública: La clave de un Par de Claves que puede revelarse públicamente por el titular de la Clave Privada correspondiente y que es utilizada por una Parte de Confianza para comprobar las Firmas Digitales creadas con la clave privada correspondiente del titular y / o cifrar mensajes para que pueda descifrarse sólo con la clave privada correspondiente del titular.

Compromiso de la Clave: Se dice que una Clave Privada está comprometida si su valor ha sido revelado a una persona no autorizada, si una persona no autorizada ha tenido acceso a ella o si existe una técnica práctica por la cual una persona no autorizada puede descubrir su valor. Una clave privada también se ve comprometida si se han desarrollado métodos que pueden calcularla fácilmente basándose en la clave pública (como una clave débil de Debian, consulte http://wiki.debian.org/SSLkeys) o si hay evidencia clara de que el método específico utilizado para generar la clave privada era defectuoso.

OCSP Responder: Servidor en línea operado bajo la autoridad de la CA y conectado a su repositorio para procesar solicitudes de estado de Certificado. Se basa en el Protocolo de Estado de Certificados en línea (en inglés Online Certificate Status Protocol).

OCSP: Protocolo de Estado de Certificados en línea: Protocolo de comprobación que permite comprobar al software de aplicación de la parte que confía si el estado de un Certificado identificado es válido. Se implementa mediante OCSP Responder.

4.2 Abreviaturas

AICPA American Institute of Certified Public Accountants
CA Certification Authority
CAA Certification Authority Authorization
ccTLD Country Code Top-Level Domain
CICA Canadian Institute of Chartered Accountants
Common Criteria The Common Criteria for Information Technology Security Evaluation (abreviadamente Common Criteria o CC) es un estándard internacional para la certificación de seguridad de sistemas informáticos (ISO/IEC 15408)
CP Certificate Policy
CPS Certification Practice Statement
CRL Certificate Revocation List
DBA Doing Business As
DNS Domain Name System
ENISA European Union Agency for Network and Information Security
ETSI European Telecommunications Standards Institute
FIPS (US Government) Federal Information Processing Standard
FQDN Fully Qualified Domain Name
IM Instant Messaging
IANA Internet Assigned Numbers Authority
ICANN Internet Corporation for Assigned Names and Numbers
ISO International Organization for Standardization
NIST (US Government) National Institute of Standards and Technology
OCSP Online Certificate Status Protocol
OID Object Identifier
PKI Public Key Infrastructure
RA Registration Authority
S/MIME Secure MIME (Multipurpose Internet Mail Extensions)
SSL Secure Sockets Layer
TLD Top-Level Domain
TLS Transport Layer Security
TSL Trusted-Service Status List. Se define en la Decisión de Ejecución (UE) 2015/1505 de la Comisión.

5 Análisis de riesgos

EADTrust lleva a cabo un análisis de riesgos siempre que se ponen en marcha nuevos servicios, se produce un cambio en sus sistemas o en los procedimientos organizativos, en el estado de la tecnología, o en cualquier otro aspecto que pudiera influir en el perfil de riesgo de la organización. Las medidas de seguridad desplegadas se enfocan en garantizar la seguridad de las operaciones y el respeto a la privacidad de los datos personales tratados conforme al artículo 32 del Reglamento de Protección de Datos Personales, el Reglamento (UE) 2016/679.

En los casos que resulte pertinente, EADTrust lleva a cabo evaluaciones de impacto conforme establece la legislación de protección de datos personales vigente. El análisis de riesgos se actualiza con periodicidad mínima anual.

El comité de aprobación de políticas aprueba formalmente el nivel de riesgo residual resultante del análisis de riesgos.

El procedimiento de identificación por videoconferencia conlleva la realización de análisis de riesgos específicos.

6 Políticas y prácticas de la CA: Aprobación y gestión

6.1 Administración de políticas

En relación con esta Declaración de Prácticas de Certificación y las Políticas a las que se hace mención en este documento, los datos de contacto son:

Organismo Supervisor	Ministerio para la Transformación Digital y de la Función Pública (Secretaría de Estado de Digitalización e Inteligencia Artificial)[34].
Nombre del PSC	EAD TRUST European Agency of digital Trust, S. L.
Dirección	C/ Mentrida, 6, 28043 Madrid - Spain
Dirección de email (en relación con las políticas de la CA)	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
EUID (BRIS)[35]	ES28065.080862918
VIES	ES-B85626240
Inscripción registral	Inscrita en el Registro Mercantil de Madrid, Tomo 26403. Folio 63. Sección 8. Hoja M-475828.

[34] La denominación del organismo supervisor puede cambiar por criterios políticos e incluso adscribirse a diferente Ministerio.

[35] https://e-justice.europa.eu/489/EN/business_registers__search_for_a_company_in_the_eu?clang=en

6.1.1 Procedimiento de aprobación de las políticas de certificados

EADTrust ha definido un Órgano de Aprobación y Gestión de Políticas de Certificación que aprueba los cambios finales realizados a las políticas, prácticas y procedimientos de la CA, una vez que determine que cumplen con los requisitos establecidos. También toma decisiones sobre la gestión y operativa de estos servicios.

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

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

6.2 Políticas de emisión de certificados y servicios relacionados

EADTrust ha unificado su documentación de políticas y prácticas de certificación y servicios relacionados a los certificados de persona física y de persona jurídica, incluidos los certificados de sello de órgano y de entidad PSD2 en este documento. Las políticas desplegadas comprenden los servicios siguientes:

1. **Servicio de emisión de certificados** de:

   - Personas físicas, actuando en su propio nombre o en representación de entidades legales (personas jurídicas o entidades sin personalidad jurídica), personas físicas empleados públicos con o sin representación, trabajadores de una empresa sin representación: QCP-N y QCP-N-QSCD;
   - Personas jurídicas, incluido el sello de órgano de la administración pública y el sello de tiempo: QCP-L y QCP-L-QSCD;
   - Entidades financieras actuando en el marco de la normativa PSD2: QCP-L y QCP-L-QSCD;
   - Certificados no cualificados (NCP), incluido el certificado no cualificado de persona jurídica para TSA cualificada.
   - Certificados cualificados de sitio web QEVCP-w y QNCP-w

2. **Servicio de gestión de identidades para la emisión/revocación de certificados electrónicos.**
   Contempla la política de verificación ya tratada.

3. **Servicio de Sellado de tiempo.**
   Sellos de tiempo cualificados firmados con certificados cualificados o no cualificados.

4. **Certificados de autenticación sitios web.**

Las políticas para la emisión de certificados de autenticación sitios web QEVCP-w QNCP-w, QCP-w y QCP-w-QSCD se incuyen en la CPS en idioma inglés y comprenden los certificados siguientes:

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

- (QWAC) PSD2.
- Variantes cualificadas QEVCP-w o QNCP-w de los certificados mencionados

Se recomienda la lectura del documento de referencia, disponible en:

- https://eadtrust.eu/download/6993/

6.3 OIDs de políticas, tipo de soporte y niveles de seguridad de los certificados

Los OIDs utilizados en los certificados de EADTust corresponden a diferentes arcos:

- Definido por EADTrust: **1.3.6.1.4.1.501**
- Definido por la Administración Pública: **2.16.724.1.3**
- Definido por la Administración de Justicia: **2.16.724.6**
- Definido por ETSI (organismo de normalización): **0.4.0**
- Referencia a OID de EADTrust con servicios a extinguir: 1.3.6.1.4.1.19126

Según el Reglamento eIDAS, y dentro del alcance de esta Declaración de Prácticas de Servicios de Confianza, las políticas de certificados y servicios relacionados descritos en este documento, los diferentes certificados que expide EADTrust se caracterizan en las siguientes tablas:

6.3.1 Tipo de Certificado: Persona Física / Persona Natural

Certificado	Standard Policy Identifier	EAD Trust Policy OID	Formato	Nivel de seguridad
Individuo	0.4.0.194112.1.0 (ETSI QCP-n) 1.3.6.1.4.1.501.2.1.0.3 (firma remota)****	1.3.6.1.4.1.501.2.1.1.**0**.41221	Software	Sustancial Presencial**
	0.4.0.194112.1.2 (ETSI QCP-n-QSCD) 1.3.6.1.4.1.501.2.1.0.3 (firma remota)****	1.3.6.1.4.1.501.2.1.1.**1**.41221	Dispositivo*	Alto Presencial**
Identidad obtenida con EUDI Wallet	0.4.0.194112.1.0 (ETSI QCP-n) 1.3.6.1.4.1.501.2.1.0.3 (firma remota)****	1.3.6.1.4.1.501.2.1.1.**3**.41221	Software	Sustancial Distancia***
	0.4.0.194112.1.2 (ETSI QCP-n-QSCD) 1.3.6.1.4.1.501.2.1.0.3 (firma remota)****	1.3.6.1.4.1.501.2.1.1.**4**.41221	Dispositivo*	Alto Distancia***
	0.4.0.194112.1.2 (ETSI QCP-n-QSCD)	1.3.6.1.4.1.501.2.1.1.**6**.41221	Dispositivo*	Alto Distancia***
Representante	0.4.0.194112.1.0 (ETSI QCP-n) 2.16.724.1.3.5.8 (OID MPR)	1.3.6.1.4.1.501.2.1.1.**0**.41222	Software	Sustancial Presencial**

Certificado	Standard Policy Identifier	EAD Trust Policy OID	Formato	Nivel de seguridad
	1.3.6.1.4.1.501.2.1.0.3 (firma remota)****0.4.0.194112.1.2 (ETSI QCP-n-QSCD) 2.16.724.1.3.5.8 (OID MPR)	1.3.6.1.4.1.501.2.1.1.**1**.41222	Dispositivo*	Alto Presencial**
	1.3.6.1.4.1.501.2.1.0.3 (firma remota)**** 0.4.0.194112.1.0 (ETSI QCP-n) 2.16.724.1.3.5.8 (OID MPR)	1.3.6.1.4.1.501.2.1.1.**3**.41222	Software	Sustancial Distancia***
	1.3.6.1.4.1.501.2.1.0.3 (firma remota)**** 0.4.0.194112.1.2 (ETSI QCP-n-QSCD) 2.16.724.1.3.5.8 (OID MPR)) 1.3.6.1.4.1.501.2.1.0.3 (firma remota)****	1.3.6.1.4.1.501.2.1.1.**4**.41222	Dispositivo*	Alto Distancia***
Empleado Público[36]	0.4.0.194112.1.0 (ETSI QCP-n) 2.16.724.1.3.5.7.2 (OID MPR) 1.3.6.1.4.1.501.2.1.0.3 (firma remota)****	1.3.6.1.4.1.501.2.1.1.**0**.41223	Software	Sustancial Presencial**
	0.4.0.194112.1.2 (ETSI QCP-n-QSCD) 2.16.724.1.3.5.7.2 (OID MPR) 1.3.6.1.4.1.501.2.1.0.3 (firma remota)****	1.3.6.1.4.1.501.2.1.1.**1**.41223	Dispositivo*	Alto Presencial**
	0.4.0.194112.1.0 (ETSI QCP-n) 2.16.724.1.3.5.7.2 (OID MPR) 1.3.6.1.4.1.501.2.1.0.3 (firma remota)****	1.3.6.1.4.1.501.2.1.1.**3**.41223	Software	Sustancial Distancia***
	0.4.0.194112.1.2 (ETSI QCP-n-QSCD) 2.16.724.1.3.5.7.2 (OID MPR) 1.3.6.1.4.1.501.2.1.0.3 (firma remota)****	1.3.6.1.4.1.501.2.1.1.**4**.41223	Dispositivo*	Alto Distancia***
Empleado público (Seudónimo/ Firma)	0.4.0.194112.1.2 (ETSI QCP-n-qscd) 2.16.724.1.3.5.4.1 (OID MPR) 1.3.6.1.4.1.501.2.1.0.3 (firma remota)****	1.3.6.1.4.1.501.2.1.1.**1**.41224	Dispositivo*	Alto Presencial**

[36] Se podrán emitir certificados con otros niveles de aseguramiento para empleado público en el futuro, siguiendo las directrices definidas en el documento "Perfiles de Certificados Electrónicos de la administración pública" que define los perfiles de certificados derivados de la aplicación del Real Decreto 203/2021, de 30 de marzo y está adaptado a las disposiciones de la Ley 39/2015 de 1 de Octubre, de Procedimiento Administrativo Común de las Administraciones Públicas, la Ley 40/2015 de 1 de Octubre, de Régimen Jurídico del Sector Publico (LRJ) y al Reglamento (UE) 910/2014.

Certificado	Standard Policy Identifier	EAD Trust Policy OID	Formato	Nivel de seguridad
	0.4.0.194112.1.2 (ETSI QCP-n-qscd) 2.16.724.1.3.5.4.1 (OID MPR) 1.3.6.1.4.1.501.2.1.0.3 (firma remota)****	1.3.6.1.4.1.501.2.1.1.**4**.41224	Dispositivo*	Alto Distancia***
Empleado público (Seudónimo/ Autenticación)[3]	0.4.0.194112.1.2 (ETSI QCP-n-qscd) 2.16.724.1.3.5.4.1 (OID MPR) 1.3.6.1.4.1.501.2.1.0.3 (firma remota)****	1.3.6.1.4.1.501.2.1.1.1.41225	Dispositivo*	Alto Presencial**
	0.4.0.194112.1.2 (ETSI QCP-n-qscd) 2.16.724.1.3.5.4.1 (OID MPR) 1.3.6.1.4.1.501.2.1.0.3 (firma remota)****	1.3.6.1.4.1.501.2.1.1.4.41225	Dispositivo*	Alto Distancia***

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

(**) Presencial: Identifica los OID de Políticas de certificados en los que la validación y autenticación de la identidad del Solicitante se realiza de manera presencial en las instalaciones de la RA.

(***) Distancia: Identifica los OID de Políticas de certificados en los que la validación y autenticación de la identidad del Solicitante se realiza por la RA, de manera remota (on line, también denominada telepresencia, o videoidentificación). Para ello pueden desplegarse medios de videoidentificación o videoconferencia. Su uso está sujeto a la aprobación por el Organismo Supervisor.

(****) Éste OID se añadirá a los certificados que vayan a usarse para firma remota (firma "on-behalf") gestionada por EADTrust.

6.3.2 Tipo de Certificado: Entidad legal / Persona Jurídica / Entidad sin personalidad Jurídica / Sello de Órgano

Certificado	Standard Policy Identifier	EAD Trust Policy OID	Formato	Nivel de seguridad
Sello corporativo (Timestamp)	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**.421 1.3.6.1.4.1.501.2.1.1.**1**.421	Software Dispositivo*	Sustancial Alto
Sello corporativo (Timestamp)	No se indica Política asociada a RFC3161	1.3.6.1.4.1.501.2.1.1.**0**.3161	Software Dispositivo*	No cualificado Distancia***
Sello Corporativo	0.4.0.194112.1.1 (ETSI QCP-l) 1.3.6.1.4.1.501.2.1.0.3 (firma remota)****	1.3.6.1.4.1.501.2.1.1.**0**.41231	Software	Sustancial Presencial**
	0.4.0.194112.1.3 (ETSI QCP-l-QSCD) 1.3.6.1.4.1.501.2.1.0.3 (firma remota)****	1.3.6.1.4.1.501.2.1.1.**1**.41231	Dispositivo*	Alto Presencial**
	0.4.0.194112.1.1 (ETSI QCP-l) 1.3.6.1.4.1.501.2.1.0.3 (firma remota)****	1.3.6.1.4.1.501.2.1.1.**3**.41231	Software	Sustancial Distancia***
	0.4.0.194112.1.3 (ETSI QCP-l-QSCD)	1.3.6.1.4.1.501.2.1.1.**4**.41231	Dispositivo*	Alto Distancia***

Certificado	Standard Policy Identifier	EAD Trust Policy OID	Formato	Nivel de seguridad
Sello Corporativo PSD2 (QSeal)	0.4.0.194112.1.1 (ETSI QCP-l) 1.3.6.1.4.1.501.2.1.0.3 (firma remota)**** 0.4.0.194112.1.3 (ETSI QCP-l-QSCD 1.3.6.1.4.1.501.2.1.0.3 (firma remota)****	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 Dispositivo*	Sustancial Distancia*** Alto Distancia***
Sello de órgano	0.4.0.194112.1.1 (ETSI QCP-l) 0.4.0.194112.1.3 (ETSI QCP-l-QSCD)	1.3.6.1.4.1.501.2.1.1.**0**.41233 1.3.6.1.4.1.501.2.1.1.**1**.41233	Software Dispositivo*	Sustancial Presencial** Alto Presencial**

(*) 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.

(**) Presencial: Identifica los OID de Políticas de certificados en los que la validación y autenticación de la identidad del Solicitante se realiza de manera presencial en las instalaciones de la RA.

(***) Distancia: Identifica los OID de Políticas de certificados en los que la validación y autenticación de la identidad del Solicitante se realiza por la RA, de manera remota (on line, también denominada telepresencia, o videoidentificación). Para ello pueden desplegarse medios de videoidentificación o videoconferencia. Su uso está sujeto a la aprobación por el Organismo Supervisor.

(****) El OID 1.3.6.1.4.1.501.2.1.0.3 (sello remoto) se añadirá a los certificados que vayan a gestionarse por EADTrust para sello remoto (sello "on-behalf").

6.3.3 Tipo de Certificado: Certificados PSD2

Certificado	Standard Policy Identifier	EAD Trust Policy OID	Formato	Nivel de seguridad
Sello Corporativo PSD2 (QSeal)	0.4.0.194112.1.1 (ETSI QCP-l) 0.4.0.194112.1.3 (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 Dispositivo*	Sustancial Distancia*** Alto Distancia***

(*) Los dispositivos habituales son HSM (Hardware Security Module), token seguro y tarjeta chip. Los tokens USB se consideran equivalentes al uso de tarjetas inteligentes considerando que incorporan la tarjeta y la chaqueta lectora en el mismo dispositivo
.
(**) Presencial: Identifica los OID de Políticas de certificados en los que la validación y autenticación de la identidad del Solicitante se realiza de manera presencial en las instalaciones de la RA.

(***) Distancia: Identifica los OID de Políticas de certificados en los que la validación y autenticación de la identidad del Solicitante se realiza por la RA, de manera remota (on line, también denominada telepresencia, o videoidentificación). Para ello pueden desplegarse medios de videoidentificación o videoconferencia. La denominación PSD2 hace referencia a a la Segunda Directiva de Pagos "Payment Services Directive (EU) 2015/2366"

Consulte los OIDs de políticas, tipo de soporte y niveles de seguridad de los certificados de autenticación de sitios web en la CPS en idioma inglés disponible en: https://eadtrust.eu/download/6993/

6.5 Términos y Condiciones del servicio

Los términos y condiciones, generales y particulares de los servicios de emisión de certificados se encuentran disponibles en la web de EADTrust. Estos términos se revisan con con periodicidad mínima anual. Se recomienda su consulta previa a la contratación de los servicios de EADTrust. En caso de incompatibilidad en lo definido en este documento de prácticas y lo estipulado en los contratos de términos y condiciones del servicio, prevalece lo establecido en esta Declaración de Prácticas.

Consultar el documento vigente en:

- https://eadtrust.eu/documentos-vigentes/

7 Responsabilidades de publicación y repositorios

Repositorios

El Repositorio de documentos legales de la Autoridad de Certificación de EADTrust está disponible públicamente, 24 horas al día, 7 días a la semana y comprende los documentos e informaciones siguientes: Políticas; prácticas; contratos de términos y condiciones de los servicios. Más detalles en:

- eadtrust.eu/documentos-vigentes/

La Política de Privacidad para los servicios de emisión de certificados esta disponible en:

- eadtrust.rgpd.de/informacion-de-proteccion-de-datos-para-solicitantes-de-certificados/

EADTrust mantiene publicadas aquellas versiones anteriores de los documentos mientras existan certificados vigentes que se hayan emitido de acuerdo con dichos documentos o sea interés del usuario para consulas históricas.

- Más detalles en: https://eadtrust.eu/historico-de-documentacion/

Los registros de todos los certificados de la CA raíz y subordinada de EADTrust, incluidos los que han sido revocados, están disponibles en el repositorio de certificados:

- eadtrust.eu/documentos-vigentes/

EADTrust también 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 responden a esta estructura:

- https://ecc-256-dv-tst.eadtrust.eu/
- https://ecc-256-dv-q-tst.eadtrust.eu/
- https://ecc-256-ev-tst.eadtrust.eu/

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

En el puerto 443, se encuentran los certificados **en vigor**. En el puerto 8443 se ubican los certificados **revocados no caducados**. Y en el puerto 9443, los certificados **caducados**.

Dada su condición de sitios web de pruebas, pudiera darse la circunstancia transitoria de certificados supuestamente “en vigor” que estén caducados mientras se expide una nueva colección de certificados de sitio web de pruebas.

P.Ej.: para los certificados RSA-2048 de Domain Validated, tendríamos:

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

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

7.1 Tiempo o frecuencia de publicación

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

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

Los documentos nuevos o actualizados de EADTrust, se ponen a disposición del público tan pronto como sea posible. Esto significa normalmente dentro de los siete días siguientes a su recepción o aprobación por el órgano de aprobación y gestión de políticas de la CA.

Los certificados nuevos o actualizados de la CA raíz y subordinada de EADTrust se ponen a disposición del público lo antes posible. Esto significa, normalmente, dentro de los siete días siguientes a su creación.

7.2 Controles de acceso a los repositorios

El acceso de sólo lectura al Repositorio Legal y de Políticas y a la información de los certificados no está restringido. El acceso de escritura está protegido por controles lógicos y físicos.

8 Identificación y autenticación

8.1 Nombres

8.1.1 Tipos de Nombres

Todos los certificados de usuario de entidad final emitidos por la Autoridad de Certificación de EADTrust, contienen un nombre dado en el campo **Subject Name**. Los atributos especificados en el nombre diferenciado en el campo de **Sujeto** están contenidos en la sección correspondiente al perfil de certificado.

El valor autenticado en el campo **Common Name** es el nombre de la persona física Solicitante. El campo **subjectAltName** también se utiliza ocasionalmente para situar un nombre que se puede utilizar para identificar al sujeto, pero que es diferente del nombre que aparece en el campo **Subject Name**.

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

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

El perfil de los certificados se incluye en esta DPC, pero además se puede solicitar a través del servicio de soporte al cliente de EADTrust:

- info@eadtrust.eu

Tambien están disponibles públicamente en la sección de políticas vigentes de la CA:

- www. eadtrust.eu/documentos-vigentes/

La estructura sintáctica y el contenido de los campos de cada certificado emitido por EADTrust, así como su significado semántico, se encuentran descritos en los perfiles de certificados

- **Persona física:** En certificados correspondientes a personas físicas la identificación del signatario estará formada por su nombre y apellidos, más su número de identificación personal (DNI, NIE, PASAPORTE u otros documentos admitidos en la norma EN 319 412-1).

- **Persona física - representante persona juridica:** Determina la relación de representación legal o de apoderado general entre la persona física (titular del certificado/Sujeto/Firmante) y una persona jurídica o entidad sin personalidad jurídica.
- **Persona física - empleado público**: Es una persona física representante de un organismo público o un empleado público adscrito a un organismo público. Existe un perfil específico para la Administración de Justicia.
- **Persona Jurídica:** En certificados correspondientes a personas jurídicas, esta identificación se realizará por medio de su denominación o razón social, y su identificación fiscal u otro número de identificación de los admitidos en la norma EN 319 412-1. En los certificados orientados a PSD2 se considerarán los contenidos exigidos por su normativa. Los certificados de sello de órgano son un caso particular de este tipo de certificados y tienen un perfil propio. En los certificados orientados a PSD2 se considerarán los contenidos exigidos por su normativa. Los certificados de sede electrónica son un caso particular de certificados "organization validated" (nivel de aeguramiento sustancia/medio) y "extended validation" (nivel de aeguramiento alto) y tienen un perfil propio.

8.1.2 Necesidad de que los nombres sean significativos

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

Cada certificado electrónico contiene un conjunto único de atributos de nombre. Estos atributos incluyen una recopilación del nombre de la persona física Solicitante, nombre de la persona jurídica Suscriptora, unidad organizacional e identificador único.

8.1.3 Anonimidad o pseudonimidad de los titulares de certificados

Se podrán emitir certificados de seudónimo en los casos previstos en la normativa. Por ejemplo, en relación con el perfil de "certificado electrónico de empleado público con seudónimo".
En este caso el certificado se identificará como de seudónimo de manera inequívoca.

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

EADTrust se compromete a no revelar la citada identidad asociada a los certificados de seudónimo, salvo cuando lo soliciten los órganos judiciales y otras autoridades públicas para el ejercicio de las funciones que tienen atribuidas.

8.1.4 Tratamientos de datos excluidos en los certificados

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

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

8.1.5 Normas para interpretar diferentes formas de nombres

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

- X.509 - ISO/IEC 9594-813[37]
- X.520 -ISO/IEC 9594-614[38]

8.1.6 Singularidad de los nombres

Los nombres de los titulares de los certificados (considerando los diferentes atributos) son únicos para cada tipo de certificado dentro de la Declaración de Prácticas de Certificación de EADTrust.

8.2 Validación inicial de la identidad

8.2.1 Método para probar la posesión de la clave privada

Cuando se genera un par de claves por la Autoridad de Certificación a instancias de la Autoridad de Registro:

- Si las claves se almacenan en un token o una tarjeta criptográfica, la prueba de posesión de la clave privada se demuestra en virtud del procedimiento confiable de entrega y aceptación del token o de la tarjeta criptográfica y del correspondiente certificado y el par de claves almacenados de forma segura.

[37] http://www.itu.int/rec/T-REC-X.509-201610-I

[38] http://www.itu.int/rec/T-REC-X.520-201610-I

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

Cuando se genera el par de claves por el solicitante:

- La posesión de la clave privada se demuestra en virtud del procedimiento de generación de claves, a través de funciones del navegador del solicitante, o por la remisión de la solicitud PKCS#10 (CSR, Certificate Request), que presume la existencia de una clave privada bien en HSM (Hardware Security Module), bien en otro entorno de gestión de solicitudes de certificación. Salvo que el solicitante acredite que la solicitud se asocia a la generación de claves en un HSM, no podrán expedirse certificados en los que se incluya la constancia de uso de Dispositivo Cualificado de Creación de Firma.

El solicitante debe aportar un informe de auditor que confirme que realmente se ha generado la clave dentro de un HSM, salvo que el personal de la RA tenga la posibilidad de comprobar por si mismo que la solicitud PKCS#10 se ha generado en un HSM.

8.2.2 Autenticación de la organización

Para los certificados emitidos a una entidad o a una persona física con atributo de representante, empleado público o vinculación a una entidad, se verificarán los datos relativos a la constitución y a la personalidad jurídica de la entidad. Para realizar esta autenticación, la RA requerirá al solicitante la documentación pertinente en función del tipo y país origen de la entidad. La RA podrá consultar esta información de fuentes oficiales que permitan comprobar de forma fehaciente los datos relativos a la constitución y a la personalidad jurídica de la entidad. Cuando las entidades no sean sociedades se utilizarán de referencia los poderes notariales aportados y publicaciones de nombramientos en los boletines oficiales.

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

- 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).

Sólo 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.

En esta Declaración de Prácticas de Certificación se toma en consideración la Lista de direcciones de correo electrónico de las autoridades nacionales competentes que seguirán el proceso de solicitud de revocación de los certificados eIDAS según lo establecido en el Dictamen de la EBA sobre el uso de los certificados eIDAS (EBA-OP-2018-7) (Versión 4, publicada el 1 de enero de 2021).[39] Esta información podrá actualizarse conforme esté disponible por parte de las Autoridades Nacionales Competentes.

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 documento Tipo de números de identificación utilizados en el Registro de la PSD2 de la EBA y en el Registro de Entidades de Crédito de la EBA, versión 2, publicado el 1 de enero de 2021[40]. Esta información podrá actualizarse y EADTrust cumplirá la vigente en el momento de expedir el certificado QSeal o QWac PSD2 solicitado.

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

Una vez que se expida un certificado PSD2, EADTrust notificará a la Autoridad Nacional Competente 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

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

[40] https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2882455/bc08f0a4-3bd6-4e33-a726-eaf73e9e4536/Identification%20numbers%20in%20the%20EBA%20registers.pdf?retry=1

- URL del servicio OCSP.

En el caso de solicitar un nuevo certificado antes del vencimiento del anterior, se vuelve a comprobar que la entidad sigue figurando en los registros correspondientes como PSP.

8.2.3 Autenticación de la identidad individual

La identificación de las personas físicas solicitantes de certificados se llevará a cabo a través de RA propias o afiliadas. La documentación a aportar varía según el tipo de certificado de interés. Las solicitudes de certificados relativas a entidades requerirán la verificación de la identidad de la persona física y acreditar su vinculación con la persona jurídica suscriptora. Más detalles sobre la documentación a aportar en la Política de gestión de identidades para la emisión/revocación de certificados de EADTrust.

En la identificación a distancia se podrán utilizar los procedimientos ya indicados (en los apartados "Autoridades de registro" y "Procedimientos de identificación y autenticación de solicitantes/suscriptores de certificados")

8.3 Identificación y autenticación de la solicitud de revocación

El inicio de una solicitud de revocación se produce:

- A solicitud de un representante de la entidad en la que prestaba servicios el titular del certificado, si el certificado es de Representante, de empleado público, de Persona Jurídica o de sitio web.
- Por el titular, por compromiso de sus claves o por cualquier otra razón que lo requiera.
- Por la Autoridad Competente en los casos previstos en la normativa PSD2.

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. 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.

9 Gestión del proceso de emisión/revocación de certificados

9.1 Solicitud del certificado

El interesado en obtener un certificado emitido por la CA de EADTrust podrá ponerse en contacto vía telefónica, por e mail, cumplimentando la solicitud de emisión de certificados disponible en la página web: www.eadtrust.eu , o por cualquier otra vía admisible en Derecho.

Luego del primer contacto, podrá agendar una cita con la RA para su identificación y verificación de la identidad declarada.

9.2 Procedimientos de identificación y autenticación de solicitantes/suscriptores de certificados

Durante el proceso de emisión/revocación de certificados de EADTrust, la Autoridad de Registro actuante podrá llevar a cabo la gestión de identidades de Solicitantes/Suscriptores en las modalidades de servicios siguientes:

- inscripción en persona con personación ante un agente de la RA conforme al Artículo 24.1 a) del Reglamento eIDAS,
- inscripción a distancia, en las variantes siguientes:
  - videoconferencia (también descrita como telepresencia) videograbación verificada (videonboarding) o videoidentificación conforme al Artículo 24.1 d) del Reglamento eIDAS (según la norma ETD/465/2021).

- verificación de identidad a través de la entidad bancaria del Solicitante/Suscriptor conforme al Artículo 24.1 b) del Reglamento eIDAS.[41] Este enfoque utiliza los servicios de un tercero (Zealid).[42]

- firma electrónica cualificada (aseguramiento sustancial o alto). En el caso en el que se utiliza una firma electrónica avanzada basada en un certificado cualificado como parte de una solicitud de certificado conforme al Artículo 24.1 c) del Reglamento eIDAS,

- reconocimiento y legitimación de firma ante un notario público (incluyendo notarios de países de sistema de derecho romano, germano, francés o similares, como los "scrivener notaries" de Londres) conforme al Artículo 7 de la Ley 6/2020, de 11 de noviembre. [43]

El Solicitante/Suscriptor del servicio podrá elegir el procedimiento de identificación que le sea más adecuado, siempre y cuando cumpla los requisitos descritos en la **Política de gestión de identidades para la emisión/revocación de certificados electrónicos** en la que se establecen los requisitos formales para la identificación, los documentos a aportar, períodos de conservación de la información, etc.

- Puede consultarse la política en cuestión en el sitio web: https://eadtrust.eu/documentos-vigentes/

Posteriormente, EADTrust enviará un e mail con la información de la fecha y hora de la cita; así como de la documentación que deberá aportar o enviar a la RA antes de la fecha de la cita agendada.

La documentación a aportar deberá estar actualizada y vigente. Los documentos que se envíen digitalizados deberán ser legibles. De optar por la modalidad presencial de verificación de la identidad, los documentos que deberán aportarse deberán ser originales.

En los casos que proceda, el solicitante del certificado indicará además si desea obtener certificados en soportes QSCD, en un servicio gestionado para firma a distancia (firma remota o firma en la nube) o en otro soporte admitido en esta política. También podrá indicar preferencias respecto a la longitud de las claves de firma que desea sean empleadas.

En la identificación a distancia es posible activar el servicio de firma remota de EADTrust. EL servicio de firma remota solo está disponible para los clientes que se dan de alta por el procedimiento de videoidentificación.

[41] Tomando como referencia las medidas de diligencia debida que las entidades deben desplegar para la identificación de sus clientes (KYC know your costumer) con mecanismos "strong costumer authentication", definidas en la legislación española de prevención de blanqueo de capitales Ley 10/2020 y las Directivas europeas AML4 y la AML5, GAFI, etc.

[42] Este servicio podrá no estar disponible en algunos países.

[43] https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-14046

Cuando el solicitante quiera utilizar una clave generada por el mismo en un QSCD y con un certificado emitido por EADTrust, deberá aportar la clave pública en un fichero de petición de certificado PKCS#10.

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

9.2.1 Aprobación o rechazo de solicitudes de certificado

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

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, la RA solicitará la aprobación de la emisión del certificado.

Una vez verificado por el segundo nivel de aprobación, la CA de EADTrust emitirá el certificado correspondiente.

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.

9.2.2 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. Una vez hechas las comprobaciones de identidad del suscriptor, el tiempo de emisión del certificado es de 24 horas en días laborables.

9.3 Emisión del certificado

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

9.3.1 Acciones de la CA durante la emisión del certificado

Los certificados QSCD se entregan en un token criptográfico, en una tarjeta inteligente o en HSM del solicitante o del Prestador (para firma remota o firma en la nube). Cuando no es un certificado QSCD, EADTrust podrá entregar el certificado en un soporte de software USB, o enviarlo por email, adjuntando el certificado en un archivo .zip/.rar cifrado, para dotar de mas seguridad al proceso.

I. Procedimiento de emisión de certificados expedidos en un token criptográfico o en una tarjeta inteligente:

- La Autoridad de Registro autentica la validez de la documentación presentada por el solicitante.
- Tras la autenticación, la Autoridad de Registro solicita la aprobación y la emisión del certificado a la CA de EADTrust.

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

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

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

EADTrust ofrece un servicio de firma remota que, de ser solicitado, implica que, tras el proceso de validación de la solicitud del certificado, la generación de claves y su gestión se realiza en un HSM gestionado por EADTrust.

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

- Junto con el formulario de solicitud, el solicitante genera un par de claves en su propio ordenador, y hace llegar a EADTrust la solicitud de certificado con formato PKCS#10. No se admitirá ninguna clave pública que haya sido previamente usada para emitir un certificado en EADTrust.
- 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.

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

- El solicitante genera el formulario de solicitud.

- La Autoridad de Registro autentica la validez de la documentación presentada por el solicitante.
- Después de recibir la documentación, EADTrust emite el certificado vinculado con la clave privada, en formato PKCS#12 cifrado, que se puede insertar en cualquier dispositivo, incluso anque 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.

9.3.2 Notificación al suscriptor sobre la emisión del certificado por la CA

Una vez emitido el certificado, el suscriptor recibirá una notificación en el correo electrónico o en teléfono móvil suministrado en la solicitud (a través de un SMS), el PIN de activación de la clave privada. Tambien recibirá las claves de acceso al archivo zip/.rar cifrado que contiene el certificado.

9.4 Aceptación del certificado

El suscriptor/propietario de la clave tiene un plazo determinado de 10 días naturales desde la entrega del certificado para asegurarse de que funciona correctamente. Transcurrido dicho plazo se considera que el suscriptor ha aceptado el certificado emitido.

Si el certificado no se ha emitido correctamente por 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.

9.4.1 Publicación del certificado por la CA

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

9.4.2 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”[44]

9.5 Par de claves y uso del certificado

9.5.1 Clave privada del titular y uso del certificado

El suscriptor de un certificado estará obligado a cumplir con los dispuesto por la normativa, por esta DPC en su condición de firmante y a lo establecido en los términos y condiciones impuestas por la CA, los

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

cuales se habrán aceptado como paso previo a la confirmación de la solicitud del certificado. En todo caso deberá usar su certificado en base a los usos permitidos, de acuerdo con lo indicado en este documento.

El titular que tiene la custodia de la clave privada:

- 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 DPC (CPS) 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 titular piense que pueda confiar en el certificado, sin demora razonable, si se produce alguna de las siguientes situaciones:
  - La clave privada del titular se ha perdido, ha sido robada o se ha visto potencialmente comprometida.
  - El control sobre la clave privada del titular 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 titular, 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 titulares 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 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 y sellado de tiempo solicitados en los términos y condiciones previstos por la CA, cuando el titular coincide 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 las políticas y 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, la política de certificado específica y de la legislación vigente.

9.5.2 Uso de la clave pública por la parte que confía y uso del certificado

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

- Evaluar independientemente la idoneidad del uso de un certificado y determinar que, de hecho, se utilizará para un propósito apropiado.
- Ser consciente de las condiciones para usar los certificados de conformidad con lo establecido en la Declaración de Práctica de Certificación, y especialmente, en la PDS (Policy Disclosure Statement), es decir, la declaración abreviada para terceros que confían.
- Comprobar la validez, o revocación de los certificados emitidos, utilizando la información sobre el estado del certificado, disponible en el servicio OCSP.
- Comprobar todos los certificados en la jerarquía de certificados antes de confiar en una firma digital o en cualquiera de los certificados de la jerarquía. En relación con los certificados cualificados, comprobar que la autoridad de certificación raíz de EADTrust en cuya jerarquía se encuentra el certificado, está inluída en la lista TSL correspondiente.[45]
- 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.

Nota: algunos certificados, por la técnica de gestión, son confiables sin requerir comprobación de su validez por OCSP o CRL. Por ejemplo, los de corta duración o los asociados a servicios conexos a la generación de firma: el certificado del respondedor OCSP o el certificado de la unidad TSU (time stamping unit).

[45]En España, la lista TSL la publica el Ministerio de Asuntos Económicos y Transformación Digital y está disponible en https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/Prestadores.aspx

9.6 Renovación del certificado

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

9.7 Modificación del certificado

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

9.8 Revocación y suspensión del certificado

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

EADTrust no realiza suspensiones de certificados. En caso de que se produzca una circunstancia que pudiera resolverse con la suspensión y posterior reactivación del certificado, se procedera a revocar el certificado anterior y en su lugar se expedirá un nuevo certificado.

9.8.1 Circunstancias para la revocación

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

- La solicitud de revocación ha sido realizada por el firmante, la persona física o jurídica representada por el firmante, un tercero autorizado o una persona física que solicitó un certificado digital para una persona jurídica.
- Los datos de creación de firma del firmante o del prestador de servicios de certificación han sido comprometidos o si el firmante o un tercero han utilizado los datos de forma incorrecta.
- Cuando se haya emitido una orden legal o administrativa a tal efecto.
- Que una Autoridad Competente indique la necesidad de revocar un certificado PSD2.
- La muerte del firmante o la extinción de la persona jurídica titular del certificado de sello, la incapacidad total o parcial imprevisible del firmante o de la persona jurídica representada por el firmante, la terminación de la representación, la disolución de la persona jurídica representada, el cambio en las circunstancias de la custodia o uso de los datos de creación de firma o de sello incluidos en los certificados expedidos a una persona jurídica.
- El caso de que EADTrust termine su actividad, excepto en los casos en que el firmante haya dado su consentimiento para que los servicios de gestión de certificados electrónicos sean transferidos a otro prestador de servicios de certificación.
- Cambio en los datos suministrados para obtener el certificado o modificación de las circunstancias verificadas para la emisión del certificado.

- Que haya perdido la clave privada asociada al certificado, que haya sido robada o no sea útil debido a daños en el soporte del certificado, o cuando se haya cambiado a otro soporte no previsto en la política de certificación.
- Una de las partes incumple sus obligaciones, como, por ejemplo, el pago.
- Se detecta un error en el procedimiento de emisión del certificado, ya sea porque uno de los requisitos previos no se ha cumplido o debido a problemas técnicos durante el proceso de emisión del certificado.
- Existe una amenaza potencial para la seguridad de los sistemas y para la fiabilidad de los certificados emitidos por EADTrust por razones distintas del compromiso de los datos de creación de firmas.
- Fallo técnico en la emisión o distribución de certificados o de la documentación asociada.
- 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.

9.8.2 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.
- En el caso de los certificados para PSD2, los organimos supervisores (Autoridades Competentes).

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

En caso de licitaciones, la solicitud de revocación la podrán realizar las personas designadas en cumplimiento de los pliegos por el poder adjudicador.

9.8.3 Procedimiento para la solicitud de revocación

El interesado en la revocación de un certificado puede solicitarla a través de:

- La página web de EADTrust: En línea, en la dirección https://eadtrust.eu/solicitud-de-revocacion/
- Por correo electrónico dirigido a autoridadregistro@eadtrust.eu, con la solicitud firmada electrónicamente utilizando un certificado cualificado. También será válida la solicitud de revocación que referencie un código designado para ese uso.
- Por correo postal, enviando la solicitud de revocación de certificado firmada y validada ante notario.
- Por un sistema de entrega certificada cualificada que acredite la identidad del remitente, que debe coincidir con uno de los sujetos legitimados para solicitar la revocación.

En el caso de los certificados para PSD2, los organimos 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. La demora máxima entre la recepción de una solicitud de revocación de certificado y la decisión de cambiar su información de estado para que esté disponible para todas las partes que confían es siempre menor de 24 horas, y usualmente menor de 10 minutos.

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

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.

9.8.4 Período 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 período 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.Tres de las posibles políticas a aplicar, en España, son la de factura electrónica[46], la de la Administración General del Estado[47] y la de la Administración de Justicia[48].

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

[46] https://www.facturae.gob.es/formato/Paginas/politicas-firma-electronica.aspx

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

[48] 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

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.

Se accede al repositorio de CRLs a través de esta URL: https://crl.eadtrust.eu/

Se accede al repositorio histórico a través de esta URL: https://crlhistory.eadtrust.eu/

9.8.5 Tiempo en el que una CA debe procesar la solicitud de revocación

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

9.8.6 Requisitos de comprobación de revocación para las partes que confían

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

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

9.8.7 Frecuencia de emisión de la CRL

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

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

La CRL para los certificados de entidad final se emite cada 24 horas o 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.

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 CRL's". 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.

9.8.8 Actualización de las 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.

9.8.9 Servicios de estado de certificado

EADTrust proporciona a las Entidades Usuarias un servicio de comprobación de validez de certificados en tiempo real basado en OCSP (Online CertificateStatusProtocol)[49].

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.

9.9 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.

[49] IETF RFC 6960 Online Certificate Status Protocol – OCSP.

10 Servicio de firma remota, firma en servidor o firma en la nube

El servicio se identifica formalmente con la siguiente política:

itu-t(0) identified-organization(4) etsi(0) SIGNATURE CREATION SERVICE-policies(19431) ops (1) policy-identifiers(1) eu-remote-qscd (3)

El servicio de firma remota se ofrece a clientes que se identifican ante EADTrust para obtener certificados, de modo que es EADTrust quien genera la pareja de claves en un HSM (DCCF) y pone a disposición del cliente las credenciales de identificación para acceder al servicio de firma remota mediante una App accionable desde un teléfono móvil. El tipo de criptografía adoptado lo selecciona el usuario. Por defecto será de RSA 4096.

Aunque la verificación de identidad se orienta a personas físicas, la aportación en el proceso de solicitud de documentos de "mandato" u "otorgamiento de poderes" permitirá la emisión de certificados a personas físicas, a personas jurídicas y a personas físicas representantes de personas jurídicas y, por tanto, la firma remota hará uso del certificado que corresponda.

Cuando expire el certificado o se revoque, se eliminará el material criptográfico del HSM.

El sistema genera una información en un log por cada intento de firma, tanto si tiene éxito como si no. Ocasionalmente generará una alerta interna si se requiere mayor investigación por el equipo de seguridad del Prestador. El registro de la información relativa a las firmas remotas en la base de datos se mantendrá al menos por 7 años tras la finalización de la vigencia del certificado.

En caso de que así se solicite, se emitirán certificados de corta duración para el servicio de firma remota.

Aunque se usa una App en el móvil para que el firmante controle la realización de firma y la prestación del consentimiento, técnicamente la generación de la firma se realiza en el servidor, según el formato que se determine.

Solo se usarán equipos HSM que estén incluidos en la lista "Compiled list of notified SSCDs/QSCDs"[50] recogida en el "Cuadro de Mandos EIDAS" de la Unión Europea. Los equipos se configuran tal como se define en la documentación para lograr el nivel de seguridad **Common Criteria EAL4+** o superior. El Prestador dispone de medios para realizar backups (copias de seguridad) seguros de material criptográfico del HSM que solo se puede restaurar en otro HSM igual.

La provisión del servicio de firma remota por EADTrust se informará en los "Términos y Condiciones" asociados al proceso de identificación a distancia con estas frases:

> Si lo desea, puede seleccionar en el proceso de solicitud de certificado la opción de disponer del servicio de firma remota prestado por EADTrust, para lo cual EADTrust generará la pareja de

[50] https://eidas.ec.europa.eu/efda/browse/notification/qscd-sscd

claves (pública y privada) en un HSM (DCCF) y pondrá a su disposición las credenciales de identificación y autenticación que necesitará para acceder al servicio usando en su teléfono móvil la App destinada a la funcionalidad de firma remota. El certificado emitido se vinculará a este DCCF. La prestación del consentimiento para que se realice la firma se llevará a cabo a través de la comprobación biométrica del teléfono móvil (algo que ***tienes***-móvil- algo que ***sabes*** -clave- algo que ***eres*** -biometría-). El usuario no debe ceder el teléfono móvil ni las credenciales a terceros.

El servicio se orienta a la firma de documentos en formato PDF (PADES-LT) de forma que se generan firmas longevas que incluyen información de sello de tiempo cualificado (timestamp) y de validez del certificado en el momento de la firma (respuesta OCSP). En el futuro podrán incorporarse al sistema otras modalidades de firma electrónica. El sello de tiempo lo genera EADTRUST.

Podrá ver en la App la lista de documentos que puede firmar y podrá revisar cada documento en la App para comprobar si es el que desea firmar.

Por requisito de la norma ETSI TS 119 431-2 se hace constar que el servicio de firma remota de EADTRUST responde al OID de política complementario: **`itu-t(0) identified-organization(4) etsi(0) CREATION SERVICE-policies(19431) ades (2) policy-identifiers(1) eu-advancedx509 (2)`**

En el contexto de la firma remota se cumplen los apartados 3 y 4 del Anexo II del Reglamento UE 910/2014.

Se le avisará con al menos 30 días de antelación si fuera preciso discontinuar el servicio, salvo que se den circunstancias de fuerza mayor, ajenas a las posibilidades de gestión del Prestador.

11 Servicio de sello de tiempo

EADTrust ofrece servicios de sello de tiempo (timestamping) cualificado y no cualificado desplegados en entornos de Cloud Computing flexible para garantizar la provisión de sello de tiempo en contexto de alta demanda.

- La Política de Sellado de Tiempo (best practices policy for time-stamp) se identifica y referencia en ETSI OID **0.4.0.2023.1.1 es decir,** {itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) baseline-ts-policy(1)}

El proveedor de servicios de confianza ha establecido diferentes OIDs para los diferentes tipos de sellos de tiempo emitidos (cualificados y no cualificados). Asimismo, ha establecido tres entornos (Preproducción, producción y test) con sus correspondientes OIDs para facilitar la puesta en marcha del servicio.

Igualmente, las peticiones de los sellos de tiempo se realizarán a su correspondiente *endpoint*, que varía en función del certificado utilizado para firmar el hash (no cualificado, cualificado sin HSM y cualificado con HSM).

A continuación, se presentan los OIDs y los *endpoints*:

1. Los OIDs y endpoints del Sello de Tiempo cualificado son:

Entorno	URL	Certificado usado	OID
TSU Test	https://tempus-tsa.eadtrust.eu/qtnqc	No Cualificado	1.3.6.1.4.1.501.2.2.3
TSU Test	https://tempus-tsa.eadtrust.eu/qtqc	Cualificado No HSM	1.3.6.1.4.1.501.2.2.3
TSU Test	https://tempus-tsa.eadtrust.eu/qtqc-hsm	Cualificado HSM	1.3.6.1.4.1.501.2.2.3
TSU Preproducción	https://saturno-tsa.eadtrust.eu/qtnqc	No Cualificado	1.3.6.1.4.1.501.2.2.5
TSU Preproducción	https://saturno-tsa.eadtrust.eu/qtqc	Cualificado No HSM	1.3.6.1.4.1.501.2.2.5
TSU Preproducción	https://saturno-tsa.eadtrust.eu/qtqc-hsm	Cualificado HSM	1.3.6.1.4.1.501.2.2.5
TSU Producción	https://cronos-tsa.eadtrust.eu/qtnqc	No Cualificado	1.3.6.1.4.1.501.2.2.1
TSU Producción	https://cronos-tsa.eadtrust.eu/qtqc	Cualificado No HSM	1.3.6.1.4.1.501.2.2.1
TSU Producción	https://cronos-tsa.eadtrust.eu/qtqc-hsm	Cualificado HSM	1.3.6.1.4.1.501.2.2.1

(ETSI-EN-319-421 REQ 8.1)

2. Los OIDs y endpoints del Sello de Tiempo no cualificado son:

Entorno	URL	Certificado usado	OID
TSU Test	https://tempus-tsa.eadtrust.eu/nqtnqc	No Cualificado	1.3.6.1.4.1.501.2.2.2
TSU Preproducción	https://saturno-tsa.eadtrust.eu/nqtnqc	No Cualificado	1.3.6.1.4.1.501.2.2.4
TSU Producción	https://cronos-tsa.eadtrust.eu/nqtnqc	No Cualificado	1.3.6.1.4.1.501.2.2.0
TSU Test (AWS)	https://jano-tsa.eadtrust.eu/nqtnqc	No Cualificado	1.3.6.1.4.1.501.2.2.2
TSU Producción (AWS)	https://eon-tsa.eadtrust.eu/nqtnqc	No Cualificado	1.3.6.1.4.1.501.2.2.0

(ETSI-EN-319-421 REQ 8.2)

A extinguir (OIDs y endpoints del Sello de Tiempo no cualificado, antiguos):

Entorno	URL	Certificado usado	OID
TSU Test (AWS)	tsa-test.eadtrust.net/tsa/default	No Cualificado	1.3.6.1.4.1.501.2.2.2
TSU Producción (AWS)	elastic-tsa.eadtrust.net/tsajson	No Cualificado	1.3.6.1.4.1.19126.2.2.3.1
TSU Producción (AWS	elastic-tsa.eadtrust.net/tsa1	No Cualificado	1.3.6.1.4.1.19126.2.2.3.1
TSU Producción (AWS	elastic-tsa-2.eadtrust.net/tsa1	No Cualificado	1.3.6.1.4.1.19126.2.2.3.1
TSU Producción (AWS	elastic-tsa-lwt.eadtrust.net/tsa1	No Cualificado	1.3.6.1.4.1.19126.2.2.3.1

El árbol OID 1.3.6.1.4.1.501 se identifica con el nombre de la plataforma de EADTrust de gestión de identidades SPRITEL (Secure Platform for Registered Identities and Trusted Electronic Ledger, Plataforma Segura para identidades registradas y Custodia Electrónica Confiable) base de la Autoridad de Registro de EADTrust.

Desde principios de 2023 se han creado nuevos certificados para la provisión de servicios de sello de tiempo cualificado diferenciados por usar diferentes algoritmos criptográficos, tamaño de clave y uso o no de Dispositivo Cualificado de Creación de Sello. Algunos están especialmente diseñados para cumplir requisitos establecidos en el Esquema nacional de Seguridad (ENS) para el Nivel de Seguridad Alto.

Los campos “CommonName” de los nuevos certificados son:

Certificado	Criptografía	Tamaño Clave	QCSD	ENS
EADT QTSU 2023 RSA 2048	RSA	2048	NO	NO
EADT QTSU 2023 ENS alto RSA 3072	RSA	3072	NO	SI
EADT QTSU QSCD 2023 ENS alto RSA 4096	RSA	4096	SI	SI
EADT QTSU 2023 ENS alto ECC 256	ECC	256	NO	SI
EADT QTSU QSCD 2023 ENS alto ECC 384	ECC	384	SI	SI

Y los endpoints:

Certificado	URL	OID
EADT QTSU 2023 RSA 2048	https://cronos-tsa.eadtrust.eu/qtqc	1.3.6.1.4.1.501.2.2.1
EADT QTSU 2023 ENS alto RSA 3072	https://cronos-tsa.eadtrust.eu/qtqcr	1.3.6.1.4.1.501.2.2.1
EADT QTSU QSCD 2023 ENS alto RSA 4096	https://cronos-tsa.eadtrust.eu/qtqcr-qscd	1.3.6.1.4.1.501.2.2.1
EADT QTSU 2023 ENS alto ECC 256	https://cronos-tsa.eadtrust.eu/qtqce	1.3.6.1.4.1.501.2.2.1
EADT QTSU QSCD 2023 ENS alto ECC 384	https://cronos-tsa.eadtrust.eu/qtqce-qscd	1.3.6.1.4.1.501.2.2.1

Endpoint de test:

Certificado	URL	OID
TSU Test	https://tempus-tsa.eadtrust.eu/qtqc	1.3.6.1.4.1.501.2.2.3

11.1 Tipos de Sellado de Tiempo

11.1.1 Sello de tiempo cualificado

El servicio de Sellado de Tiempo cualificado se suministrará a través de la TSA Madrid, desplegada en las instalaciones de EADTrust.

EADTrust contempla en su servicio de sello de tiempo cualificado la posibilidad de usar diferentes tipos de certificados (no cualificado, cualificado sin HSM, cualificado con HSM). En función del tipo de certificado seleccionado, los *endpoints* a los que se dirigirán las peticiones variarán.

La organización se compromete a mayores garantías de seguridad respecto a la gestión de los certificados utilizados en su TSU y en su gestión.

11.1.2 Sello de Tiempo No Cualificado

EADTrust suministrará el servicio de Sellado de Tiempo no cualificado, a través de la TSA Dublín desplegada en Cloud. Este servicio tiene altas presunciones de veracidad técnica, ya que se gestiona de la misma manera que los servicios cualificados.

Asimismo, se ofrecerá también la posibilidad de consumir el servicio desde el CPD de EADTrust en Madrid. El uso de TSU en Madrid reduce los tiempos de latencia, pero no cuenta de la capacidad elástica de la TSU Dublín.

11.2 Variantes del servicio

A los efectos de esta Declaración de Prácticas, se establecen las siguientes variantes de sellado de tiempo:

- Sellado de tiempo inicial. Los sellos de tiempo podrán ser generados inicialmente para un documento electrónico.
- Resellado de tiempo. Los sellos de tiempo podrán ser generados posteriormente para el mantenimiento de un documento o sello previamente existentes.

11.3 Opciones del Servicio

Los sellos de tiempo podrán ofrecer opciones, entre las que se pueden mencionar las siguientes:

- Formato del sello de tiempo, que podrá ser RFC3161
- Precisión del sello de tiempo, que por defecto será de un (1) segundo.
- Custodia del sello producido por EADTrust.

Los perfiles de sello de tiempo se ajustan a las siguientes normas:

- ETSI EN 319 422 V1.1.1 (2016-03) - Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.
- IETF RFC 3161: Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).
- IETF RFC 3628: Policy Requirements for Time-Stamping Authorities (TSAs).
- XML Timestamping Profile of the OASIS Digital Signature Services Version 1.0. OASIS Standard. 11 April 2007.

11.4 Fuentes de tiempo

La fuente de tiempo utilizada en los sistemas de EADTrust es la proporcionada por un sistema de alta precisión sincronizado con la constelación de satélites GPS y Galileo, en concreto se usa un servidor con un receptor simultáneo multisatélite y soporte para GPS, GLONASS, GALILEO y BEIDOU.

Existe una opción de contingencia que prevé la sincronización con la referencia horaria del Real Instituto y Observatorio de la Armada en San Fernando (Cádiz), a través de la Sección de Hora, que resulta accesible mediante el servicio NTP, conforme al RFC 5905 - Network Time Protocol Version 4: Protocol and Algorithms Specification.

Este organismo tiene entre sus misiones la del mantenimiento de la unidad básica de Tiempo, declarado a efectos legales como Patrón Nacional de dicha unidad, así como el mantenimiento y difusión oficial de la escala de "Tiempo Universal Coordinado", considerada a todos los efectos como la base de la hora legal en todo el territorio nacional, según el Real Decreto 1308/1992, de 23 de octubre.

Todos los sistemas que constituyen la infraestructura de Clave Pública de EADTrust están sincronizados en fecha y hora.

El sistema de fuente de tiempo de intranet puede configurarse en base al protocolo NTP o PTP, si bien la precisión necesaria en entornos de uso convencional es de 1 segundo. La precisión interna de la fuente se deriva de la proporcionada por la constelación de satélites:

- **GPS**. US Naval Observatory estableció una escala de tiempo atómico, llamada **Tiempo GPS**, cuya unidad de medida es el segundo atómico internacional. El tiempo de satélite es mantenido, en cada satélite, por dos o por cuatro relojes atómicos. Los relojes de los satélites son monitorizados por las estaciones de seguimiento y los centros de control de la Tierra que en ocasiones los reajustan para mantener cada reloj dentro del Tiempo GPS.
- **Galileo** es el programa europeo de radionavegación y posicionamiento por satélite, desarrollado por la Unión Europea (UE) conjuntamente con la Agencia Espacial Europea. Este programa dota a la Unión Europea de una tecnología independiente del GPS estadounidense y el GLONASS ruso. Galileo proporciona una referencia temporal de alta precisión.

Los tokens de sellado de tiempo se sellan con los certificados EADTrust de TSU, emitidos bajo la Cadena de Certificación descrita en la Declaración de Prácticas de Certificación. Se prevé el uso de certificados cualificados y no cualificados para el servicio de sello de tiempo cualificado. La validez de los certificados cualificados orientados al sellado de tiempo se establece en los propios certificados.

- La calibración de los relojes debe ser mantenida de forma que no resulte previsible un desplazamiento en el tiempo de los mismos.
- Los relojes serán protegidos contra amenazas que pudieran resultar en un cambio no detectado que descalibre el reloj.
- Se asegurará que se detectarán los desplazamientos y saltos del reloj, que impidan su sincronización con Tiempo Universal Coordinado.
- Se asegurará que se mantiene la sincronización del reloj cuando se notifica un segundo de salto, notificado por el órgano competente.

11.5 Participantes en los servicios de sellado de tiempo

Los participantes en los servicios de sellado de tiempo serán los siguientes:

- Prestadores de Servicios de Sellado de Tiempo.
- Entidades y usuarios finales.

Para poder usar el servicio de sello de tiempo, la organización solicitante debe firmar un acuerdo con EADTrust. Dentro de este marco, la entidad usuaria obtendrá suficientes instrucciones y privilegios para autenticarse ante el proveedor del servicio y para enviar datos electrónicamente a la TSA con el fin de crear un sello de tiempo electrónico vinculado a esos datos.

EADTrust puede operar diferentes TSU (timestamping Unit), que podrán desplegarse en las infreatructuras propias o en las instalaciones de las entidades cliente. Para ofrecer garantías de alta disponibilidad, continuidad de negocio, u otros criterios de seguridad que lo justifiquen.

Las características del sello de tiempo son las siguientes:

- Los algoritmos de hash soportados son los de la familia SHA-2
- La TSU emite sellos de tiempo, en referencia a UTC (tiempo universal coordinado) con una precisión mejor que 1 segundo. Se monitoriza esta precisión y se bloquea la posibilidad de emisión de sellos de tiempo si llega a ser peor de 1 segundo. Se tiene en cuenta la posibilidad de reflejar segundos intercalares si fuera necesario en el contexto de mantenimiento del patrón.
- Se limita el uso de los sellos de tiempo de EADTrust a la función de garantizar la existencia de ciertos datos electrónicos con anterioridad a un determinado momento y a su empleo por los organismos o entidades que lo hayan contratado. Un posible uso es el empleo de sellos de tiempo para crear versiones longevas de firmas electrónicas y sellos electrónicos aplicados a documentos electrónicos.
- EADTrust custodia de forma segura los sellos de tiempo expedidos, de forma que puede dar testimonio de su generación más allá del período de vigencia de los certificados, al margen de que los propios sellos de tiempo se incorporen a otros contextos de uso, como por ejemplo la extensión de firmas electrónicas.
- El subscriptor debe hacer uso del servicio mediante el mecanismo de autenticación proporcionado por EADTrust y cumplir sus compromisos de pago. En caso de instalación en sus

infraestructuras, deberá proporcionar un sistema de alimentación eléctrica y de comunicaciones adecuado. Deberá configurar los firewalls de forma que permitan la administración remota.

- Los terceros que confían en los sellos de tiempo de EADTrust deberían ser capaces de comprobar los sellos de tiempo y los certificados que los acompañan. Las TSU solo emiten sellos de tiempo mientras el certificado está vigente y si fuera preciso revocarlo, se deja de usar la clave privada asociada. Aunque no se prevé que pueda quedar expuesta la clave privada, la consulta de la revocación de certificado permite descartar cualquier riesgo en ese sentido.

En cuanto a los certificados que respaldan los sellos de tiempo, consulte la sección de perfiles de certificados en esta DPC (CPS). Se contemplan certificados cualificados y no cualificados para la expedición de sellos de tiempo cualificados.

12 Uso de los sellos de tiempo

12.1 Usos permitidos

Los sellos de tiempo se podrán solicitar para cualquier tipo de documento, firmado o no electrónicamente, y para cualquier tipo de objeto digital, incluso código ejecutable, garantizándose la existencia de dichos contenidos a la fecha indicada dentro del sello. También podrán solicitarse sellos sobre sellos anteriormente expedidos (resellado).

13 Límites y prohibiciones de uso de los sellos de tiempo

13.1 Límites de uso

Los sellos se emplearán para su función propia y finalidad establecida, sin que puedan emplearse en otras funciones y con otras finalidades.

Los sellos pueden incorporar límites de uso por razón de la materia y de la cuantía, que se establecen en las extensiones del certificado de Entidad de Sellado de Tiempo emitido por EADTrust, así como en la correspondiente política de sellado de tiempo, que se indicarán en las correspondientes condiciones generales de emisión y uso de sellos de tiempo.

13.2 Prohibiciones de usos

Los sellos no se han diseñado, no se pueden destinar y no se autoriza su uso en equipos de control de situaciones peligrosas o para usos que requieren actuaciones a prueba de fallos, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicaciones aéreas, o sistemas de control de armamento, donde un fallo pudiera directamente conllevar la muerte, lesiones personales o daños medioambientales severos.

Todas las responsabilidades legales, contractuales o extra contractuales, daños directos o indirectos que puedan derivarse de usos limitados y/o prohibidos quedan a cargo del suscriptor. En ningún caso podrán el suscriptor o los terceros perjudicados reclamar a EADTrust compensación o indemnización alguna por daños o responsabilidades provenientes del uso de los sellos para los usos limitados y/o prohibidos.

14 Ciclo de Vida de los Sellos de Tiempo

14.1 Solicitud de sello de tiempo

14.1.1 Legitimación para solicitar la emisión

Antes de la emisión de sellos de tiempo, debe existir un procedimiento de alta de suscriptor al servicio de sellado, en el que se determinarán las personas y sistemas que podrán solicitar sellos de tiempo, y de acuerdo con qué calidades y opciones.

14.1.2 Procedimiento de alta

Antes del alta como suscriptor, EADTrust informará al suscriptor de los términos y condiciones aplicables al servicio. La citada información se comunicará en soporte duradero, en papel o electrónicamente y en lenguaje fácilmente comprensible, y tendrá los siguientes contenidos mínimos:

- La información de contacto de la Entidad de Sellado de Tiempo.
- La política de sellado de tiempo aplicable.
- Al menos un algoritmo de resumen criptográfico que se pueda emplear para representar los datos para los que se solicita el sello de tiempo.
- El periodo previsto de vida de la firma electrónica empleada para firmar el sello de tiempo (Esta duración dependerá del algoritmo de resumen, algoritmo de firma y longitud de clave privada empleados por la Entidad de Sellado de Tiempo).
- La precisión del tiempo del sello, con respecto al Tiempo Universal Coordinado.
- La disponibilidad del servicio, incluyendo los tiempos previstos de recuperación y de parada programados.
- Cualesquiera limitaciones en el uso del servicio de sellado de tiempo.
- Las obligaciones del suscriptor del servicio de sellado de tiempo.
- Las obligaciones del tercero que confía en sellos de tiempo.
- Información sobre cómo verificar el sello de tiempo, de forma que el tercero pueda decidir de forma razonable confiar o no en el mismo, así como cualesquiera limitaciones en el periodo de validez del sello.
- El periodo durante el cual la Entidad de Sellado de Tiempo retiene registros de auditoría.
- El sistema jurídico que resulte aplicable a la prestación del servicio, incluyendo el cumplimiento de los requisitos establecidos por la legislación aplicable.
- Limitaciones de responsabilidad.

- Procedimientos de reclamaciones y resolución de disputas.
- Si la Entidad de Sellado de Tiempo ha sido declarada conforme con la política de sellado aplicable, y en este caso, por qué organismo independiente.

Tras la adhesión a las condiciones generales del servicio por el suscriptor, EADTrust procederá a su alta en el sistema, habilitando los medios técnicos para recibir solicitudes de sello. EADTrust soportará protocolos de transporte (RFC 3161, sección 3) de las solicitudes de sellado de tiempo que sean síncronos o asíncronos, y entre ellos, al menos dispondrá de la posibilidad de solicitar el servicio empleando HTTP.

14.2 Procesamiento de la solicitud de sello de tiempo

Una vez recibida una solicitud de sello de tiempo, EADTrust debe verificar los siguientes aspectos:

- La procedencia y la autenticidad de la solicitud, mediante el protocolo de seguridad apropiado al medio de transporte empleado, incluyendo al menos SSL/TLS para el protocolo HTTP (RFC 3161 no establece ningún método para autenticar al solicitante de sellos, sino que esta posibilidad debe implantarse mediante la seguridad del protocolo de transporte de las solicitudes, como es HTTPS).
- La corrección técnica (RFC 3161, sección 2.4.1) de la solicitud, de acuerdo con el protocolo escogido y, en concreto, que la solicitud contiene:
- El número de versión.
- Un resumen criptográfico válido conforme a uno de los algoritmos apropiados, según se expone posteriormente.
- Opcionalmente, el número de ocurrencia única (nonce), generado por el suscriptor.
- Se considerarán válidos los algoritmos de resumen SHA-2 o posteriores
- La solicitud no deberá contener extensiones
- En caso de verificación incorrecta de la solicitud, se devolverán los mensajes de error apropiados (RFC 3161, sección 2.4.2).

14.3 Emisión del sello de tiempo

Tras la verificación de la solicitud se procederá a la emisión del sello de tiempo, de forma segura. EADTrust deberá

- Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de sellado de tiempo a los que sirven de soporte.
- Emplear fuentes de tiempo fiables, de acuerdo con los requisitos establecidos en la sección correspondiente de esta política.
- Generar sellos de tiempo conteniendo las informaciones incluidas en la sección 17 de esta política.
- Emplear una clave específica para la firma de los sellos generados, de acuerdo con los requisitos de gestión de claves especificados en la sección 15.2de esta política.

14.4 Entrega del sello de tiempo

14.4.1 Entrega del sello de tiempo

EADTrust deberá entregar el sello al solicitante, mediante el protocolo de transporte empleado para la solicitud. La respuesta protocolaria deberá contener el resultado de la solicitud y, en su caso, el sello emitido (RFC 3161, sección 2.4.2).

14.4.2 Publicación del sello de tiempo

EADT no publica los sellos de tiempo. En su defecto se conservará almacenados en las bases de datos habilitados a este efecto y en las copias de seguridad de estas bases de datos pudiendo obtenerse un listado completo o parcial de los emitidos para un subscriptor mediante solicitud previa.

14.4.3 Notificación de la emisión a terceros

EADTrust podrá establecer casos y métodos en que se notifique la emisión a terceros, de acuerdo con las necesidades de los suscriptores.

14.4.4 Finalización de la suscripción

Transcurrido el plazo contractualmente establecido, finalizará la suscripción al servicio, y no se podrán seguir solicitando sellos de tiempo.

15 Gestión y funcionamiento del prestador de servicios de confianza

15.1 Organización interna

15.1.1 Fiabilidad de la organización

EADTrust está sujeta a las validaciones anuales de la norma UNE-ISO/IEC 27001 que regula el establecimiento de procesos adecuados para garantizar una correcta gestión de la seguridad en los sistemas de información. Con periodicidad anual lleva a cabo otras auditorías UNE-ISO relativas a las normas de calidad ISO 9001, ISO 20000-1 respectivamente. Desde 2022 se audita el cumplimiento de los requisitos de ENS (Esquema nacional de Seguridad) de nivel medio.

EADTrust aplica principios de no discriminación entre sus clientes y entre sus trabajadores. Con este enfoque ha implantado en su operativa interna un Plan de Igualdad de oportunidades en el marco de la relación laboral, con medidas concretas para eliminar barreras que puedan limitar o impidir el desarrollo profesional de ningún colectivo.

En este mismo sentido trabaja para ofrecer servicios cada vez más accesibles y comprometidos con los objetivos de sostenibilidad de las NNUU[51].

EADTrust podrá externalizar o subcontratar a terceros algunas de las operativas requeridas en la emisión/revocación de certificados. En todos los casos la relación contractual se documentará por escrito.

En caso de producirse afectaciones a terceros por la actuación del subcontratista, EADTrust mantiene la responsabilidad general sobre los servicios. No obstante, se reservará el derecho de utilizar las herramientas legales que estime pertinentes, para repetir contra el subcontratado que incumpla los requisitos definidos en la legislación vigente, en esta Declaración de Prácticas de Certificación y en la Política específica de servicios de confianza aplicable al certificado de interés.

15.1.2 Segregación de tareas

Existen tareas que se han separado de acuerdo a las funciones a desempeñar. EADTrust sigue la política de seguridad CIMC (Certificate Issuing and Management Component)[52] que se define en su modelo de seguridad.

15.2 Recursos Humanos

15.2.1 Antecedentes, cualificaciones, experiencia y requisitos de aplicación

EADTrust mantiene una política de contratación de personal que busca los perfiles adecuados para su actividad y cuenta con criterios de idoneidad para la asignación de roles y responsabilidades.

EADTrust cumple con sus obligaciones en materia de igualdad y, en el marco de las relaciones con sus empleados, tiene asumido un compromiso fehaciente para la promoción e implantación efectiva de los principios de igualdad de oportunidades entre mujeres y hombres, y de no discriminación por razón de género, raza, origen, religión, etc.

En este mismo sentido manifiesta su compromiso de trabajo para garantizar la accesibilidad de sus servicios e instalaciones a todas las personas, independientemente de sus capacidades técnicas, cognitivas o físicas.

Todo el personal con funciones de confianza está libre de cualquier interés que pueda afectar su imparcialidad con respecto a las operaciones de EADTrust.

[51] https://www.un.org/sustainabledevelopment/es/objetivos-de-desarrollo-sostenible/

[52] https://www.commoncriteriaportal.org/files/ppfiles/cert-issu-v15-sec-eng.pdf.

15.2.2 Procedimientos de comprobación de antecedentes penales

Según la legislación española no es aplicable la solicitud de antecedentes penales a los trabajadores por parte de las empresas. Existe una prohibición general de discriminar a cualquier trabajador, por cualquier motivo, tanto en el empleo como en el acceso al mismo. Así se prevé específicamente en el artículo 14 de la Constitución Española, el artículo 4.2 del Estatuto de los Trabajadores y el artículo 73.2 de la Ley General Penitenciaria. Conforme a la legislación española y por criterio reiterado de los tribunales, debe primar el derecho a la intimidad y a la reinserción laboral.

15.2.3 Requisitos de formación

El personal contratado por EADTrust deberá ser capaz de cumplir el requisito de "conocimientos, experiencia y cualificaciones" mediante formación y credenciales formales, o experiencia real, o una combinación de ambas.

EADTrust proporciona a su personal la formación necesaria para desempeñar sus responsabilidades laborales de manera competente y satisfactoria. La formación del personal de nueva incoporación incluye lo siguiente:

- Una copia de la Declaración de Prácticas de Servicios Electrónicos de Confianza.
- Manual de Bienvenida
- Politica de seguridad de la Información
- Sensibilización sobre la seguridad.
- Funcionamiento del software y hardware para cada función específica.
- Procedimientos de seguridad para cada función específica.
- Procedimientos de gestión y operación para cada función específica.
- Procedimiento de recuperación de desastres.
- Procedimiento de gestión de incidencias

Entre los requisitos de seguridad aplicable se encuentran los recogidos en el Sistema de Gestión de la Seguridad de la Información desarrollado en el marco de la certificación ISO 27001.

15.2.4 Frecuencia y requisitos de cursos de perfeccionamiento

Cualquier cambio significativo en las operaciones de la PKI de EADTrust requerirá un plan de formación y la implementación del plan será documentada. Con periodicidad mínima anual (cada 12 meses) se llevan a cabo acciones formativas internas y externas para mantener actualizados los conocimientos; en particular sobre las nuevas amenazas y las prácticas de seguridad más actuales.

15.2.5 Rotación y secuencia laboral

No aplica

15.2.6 Sanciones para acciones no autorizadas

Incidentes de seguridad de la información. EADTrust tiene un plan de gestión de incidentes de seguridad.

Sanciones para acciones no autorizadas. EADTrust aplica el régimen disciplinario y las sanciones definidas en la legislación laboral vigente, para lo cual toma en consideración las circunstancias de los hechos, las personas involucradas, y la gravedad de las actuaciones.

15.2.7 Puestos de confianza

En las descripciones de los puestos de trabajo disponibles para todo el personal afectado, se documentan las funciones y responsabilidades de seguridad, generales y específicas; tal como se establece en la política de seguridad de la información de EADTrust. Entre ellas las funciones de confianza a cumplir en roles concretos.

Un "puesto de confianza" se define como las funciones asignadas a una persona o más personas que pueden conllevar problemas de seguridad si no se realizan satisfactoriamente, ya sea de forma accidental o intencionada.

Por política, cada rol de confianza de la CA de EADTrust tiene asignado una o varias personas en el rol específico y su sustituto, todos nombrados por la Direccion general de EADTrust. De esta manera se garantiza la continuidad de las operaciones.

A continuación, se describen los roles de confianza para la operación de la CA de EADTrust y el número de personas requeridas para la ejecución de las tareas de cada rol de confianza en la regla n de m personas:

Roles de confianza	Descripción	Número de personas requeridas por tarea	Reglas de segregación de tareas
Oficial de Seguridad CA/TSA	Responsable general de coordinar, controlar y hacer cumplir las medidas de seguridad definidas en la Politica de seguridad de la organización.	1 rol principal y 1 Sustituto	Incompatible con Auditor Interno y Administrador de Sistemas.
Administrador de Sistemas de la CA	Autorizados a instalar, configurar y mantener los sistemas de confianza del TSP para la gestión de servicios. Esto incluye la recuperación del sistema de la CA y la TSA	1 rol principal y 1 Sustituto	Incompatible con Auditor Interno y Oficial de Seguridad.
Operador de Sistemas de la CA	Responsable de operar los sistemas de confianza del TSP diariamente. Autorizados a realizar las copias de seguridad del sistema.	1 rol principal y 1 Sustituto	Incompatible con Auditor Interno y Oficial de Seguridad.
Operador de RA Rango II (Emisión)	Identificación de Solicitantes/Suscriptores de certificados para emisión	2 roles principales y 1 sustituto	Incompatible con Auditor Interno. Un operador de RA que haya emitido un certificado no podrá realizar la revocación del mismo certificado.

Operador de RA Rango II (Revocación)	Identificación de Solicitantes de revocación de certificados.	1 rol principal y 1 sustituto	Incompatible con Auditor Interno. Un operador de RA que haya emitido un certificado no podrá realizar la revocación del mismo certificado.
Operador de RA Rango I (Validación)	Validación de identidad declarada por el Solicitante/Suscriptor del certificado ante el operador de RA de Rango II. Aprobación de la emisión/revocación del certificado.	2 roles principales que se sustituyen entre si	Incompatible con Auditor Interno.
Especialista en Validación de certificados web	Validación y comprobación de nombres de dominio.	1 rol principal y 1 Sustituto	Incompatible con Auditor Interno.
Auditor Interno	Responsable de verificar el cumplimiento de los procedimientos operativos de la CA t la TSA de EADTrust	1 de 1 persona	Incompatible con cualquier otro rol.

15.2.8 Identificación y autenticación para cada puesto

El personal nombrado en un rol de confianza accede a las operaciones con certificado o usuario y contraseña únicos que le identifican bajo los principios de menor acceso posible. Al mismo tiempo, se aplican políticas de control dual de las operaciones, de manera que una persona no puede completar por sí sola, todo el proceso de emisión/revocación de certificados. La operativa requiere de permisos y validaciones adicionales de otros roles nombrados.

15.3 Gestión de activos

15.3.1 Requisitos Generales

EADTrust mantiene actualizado un inventario de todos los activos de información a los que ha asignado una clasificación coherente con la evaluación de riesgos y aplica controles que garantizan la seguridad y privacidad de la información.

El Sistema de gestión de la Seguridad de la Información (SGSI) es auditado con periodicidad mínima anual, con el fin de garantizar un nivel adecuado de protección de los activos; incluidos los activos de información.

15.3.2 Manejo de medios

EADTrust ha desplegado políticas y procedimientos para el manejo seguro de medios, equipamiento y soportes de información. Para protegerlos de daños, robos, el acceso no autorizado y la obsolescencia.

Los procedimientos de gestión de soportes regulan medidas contra la obsolescencia y el deterioro de los soportes en el período de tiempo en que se requiere la conservación de los registros.

15.4 Control de accesos

La política de control de accesos de EADTrust se ha diseñado teniendo en cuenta las funciones a desempeñar en cada puesto de trabajo, los roles de confianza y su intervención en operaciones críticas de la CA y la organización.

La configuración y administración de permisos de acceso se gestionan bajo el principio de "menor privilegio" de acceso; garantizando la separación de las funciones de administración y operación de la seguridad y estableciendo controles sobre el uso de los programas de utilidad del sistema.

El personal que opera en roles de confianza para realizar tareas críticas de la CA posee cuentas que requieren la identificación y autenticación antes de llevar a cabo alguna de las citadas tareas. EADTrust conserva los registros de eventos relacionados con el acceso.

15.5 Controles criptográficos

EADTrust establece controles de seguridad apropiados para la gestión de claves criptográficas y de dispositivos criptográficos a lo largo de su ciclo de vida.

15.5.1 Generación del par de claves

Los sistemas de gestión de claves propios de EADTrust como Prestador de Servicios de Confianza Digital en sus jerarquías de certificación emplean software y dispositivos específicos para la protección de claves privadas.

Las Root CA se gestionan mediante procedimientos Off-line, mientras que las CA subordinadas se gestionan en dispositivos cualificados de creación de firma que permiten una operación on-line con rigurosos controles operativos.

Antes de la caducidad de un certificado de CA, EADTrust realizará, con suficiente antelación, al menos de un (1) mes, una nueva ceremonia de generación de claves para la CA a la que afecte esta situación.

No se emitirán certificados de Sub CA con una fecha de caducidad posterior a la de la CA que la emite.

No se emitirán certificados de entidad final con una fecha de caducidad posterior a la de la CA que la emite.

Los certificados de CAs roots y subordinadas estarán disponibles en los repositorios de EADTrust accesibles a través de la web, incluso cuando hayan caducado.

15.5.2 Entrega de la clave privada al suscriptor/titular de la clave

Método de entrega de clave privada al suscriptor/titular del certificado:

- Certificados emitidos en un token criptográfico o en una tarjeta criptográfica: las claves privadas para la autenticación y la firma se entregan en un dispositivo criptográfico.
- Certificados gestionados en nombre del firmante: se entrega al usuario, los medios de identificación y autenticación para garantizar su control exclusivo de los medios de creación de firma. En el servicio de firma o sello electrónico en nombre del firmante no se contemplan otros usos diferentes de la clave privada.
- Certificados emitidos en HSM: las claves privadas para la autenticación y la firma se alojan en un dispositivo criptográfico.
- Certificados emitidos en un mecanismo de software: la clave privada es generada por el servidor o PC del usuario.
- Certificados emitidos en un mecanismo de software con generación de clave privada. En este caso se entrega un fichero PKCS#12 cifrado con un mecanismo de entrega de clave de descifrado diferente, reforzado con diversidad de canal. La clave privada se elimina al generar el fichero PKCS#12 y el fichero PKCS#12 se elimina cuando se confirma la descarga por el cliente.

15.5.3 Entrega de la clave pública al emisor del certificado

El método utilizado para entregar la clave pública a la RA de EADTrust es el siguiente:

- CAs emisoras: la clave pública se envía a la entidad emisora raíz en formato X.509 o PKCS#10 (este es el caso de solicitud de certificados).
- Certificados emitidos en un dispositivo criptográfico: se leen desde el dispositivo criptográfico.
- Mecanismo de software de certificado: la clave pública se envía a la CA de EADTrust en formato PKCS#10.

15.5.4 Entrega de la clave pública de la CA a los terceros que confían

Las claves públicas de la CA de EADTrust están diponibles a través del sitio web de EADTrust.

15.5.5 Tamaños de clave

El algoritmo de hash utilizado es SHA-2 o posteriores. Se excluye el uso del algoritmo SHA-1

El tamaño de la clave de la autoridad raíz, dependiendo de cada caso, es:

- Respecto al algoritmos RSA: tamaños de clave de 2048 bits, 4096 y 8192.
- Respecto al algoritmos ECC: ECDSA 256 (prime256v1) y ECDSA 384 (secp384r1).

15.5.6 Generación y comprobación de calidad de los parámetros de clave pública

Se ha verificado la generación de claves para que no sea susceptible de un ataque de tipo ROCA (Return Of Coppersmith Attack)[53]

[53] https://github.com/crocs-muni/roca

15.5.7 Propósitos de uso de la clave (según el campo de uso clave X.509 v3)

Todos los certificados incluyen la extensión del Key Usage and Extended Key Usage, que indica los usos de clave activada.

La extensión de "Key Usage" contempla la firma digital (digital signature) como mecanismo de autenticación), el cifrado de claves y de datos y el compromiso con el contenido (content commitment), en el sentido de mecanismo de firma con certeza de prestación el consentimiento.

La extensión de "Extended Key Usage" contempla la autenticación de cliente o servidor, el inicio de sesión con un token criptográfico o tarjeta inteligente o la protección de correo electrónico.

Las claves de CA raíz sólo se utilizarán para firmar certificados de CA subordinados y las CRLs y las claves para las CA subordinadas o emisoras sólo se utilizarán para firmar certificados de usuario final, CRL y respuestas a OCSP.

15.6 Protección de la clave privada en módulo criptográfico

Las Autoridades de certificación raíz se gestionan OFF-LINE y están cifradas mediante un dispositivo criptográfico. Existen varias claves privadas según los algoritmos RSA y ECC y tienen diferentes tamaños de clave (Hasta 8192 Bits en RSA y 384 bits en ECC – Elliptic Curve Cryptography)

El dispositivo criptográfico utilizado está certificado FiPS140-2 nivel 3. Versiones posteriores del mismo dispositivo, han superado la certificación Common Criteria EAL 4 +.

Cuando se preste el servicio de firma o sello electrónico en nombre del firmante, el dispositivo criptográfico estará certificado según la certificación Common Criteria EAL4+.

15.6.1 Normas y controles del módulo criptográfico

Un módulo de seguridad de hardware (HSM) es un dispositivo de seguridad que genera y protege claves criptográficas. Los HSM deben cumplir con un mínimo de FIPS 140-2 Nivel 3 o Common Criteria EAL4+ o posteriores.

EADTrust mantiene protocolos para verificar que un HSM no ha sido manipulado durante el transporte y el almacenamiento.

Los dispositivos criptográficos con certificados de firma electrónica cualificados, adecuados como dispositivos cualificados de creación de firmas (DCCF, en inglés QSCD, qualified signature creation device), cumplen con los requisitos del nivel de seguridad CC EAL4+, aunque también son aceptables las certificaciones que cumplan con un mínimo de FIPS 140-2 Nivel 3.

EADTrust, en cualquier caso, mantiene el control sobre la preparación, el almacenamiento y la distribución de los dispositivos de abonado en los que EADTrust genera claves.

EADTrust monitoriza que los dispositivos utilizados mantengan la certificación. Entre otras referencias se utiliza la siguiente: "Compilation of: Member States' notifications on: Designated Bodies under Article 30(2) and 39(2) of Regulation 910/2014 and Certified Qualified Signature Creation Devices under Article 31(1)-(2), and Certified Qualified Seal Creation Devices under Article 39(3) of Regulation 910/2014, and information from Member States on: Secure Signature Creation Devices benefiting from the transitional measure set in article 51(1) of Regulation 910/2014".[54]

15.6.2 Control multi-persona (n de m) de la clave privada

El uso de claves privadas de CA requiere la actuación de al menos dos personas. Por un lado, el control de acceso a los dispositivos, y por otro el conocimiento de las claves y el acceso a los procesos informáticos que permiten la generación de claves y certificados.

15.6.3 Escrow de clave privada de la CA

Existe un procedimiento de gestión de seguridad que permite reconstruir la clave privada del mecanismo de cifrado de claves de root accediendo a un Notario que custodia una fracción de la clave, pero que además requiere otra fracción custodiada en los sistemas de seguridad física de EADTrust.

15.6.4 Copia de seguridad de la clave privada

Existe un procedimiento para la recuperación de claves al módulo criptográfico de la CAs subordinadas que puede aplicarse en caso de contingencia. Se aplicarán los mismos controles multipersona indicados.

15.6.5 Archivo de la clave privada

EADTrust no archivará la clave privada de firma de certificados una vez caducada.

Las claves privadas de los titulares de los certificados se gestionan por ellos. EADTrust no conserva claves privadas de los titulares, salvo en el caso de que estos hayan contratado un servicio de firma en servidor. Si la clave privada ha sido generada por EADTrust antes de su entrega al suscriptor, se elimina tras comprobar que el suscriptor la ha recibido, según el procedimiento de registro.

Cuando el titular del certificado ha contratado el servicio de firma en servidor, las claves residen en un HSM y la información que habilita su uso no es conocida por EADTrust. Para hacer uso de la firma en servidor se gestionan sistemas de identificación y autenticación que conllevan el empleo de ciertos datos por el usuario que son necesarios para activar su clave privada.

15.6.6 Transmisión de la clave privada a módulo criptográfico

Sólo en caso de contingencia se utilizará el procedimiento descrito anteriormente haciendo referencia a un notario para recuperar claves privadas en los módulos criptográficos.

[54] https://eidas.ec.europa.eu/efda/browse/notification/qscd-sscd

15.6.7 Almacenamiento de la clave privada en un módulo criptográfico

Existe un documento de procedimiento de la clave de la CA que describe los procesos para generar la clave privada y el uso de hardware criptográfico.

En la generación de claves de la CA, EADTrust sigue las recomendaciones de ETSI EN 319 411 y las Directrices de Requisitos Básicos 17.7.[55]

En los casos en que las claves privadas se almacenen fuera de los módulos criptográficos, se protegerán para garantizar el mismo nivel de protección que si estuvieran físicamente dentro de los módulos criptográficos. Todos los HSM utilizados por EADTrust para almacenar claves privadas para las Autoridades de Certificación tienen certificación FIPS 140-2 de nivel 3, o Common Criteria EAL4+.

15.6.8 Método de activación de una clave privada

La CA raíz y las claves de las CAs subordinadas se activan mediante un proceso que requiere al menos control dual para el acceso y gestión de los dispositivos criptográficos (tokens criptográficos o tarjetas).

El suscriptor/titular del certificado accede a la clave privada mediante un PIN. El dispositivo tiene un sistema que lo protege contra los intentos de acceso que lo bloquean cuando se introduce el código incorrecto cierto número de veces. El suscriptor /titular del certificado tiene un código de desbloqueo de dispositivo. Si se introduce erróneamente cierto número de veces, el dispositivo se bloquea definitivamente y no se puede recuperar la información contenida en su interior.

15.6.9 Método de desactivación de una clave privada

La desactivación de la clave privada se llevará a cabo con la revocación del certificado asociado a la clave publica correspondiente a la clave privada desactivada.

15.6.10 Método de destrucción de una clave privada

Existe un procedimiento para la destrucción de claves de CA.

En caso de retirar el HSM que contiene las claves de la CA, estas serán destruidas. El propio HSM incluye un sistema de detección de movimiento que inicializa el dispositivo.

15.6.11 Calificación del módulo criptográfico

Como se ha indicado en el apartado “Normas y controles del módulo criptográfico de esta sección.

[55] https://cabforum.org/baseline-requirements-documents/

15.7 Otros aspectos de la gestión del par de claves

15.7.1 Archivo de la clave pública

Los certificados generados por la CA, y por lo tanto las claves públicas, son almacenados por la CA durante el período de tiempo previsto de custodia de la documentación.

15.7.2 Periodos operacionales del certificado y del par de claves

El período en el que se puede utilizar la clave privada asociada a la clave pública incluida en los certificados debe estar comprendido entre la fecha de emisión del certificado y la de caducidad.

El período de vigencia de los certificados emitidos por EADTrust puede verificarse, consultando la información recogida en el campo del certificado denominado: **validity**.

15.8 Datos de activación

15.8.1 Generación e instalación de datos de activación

- Certificados emitidos en un dispositivo criptográfico: Se necesitan datos de activación (PIN) o una contraseña para operar la clave privada asociada a cada certificado.
  Los datos de activación (PIN) o contraseña son:
  - Generados aleatoriamente por el software de EADTrust y almacenados en el dispositivo criptográfico soportado por el certificado,
  - Generados e impresos al emitir el certificado.
  - Entregados al usuario a través de un sistema que asegura la confidencialidad.
  - EADTrust proporciona a los suscriptores una opción para cambiar el código PIN de la tarjeta o del token.
  - El PIN nunca se almacena por parte de EADTrust.
- Certificados emitidos en un mecanismo de software: la instalación y activación de la clave privada asociada a un certificado requiere el uso de sistemas de seguridad definidos por el usuario.

15.8.2 Protección de los datos de activación

Con respecto a los datos de activación de firmas, los usuarios de certificados deben:

- Memorizar los datos.
- Hacer todo lo posible para proteger los datos.
- Abstenerse de almacenar datos de activación (PIN o PUK) junto al dispositivo criptográfico o compartirlo con otras personas.
- Cambiar el PIN antes de usarlo.

15.8.3 Otros aspectos de los datos de activación

La vida útil de los datos de activación no está estipulada. Sin embargo, deben cambiarse periódicamente para disminuir la posibilidad de que sean expuestos.

15.9 Seguridad física y ambiental

EADTrust está sujeta a las validaciones anuales de la norma UNE-ISO/IEC 27001 que regula el establecimiento de procesos adecuados para garantizar una correcta gestión de la seguridad en los sistemas de información.

EADTrust tiene establecidos controles de seguridad física y ambiental para proteger los recursos de las instalaciones donde se encuentran los sistemas, los propios sistemas y los equipamientos empleados para las operaciones.

La política de seguridad física y ambiental aplicable a los servicios de generación certificados ofrece protección frente:

- Controles físicos de entrada.
- Seguridad de oficinas, despachos e instalaciones.
- Protección contra las amenazas externas y ambientales.
- Trabajo en áreas seguras.
- Áreas de carga y descarga.
- Emplazamiento y protección de equipos.
- Instalaciones de suministro.
- Seguridad del cableado.
- Mantenimiento de los equipos.
- Retirada de materiales propiedad de la empresa.
- Seguridad de los equipos fuera de las instalaciones.
- Reutilización o eliminación de equipos.
- Política de dispositivos móviles.

15.9.1 Localización y construcción de las instalaciones

EADTrust cuenta con infraestructura adecuada para prestar servicios de confianza digital en sus instalaciones de Madrid, y además para ciertos servicios (OCSP, por ejemplo) podrán contratarse Prestadores de Servios de Hosting y de Cloud Computing, como por ejemplo Amazon[56] y OVH[57]

[56] Aspectos de cumplimiento de Amazon: https://aws.amazon.com/es/compliance/

[57] Aspectos de cumplimiento de OVH: https://www.ovh.com/world/private-cloud/documentation/certifications.xml

15.9.2 Acceso físico

La protección física de las instalaciones se lleva a cabo mediante la creación de perímetros de seguridad con protección física contra la intrusión, controles de acceso a través del perímetro de seguridad y alarmas para detectar la intrusión.

La calidad y solidez de los materiales de construcción de las instalaciones garantiza unos adecuados niveles de protección frente a intrusiones por la fuerza bruta y su ubicación en una zona de bajo riesgo de desastres, permite un rápido acceso ante cualquier contingencia.

La sala donde se realizan las operaciones criptográficas en el Centro de Proceso de Datos cuenta con redundancia en sus infraestructuras, así como varias fuentes alternativas de electricidad y refrigeración en caso de emergencia. Se dispone de instalaciones que protegen físicamente la prestación de los servicios de aprobación de solicitudes de certificados y de gestión de revocación, del compromiso causado por acceso no autorizado a los sistemas o a los datos, así como a la divulgación de los mismos.

- Control sobre el acceso físico a la instalación.
  - Sólo se permite el acceso al personal autorizado.
  - Los derechos de acceso al área de seguridad son revisados y actualizados periódicamente.
  - Todo el personal está identificado y no es posible circular en el edificio sin estar identificado y acompañado por un empleado.
  - El personal que no está en la lista de acceso de EADTrust y que puede estar trabajando en el sitio está debidamente supervisado.
- El acceso a las instalaciones que acogen los servidores implica la videograbación de la actividad y requiere identificación biométrica y control dual de los accesos.
- Se lleva a cabo el registro de los accesos a las instalaciones que acogen los servidores.
  Se cuenta con medidas adicionales de limitación de accesos al edificio en las oficinas de EADTrust.
- Las RAs cumplen con los criterios de seguridad necesarios definidos en el documento de securitización del sitio de registro.

El acceso a la zona de oficinas y salas de reuniones por personal ajeno a la entidad se controla mediante un registro de visitas.

15.9.3 Electricidad y aire acondicionado

El centro de procesamiento de datos dispone de energía y aire acondicionado suficientes para crear un entorno operativo fiable.

Los equipos de servicio son de bajo consumo y de baja disipación térmica por lo que pueden continuar en uso incluso si falla el aire acondicionado por un período prolongado.

Los sistemas de alimentación ininterrumpida garantizan un tiempo de funcionamiento superior a 10 horas en caso de que se produzca un corte prolongado de suministro eléctrico.

En caso de corte eléctrico prolongado, se procederá a la parada ordenada de sistemas. Los sistemas OCSP que informan sobre el estado de revocación de los certificados no se ven afectados por la parada de sistemas ya que pueden gestionarse en un entorno de alta disponibilidad alojado externamente.

15.9.4 Exposición al agua

EADTrust ha tomado las precauciones necesarias para minimizar el impacto de la exposición al agua. Sus instalaciones se encuentran en un emplazamiento geográficamente elevado.

15.9.5 Prevención y protección contra incendios

El centro de procesamiento de datos de EADTrust tiene barreras físicas que se extienden desde el suelo hasta el techo, así como sistemas automáticos de medida de humedad y temperatura que registrarán situaciones anómalas antes de que pueda producirse un incendio.

Cuenta con equipos de extinción debidamente señalizados y adecuados al tipo de equipamiento existente. La puerta cuenta con una protección adicional de espuma ignífuga.

15.9.6 Almacenamiento de soportes

Los soportes que contienen información de backup se almacenan de forma segura.

15.9.7 Eliminación de residuos

Existe una política para regular los procedimientos que rigen la destrucción de los medios de información.

Los soportes de almacenamiento que contienen información confidencial se destruyen para garantizar que los datos no sean legibles o recuperables después de la eliminación. EADTrust ha adoptado una política de gestión de residuos diseñada para poder superar una auditoría ISO 14001.

15.9.8 Copia de seguridad externa

EADTrust mantiene un sistema de copias de seguridad cifradas de ciertas claves en un repositorio seguro en las propias instalaciones.

Además, se mantienen backups cifrados de los sistemas de las bases de datos y del código fuente en un repositorio en la nube.

15.10 Seguridad de las operaciones

15.10.1 Controles de desarrollo del sistema

EADTrust utiliza sistemas y productos de confianza que están protegidos contra las modificaciones y que garantizan la seguridad técnica y la fiabilidad de los procesos soportados por ellos. Existe un repositorio para el control de versiones de software.

Los sistemas de producción se revisan periódicamente para comprobar que las actualizaciones de seguridad publicadas por los desarrolladores están correctamente aplicadas. En particular: sistema operativo, bases de datos y aplicaciones críticas. Los desarrollos propios se verifican antes de su paso a producción. En la fase de diseño y especificación de requisitos de cualquier proyecto de desarrollo de sistemas se analizan los riesgos y se toman medidas para prevenir, mitigar y erradicar posibles riesgos y vulnerabilidades en los sistemas.

Para evitar posibles problemas con estos sistemas, se aplican los siguientes controles:

- Existen prácticas de coordinación para actualizar las bibliotecas del software (incluidos los parches) en la producción. La autorización se concede sólo después de asegurarse de que funciona correctamente.
- El sistema de pruebas se mantiene separado del sistema de producción para asegurarse de que funciona correctamente antes de pasar a producción.
- Existe un registro de dependencias para garantizar que una actualización no inhabilita una función de seguridad requerida de modo que se pueda controlar el nivel de versión adecuado.
- Se conservan las versiones anteriores del software propio.
- El software adquirido se mantiene al nivel soportado por el proveedor, salvo que existan dependencias identificadas que requieran una versión anterior.
- Se documentan los cambios y se protege la integridad de los sistemas y de la información contra virus, software maliciosos y no autorizados.
- Se definen procedimientos para aplicar parches de seguridad en plazos razonalbes una vez están disponibles. Se documentan los motivos de no actualizar algún parche de seguridad que generen vulnerabilidades o inestabilidad en los sistemas.

15.10.2 Controles de gestión de seguridad

EADTrust lleva a cabo auditorías internas y externas para comprobar la correcta aplicación de sus políticas. Entre ellas se incluyen:

- Auditoría respecto a la norma ISO 27001;
- Auditorías de tipo “ethical hacking” (Test de penetración);
- Auditorías respecto a la norma eIDAS.
- Auditorías respecto al Esquema Nacional de Seguridad (ENS). la norma eIDAS.

15.10.3 Controles de seguridad del ciclo de vida

Los servicios de EADTrust que impliquen una relación de confianza con los clientes y los usuarios conllevarán la gestión del ciclo de vida de la relación. El ciclo de vida de la expedición de certificados es uno de los que se contemplan en esta relación.

Los controles de seguridad aplicados en el ciclo de vida de los certificados inciden, especialmente, en la solicitud de certificados y en su revocación.

15.11 Seguridad de la red

EADTrust protege sus redes y sus sistemas de potenciales ataques o accesos no autorizados. A estos fines ha segmentado sus sistemas en redes o zonas basándose en una evaluación de riesgos teniendo en cuenta la relación funcional, lógica y física (incluida la ubicación) entre los sistemas y servicios de confianza.

En la red interna de EADTrust existen sistemas de monitorización para registrar incidencias, incluidas las que afectan a la seguridad y para notificar la necesidad de actuación a los operadores.

Los firewalls se revisan cuando sea preciso actualizar las reglas de filtrado. Se llevan a cabo escaneos de vulnerabilidades con peridocidad mínima trimestral y una prueba de intrusión en los sistemas en el momento de la puesta en marcha y después de modificaciones de la infraestructura o las aplicaciones criticas con periodicidad mínima anual. Todas las medidas de seguridad y los controles especificados para el resto de los sistemas se aplican a los dispositivos de red y se recogen en la Política de Seguridad.

Los usuarios sólo pueden acceder a los servicios para los que están autorizados.

15.12 Gestión de incidentes

EADTrust ha creado y mantiene un procedimiento de respuesta a incidentes para una serie de situaciones potenciales de compromiso y desastre. Dichas situaciones incluyen, entre otras, las catástrofes naturales, los incidentes de seguridad, incluidos los relacionados con el tratamiento de datos personales y; los fallos de los equipos. Los planes de respuesta a incidentes se revisan, se actualizan potencialmente y se prueban al menos una vez al año.

La documentación de gestión de incidentes de seguridad ha sido diseñada tomando en consideración las directrices técnicas definidas por la European Union Agency For Network And Information Security ENISA en el documento*; "Article 19 Incident reporting. (Incident reporting framework for eIDAS Article 19)."*[58] Estos se complementan con procedimientos de notificación y comunicación de incidentes de seguridad a terceros interesados.

El personal de confianza designado monitoriza y hace seguimiento de las alertas de eventos de seguridad potencialmente críticos y garantiza que los incidentes pertinentes se notifiquen a los organismos supervisores y a otras partes interesadas, dentro de los plazos mínimos definidos en la legislación vigente.

15.13 Recogida de evidencias

Los registros de auditoría se utilizan para reconstruir los eventos significativos registrados en el software de EADTrust o de la Autoridad de Registro y el usuario o evento que dió origen al registro. Los registros

[58] https://www.enisa.europa.eu/publications/article19-incident-reporting-framework

también se utilizarán en el arbitraje para resolver cualquier posible conflicto comprobando la validez de una firma en un momento dado.

15.13.1 Tipos de eventos registrados

EADTrust registra y guarda los registros de auditoría de todos los eventos relativos al sistema de seguridad de la AC.

Se registrarán los siguientes eventos:

- Encendido y apagado del sistema.
- Intentos de creación, borrado, establecimiento de contraseñas o cambio de privilegios.
- Intentos de inicio y fin de sesión.
- Intentos de accesos no autorizados al sistema de la CA a través de la red.
- Intentos de accesos no autorizados al sistema de archivos.
- Acceso físico a los registros de auditoría.
- Cambios en la configuración y mantenimiento del sistema.
- Registros de las aplicaciones de la CA.
- Encendido y apagado de la aplicación de la CA.
- Cambios en los detalles de la CA y/o sus claves.
- Cambios en la creación de políticas de certificados.
- Generación de claves propias.
- Registros de peticiones de generación y revocación de certificados.
- Registros de generación y revocación de certificados.
- Eventos relacionados con el ciclo de vida del módulo criptográfico, como recepción, preparación, uso y desinstalación de este.
- La hora exacta de los eventos ambientales, de gestión de claves y de sincronización del reloj de EADTrust.

La hora utilizada para registrar los eventos requeridos en el registro de auditoría deberá estar sincronizada con UTC al menos una vez al día.

EADTrust también conserva, mediante un procedimiento no automatizado o electrónico, la siguiente información:

- La ceremonia de generación de claves y las bases de datos de gestión de claves.
- Registros de acceso físico.
- Mantenimientos y cambios de configuración del sistema.
- Informes de incidentes.
- Control de material destinado a gestión de claves y registro de entregas
- Preparación de dispositivos (tokens criptográficos y tarjetas) para entregárselos a los suscriptores.
- Posesión de datos de activación, para operaciones con la clave privada de la Entidad de Certificación.
- Informes completos de los intentos de intrusión física en las infraestructuras que dan soporte a la emisión y gestión de certificados.

15.13.2 Frecuencia de procesamiento del registro

Los registros de auditoría son revisados regularmente por el auditor interno de EADTrust.

15.13.3 Período de retención del registro de auditoría

EADTrust almacena la información de los registros de auditoría al menos durante 10 años.

Los auditores tienen derecho a acceder a los registros de auditoría.

La eliminación o modificación no autorizada de las entradas de registro se evita escribiendo registros de auditoría utilizando medios no aptos para su reescritura o borrado sin detección.

En el caso de la bitácora (en papel) se realizan copias de seguridad periódicas y se usan técnicas de cumplimentación que limitan la posibilidad de manipulación o eliminación de información.

15.13.4 Procedimientos de copia de seguridad para registros de auditoría

Los sistemas de gestión de copias de respaldo están contemplados entre las medidas de seguridad adoptadas por la entidad.

Cuando haya cualquier gestión de CA se hace la copia de respaldo de la situación anterior y además la actuación se registra en la bitácora.

15.13.5 Evaluaciones de vulnerabilidades

El análisis de vulnerabilidades queda cubierto por los procesos de auditoría de EADTrust.

Anualmente se revisan los procesos de gestión de riesgos y vulnerabilidades dentro del marco de revisión de la certificación **UNE-ISO/IEC 27001** que están reflejados en el documento de Análisis de riesgos de EADTrust.

En este documento se especifican los controles implantados para garantizar los objetivos de seguridad requeridos.

Además, se contratan externamente auditorías de “White Hat Ethical Hacking” o “Penetration Testing”.

Trimestralmente se realizan evaluaciones de seguridad semejante a las auditorías anuales con personal interno.

15.13.6 Cambio de clave

No hay previsión específica sobre cambio de claves.

Cada vez que se genera una CA o una Sub CA se lleva a cabo en el marco de una ceremonia de la que se conserva registro y en la que se establecen claves privadas y públicas dejando las públicas recogidas en el certificado asociado a la generación, con los datos que correspondan al tipo de CA.

15.14 Gestión de la continuidad del negocio

15.14.1 Continuidad del servicio de emisión de certificados

EADTrust dispone de un Plan de Contingencias que define las acciones a realizar, recursos a utilizar y personal a emplear en el caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos y los servicios de certificación prestados por la entidad.

- **Compromiso de los recursos informáticos, el software y/o los datos**: EADTrust evaluará la situación, incluyendo su impacto en la integridad y seguridad de la AC, y tomará las medidas oportunas. Las operaciones de la AC pueden quedar suspendidas hasta que se complete la mitigación. Los suscriptores podrán ser notificados si la corrupción o el daño tienen un impacto material en el servicio que se les proporciona.

- **Compromiso de la clave privada de una CA subordinada:**
  - La CA Raíz revocará el certificado de una CA emisora en el caso que la clave privada de esa CA se haya comprometido.
  - En el caso que la CA Raíz deba revocar el certificado de la CA emisora, lo notificará inmediatamente a:
    i. La CA emisora
    ii. Las RAs asociadas a dicha CA
    iii. Los titulares de certificados emitidos por esa CA.
- La CA Raíz, publicará el certificado revocado en la ARL (Lista de Revocación de Autoridades de Certificación).
- Después de resolver los factores que dieron lugar a la revocación, la CA Raíz puede:
  i. Generar un nuevo certificado para la CA subordinada.
  ii. Asegurar que todos los nuevos certificados y CRL emitidos por la CA son firmados utilizando la nueva clave.
  iii. La CA emisora podrá emitir certificados a todas las entidades finales afectadas.

- **Compromiso de la clave de la CA raíz:** se eliminará el certificado de todas las aplicaciones y se distribuirá uno nuevo. Se notificará a las entidades que distribuyan Listas de confianza, como por ejemplo los desarrolladores de navegadores y órganos supervisores que compilen listas TSL. Se suspenderá la operación de la CA hasta que se haya completado el procedimiento de recuperación de desastre y se encuentre funcionando correctamente en el centro principal o alternativo. En la notificación se incluirá al CAB (Conformity Assessment Body).

- **Compromiso de los algoritmos de la CA:** En casos en que los algoritmos o parámetros asociados al algoritmo, utilizados por la CA de EADTrust o por los suscriptores llegue a ser obsoleto para continuar su uso en la prestación del servicio. La CA programará la revocación del certificado y lo comunicará a los suscriptores, partes que confían, el organismo supervisor y cualquier otro tercero interesado. En la notificación se incluirá al CAB (Conformity Assessment Body).

- **Recuperación de claves y gestión de backups:**
    i. El equipo de gestión de claves esta duplicado para permitir una recuperación en caso de incidencia.
    ii. Si se trata de un compromiso de clave o sospecha de compromiso, las claves y los certificados emitidos seran revocados.
    iii. Procedimiento ante notario: El procedimiento de recuperación de clave con información depositada ante notario permite recuperar las claves de gestión con las que se operan las CAs root y subordinadas
    iv. Las claves privadas de de gestión para descifrar las roots en procesos de generación de CA subordinadas.

15.14.2 Continuidad del servicio de sellado de tiempo

El Plan de continuidad de negocio de EADTrust considera desastre, tanto el compromiso de la clave privada de la TSU, como la sospecha de compromiso o pérdida de las citadas claves; tambien la pérdida de calibración de un reloj TSU, lo que puede haber afectado sello de tiempo que se han emitido.

En el caso de un compromiso, o sospecha de compromiso o pérdida de calibración al emitir el sello de tiempo de la TSA, EADTrust relaizará como mínimo las acciones siguientes:

- Pondrá a disposición de todos los suscriptores y partes confiantes una descripción del compromiso de claves, identificando los sellos de tiempo afectados, siempre respetando la privacidad de los datos personales conforme establece la legislación vigente en la materia.
- Suspenderá la emisión de sellos de tiempo en el periodo en que se estén tomando medidas para la recuperación.

15.15 Terminación del TSP y plan de cese

15.15.1 Autoridad de certificación

EADTrust tiene un Plan de Terminación de Servicio de la CA que especifica el procedimiento que se llevará a cabo en caso de que tal evento ocurra. Al respecto EADTrust ha tomado en consideración las directrices técnicas definidas por la European Union Agency for Network and Information Security (ENISA), en particular las siguientes: "*Guidelines on Termination of Qualified Trust Services*"[59].

En correspondencia con lo establecido en el art.9.3.c) de la Ley 6/2020, EADTrust notificará a los suscriptores al menos dos meses antes de la terminación de las operaciones, por cualquier medio que garantice la transmisión y recepción adecuadas, de su intención de cesar su actividad como prestador de

[59] https://www.enisa.europa.eu/publications/tsp-termination

servicios de certificación e informará, en su caso, sobre las características del prestador al que se propone la transferencia de la gestión de los certificados.

También se notificará a los PSC y cualquier entidad con la que EADTrust haya celebrado una relación contractual para la utilización de sus certificados.

La Dirección General de EADTrust es responsable de dicha notificación y determinará el mecanismo más apropiado para hacerlo.

Si EADTrust decide transferir sus operaciones a otro proveedor de servicios de certificación, notificará al Organismo Supervisor y a los suscriptores de sus certificados de los acuerdos de transferencia. En tal caso, EADTrust enviará un documento explicando los términos y condiciones de la transferencia y los términos y condiciones de uso que regirán la relación entre el suscriptor y el nuevo PSC. La notificación se hará por cualquier medio que asegure la transmisión y recepción apropiadas de los mismos por lo menos dos meses antes del cese de sus operaciones.

Los suscriptores expresarán su consentimiento expreso a la transferencia de certificados, aceptando así los términos y condiciones presentados por el nuevo PSC. Si el período de dos meses ha transcurrido sin acuerdo de transferencia o el abonado no ha dado su consentimiento expreso, los certificados serán revocados.

Si ha transcurrido el período de dos meses y no se ha llegado a un acuerdo con otro PSC, todos los certificados serán revocados automáticamente.

Cualquier autorización con una tercera parte con la que EADTrust tenga un contrato de prestación de servicios (identificación, emisión, alojamiento, etc.) se considerará finalizada.

EADTrust comunicará al Organismo de supervision correspondiente en España el cese de su actividad y el destino que vaya a dar a los certificados, especificando en su caso: si los va a transferir, a quién, o si los dejará sin efecto. La notificación a dicho organismo se realizará con al menos dos (2) meses de antelación, en documento firmado manuscrita o electrónicamente. Además, se remitirá a dicho organismo la información relativa a los certificados cuya vigencia haya sido extinguida para que éste se haga cargo de su custodia a los efectos pertinentes.

La última CRL generada contendrá los certificados revocados y no caducados. Siempre que sea posible, se gestionarán las CRLs en el proceso de terminación de manera que no queden certificados vigentes al generar la última CRL.

EADTrust ha contratado un dominio especial para incluir la información necesaria tras el cese. La continuidad del servicio asociado al dominio no depende de la continidad de EADtrust. El dominio es

- https://eadtrust.services/

15.15.2 Autoridad de registro

Después de que una Autoridad de Registro deje de realizar sus operaciones, transferirá a EADTrust los registros relativos a la identificación de solicitantes de certificados y a los registros de auditoría.

Cualquier otra información será cancelada y destruida.

16 Otras cuestiones empresariales y legales

16.1.1 Tarifas

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

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

16.1.2 Tarifas de emisión de certificados

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

16.1.3 Tarifas de consulta OCSP

Los servicios OCSP de EADTrust respecto a sus propios certificados son gratuitos.

Los servicios OCSP de EADTrust respecto a los certificados de otros prestadores están sujetos a un coste de alta, un coste mensual y un coste unitario que se comunicará previa solicitud. Este servicio solamente se presta a empresas.

16.2 Consideraciones de protección de datos de carácter personal

Todos los datos correspondientes a las personas físicas están sujetos a la normativa sobre protección de datos de carácter personal. De conformidad con lo establecido en el Reglamento (UE) 679/2016 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (Texto pertinente a efectos del EEE), también conocido como RGPD.

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

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

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

Los siguientes datos son considerados información privada:

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

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

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

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

16.2.1 Consentimiento para usar datos de carácter personal

EADTrust S.L informa que los datos personales a los que tenga acceso en el marco de la prestación de sus servicios serán incorporados al registro de actividades de tratamiento del que es Responsable. EADTrust fundamenta el tratamiento de datos fundamentalmente en: el interés legitimo 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 EADTrut consulte la nota legal más extensa, incluida en:

- http://eadtrust.rgpd.de/politica-de-privacidad

16.2.2 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.

16.3 Garantías de la CA

Al emitir un Certificado, la CA otorga las siguientes garantías de certificado a los siguientes beneficiarios del certificado:

a. El Suscriptor que es parte del Acuerdo de Suscriptor o los Términos de Uso del Certificado;
b. Todos los proveedores de software de aplicación con los que la CA raíz ha celebrado un contrato para la inclusión de su certificado raíz en un software distribuido por dicho proveedor de software de aplicación; y
c. Todas las partes fiables que confían de manera razonable en un certificado válido.

La CA declara y garantiza a los Beneficiarios del Certificado que, durante el período en que el Certificado es válido, la CA ha cumplido con estos Requisitos y su Política de Certificado y / o Declaración de Prácticas de Certificación en la emisión y gestión del Certificado.

Las garantías del certificado incluyen:

1. **Derecho a usar el nombre de dominio o la dirección IP:** que, en el momento de la emisión, la CA (i) implementó un procedimiento para verificar que el Solicitante tenía derecho a usar o tenía control del Nombre/s Dominio/s y dirección/es IP que figuran en el campo Asunto del certificado y la extensión subjectAltName (o, solo en el caso de los Nombres de Dominio, se delegó tal derecho o control por alguien que tenía tal derecho para usar o controlar); (ii) siguió el procedimiento al emitir el Certificado; y (iii) con precisión describió el procedimiento en la Política de Certificación de CA y / o la Declaración de Práctica de Certificación;

2. **Autorización para el Certificado:** Que, en el momento de la emisión, la CA (i) implementó un procedimiento para verificar que el Sujeto autorizó la emisión del Certificado y que el representante del solicitante está autorizado a solicitar el Certificado en nombre del Sujeto; (ii) siguió el procedimiento al emitir el Certificado; y (iii) describió con precisión el procedimiento en la Política de Certificación de CA y / o la Declaración de Práctica de Certificación;

3. **Exactitud de la información:** que, en el momento de la emisión, la CA (i) implementó un procedimiento para verificar la exactitud de toda la información contenida en el Certificado (con la excepción del atributo subject: organizationalUnitName); (ii) siguió el procedimiento al emitir el Certificado; y (iii) describió con precisión el procedimiento en la Política de certificación de CA y / o la Declaración de práctica de certificación;

4. **Sin información engañosa:** que, al momento de la emisión, la CA (i) implementó un procedimiento para reducir la probabilidad de que la información contenida en el atributo del Certificado subject: organizationalUnitName es engañosa; (ii) siguió el procedimiento cuando emitió el Certificado; y (iii) describió con precisión el procedimiento en la Política de certificación de CA y / o la Declaración de práctica de certificación;

5. **Identidad del solicitante:** que, si el Certificado contiene información de identidad del sujeto, la CA (i) implementó un procedimiento para verificar la identidad del Solicitante de acuerdo con las Secciones 3.2 y 11,2; (ii) siguió el procedimiento al emitir el Certificado; y (iii) describió con precisión el procedimiento en la Política de certificación de CA y / o la Declaración de práctica de certificación;

6. **Acuerdo del suscriptor:** que, si la CA y el suscriptor no están afiliados, el suscriptor y la CA son partes de un acuerdo de suscriptor legalmente válido y exigible que cumple estos requisitos, o, si la CA y el suscriptor son la misma entidad o están afiliados, el representante del solicitante reconoció los Términos de Uso;

7. **Estado:** que la CA mantiene un repositorio de acceso público 24 x 7 con información actual con respecto al estado (válido o revocado) de todos los Certificados no expirados; y

8. **Revocación:** que la CA revocará el Certificado por cualquiera de los motivos especificados en estos Requerimientos.

La entidad a cargo de la Autoridad Root será responsable del desempeño y las garantías de las entidades que puedan gestionar una CA subordinada, respecto al cumplimiento de los requisitos aplicables.

16.4 Garantías del suscriptor

EADTrust exigirá, como parte del Acuerdo del Suscriptor o de los Términos de Uso, que el Solicitante asuma los compromisos y garantías en esta sección. Antes de la emisión de un Certificado, la CA gestionará un paso de verificación respecto a:

1. El acuerdo del solicitante con el Acuerdo del suscriptor con la CA, o
2. El reconocimiento del solicitante de los Términos de uso.

Tanto el Acuerdo de Suscriptor como los Términos de Uso del certificado, serán legalmente exigibles al Solicitante del certificado.

Se podrá usar un Acuerdo separado para cada solicitud de certificado, o bien un Acuerdo único para cubrir múltiples solicitudes de certificados futuras y los Certificados resultantes, siempre que cada Certificado emitido al Solicitante esté claramente cubierto por el Acuerdo de Suscriptor o los Términos de Uso.

El Acuerdo de Suscriptor o los Términos de Uso contendrán disposiciones que impongan al Solicitante mismo (o su principal) las siguientes obligaciones y garantías:

1. **Exactitud de la información**: Obligación y garantía de proporcionar información precisa y completa en todo momento a la CA, tanto en la solicitud del certificado como en cualquier otra forma solicitada por la CA en relación con la emisión del Certificado/s a ser suministrado por la CA;
2. **Protección de la clave privada:** Obligación y garantía del solicitante de tomar todas las medidas razonables para garantizar el control, la confidencialidad y la protección adecuada en todo momento de la clave privada que corresponde a la clave pública que se incluirá en el/los certificados/s solicitado/s (y cualquier dispositivo o datos de activación asociados, por ejemplo, contraseña o token)
3. **Aceptación del Certificado:** Obligación y garantía de que el Suscriptor revisará y verificará la exactitud del contenido del Certificado;
4. **Uso del Certificado:** Obligación de usar el Certificado únicamente a las leyes aplicables y únicamente de acuerdo con el Acuerdo de Suscriptor o los Términos de Uso;
5. **Informes y revocación:** Obligación y garantía de: (a) solicitar de inmediato la revocación del Certificado y dejar de usarlo, así como su Clave privada asociada, si existe un uso indebido real o sospechado, o compromiso de la Clave privada del suscriptor asociada con la Clave pública incluida en el Certificado, y (b) solicitar de inmediato la revocación del Certificado y dejar de usarla, si hay información en el Certificado que es o se vuelve incorrecta o inexacta.
6. **Finalización del uso del certificado:** Obligación y garantía de suspender de inmediato el uso de la clave privada correspondiente a la clave pública incluida en el certificado tras la revocación de dicho certificado por razones de compromiso de la clave.
7. **Capacidad de respuesta:** Obligación de responder a las instrucciones de la CA con respecto al Compromiso de la clave o al uso indebido del Certificado dentro de un período de tiempo específico.

8. **Reconocimiento y aceptación:** Un reconocimiento y aceptación de que la CA tiene derecho a revocar el certificado de inmediato si el Solicitante viola los términos del Acuerdo de Suscriptor o los Términos de Uso o si la CA descubre que el Certificado se está utilizando para permitir actividades delictivas, como ataques de phishing, fraude o distribución de malware.

16.5 Responsabilidad contractual y extracontractual

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

16.5.1 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 DPC 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 DPC y en la normativa de aplicación.

16.5.2 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 DPC.

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 EADrust, 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 electrónicos.

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.

16.5.3 Autoridad 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.

16.5.4 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 esta 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.

16.6 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 DPC.
- Ocasionado por el uso indebido o fraudulento de los certificados o CRLs emitidos por la infraestructura de Certificación de EADTrut.
- Ocasionados por el mal uso de la información contenida en el certificado.
- La Autoridad de Certificación no será responsable del contenido de aquellos documentos firmados electrónicamente ni de cualquier otra información que se utilice en un proceso de autenticación en la que esté involucrado un certificado emitido por ella.

16.6.1 Perjuicios derivados del uso de servicios y certificados

A excepción de lo establecido por las disposiciones de la presente DPC, 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.

16.6.2 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.

16.7 Enmiendas y cambios

16.7.1 Procedimiento para realizar cambios

Las modificaciones de este documento serán aprobadas por el órgano de aprobación y gestión de políticas de certificación de EADTrust.

Estas modificaciones estarán recogidas en un documento de actualización de la Declaración de Prácticas de Servicios Electrónicos de Confianza cuyo mantenimiento está garantizado por EADTrust.

Las versiones actualizadas de la Declaración de Prácticas de Servicios Electronicos de Confianza junto con la relación de modificaciones realizadas pueden ser consultadas en la dirección www.eadtrust.eu y más concretamente en www.policy.eadtrust.eu

EADTrustpodrá modificar la Declaración de Prácticas de Servicios Electrónicos de Confianza para lo que actuará según el siguiente procedimiento:

- La modificación estará justificada desde el punto de vista técnico, legal o comercial.
- Se deberán contemplar todas las implicaciones técnicas y legales de la nueva versión de especificaciones.
- Se establecerá un control de modificaciones, para garantizar, que las especificaciones resultantes cumplen con los requisitos que se intentaban cumplir y que dieron pie al cambio.
- Se valorarán las implicaciones que puedan tener sobre los usuarios el cambio de especificaciones, por si fuera preciso comunicarles el cambio.

16.7.2 Mecanismo y período de modificación

En la fase preparatoria de las auditorías bienales, EADTrust revisará el presente documento para asegurarse de que permanece actualizado en relación con los cambios que se vayan produciendo en los siguientes aspectos:

- Marco legislativo de aplicación.
- Pautas de funcionamiento de Servicios Electrónicos de Confianza publicadas por el Órganismo Nacional de Supervisión
- Publicacion de estándares.
- Mejoras o no conformidades identificadas en las auditorías.
- Mejoras realizadas en los servicios o lanzamiento de nuevos servicios.
- Adopción de productos y servicios de terceros que se itegren con los ofrecidos por EADTrust.

EADTrust podrá realizar modificaciones de este documento sin necesidad de informar previamente a los usuarios, como, por ejemplo:

- Correcciones de errores tipográficos en el documento
- Cambios en la información de contacto.

EADTrust podrá realizar modificaciones de este documento de las que se informará a los usuarios por email, tales como:

- Cambios en las especificaciones o condiciones del servicio.
- Modificaciones de URLs.

16.8 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, autoridadregistro@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.

17 ANEXOS

17.1 Perfiles de certificado

Los certificados emitidos por EADTrust cumplen con las siguientes normas:

- RFC 5280: Certificado de Infraestructura de Clave Pública X.509 de Internet y Perfil de CRL -abril de 2002.
- RFC 4325: Extensión de la lista de revocación de certificados de acceso a la información de la autoridad de infraestructura de claves públicas X.509 de Internet - diciembre de 2005.
- RFC 4630: Actualización del procesamiento de DirectoryString en el perfil de la lista de revocación de certificados y certificados de la infraestructura de la clave pública X.509 de Internet - agosto de 2006.
- RFC 6066 - Online Certificate Status Protocol Stapling. Transport Layer Security (TLS) Extensions: Extension Definitions
- UIT-T. Recomendación X.509 (2005): Tecnología de la información - Interconexión de sistemas abiertos - El Directorio: Marco de autenticación.
- Perfil de Certificado Cualificado ETSI TS 319 412 (documentos 1 a 5).
- RFC 3739: Internet X.509 Infraestructura de clave pública - Perfil de Certificado Cualificado.
- Perfil de certificado de las administraciones públicas españolas.[60]
- Perfil de Certificado con Seudónimo Justicia del CTEAJE.[61]

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

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

[61] https://www.administraciondejusticia.gob.es/documents/7557301/7558179/CTEAJE-Perfil+Certificado+Seudonimo+Justicia_v1.0.pdf

- ITU-T Recommendation X.509 (1997): Information Technology – Open Systems Interconnection - The Directory: Authentication Framework, June 1997, con sus actualizaciones y correcciones posteriores.

Adicionalmente, los certificados cualificados de firma electrónica serán conformes con las siguientes normas:

- ETSI EN 319 412-1 V1.1.1 (2016-02) - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.
- ETSI EN 319 412-2 V2.1.1 (2016-02) - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.
- ETSI EN 319 412-3 V1.1.1 (2016-02) - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons.
- ETSI EN 319 412-4 V1.1.1 (2016-02) - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates.
- ETSI EN 319 412-5 V2.2.1 (2017-11) - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.
- RFC 3739 : Internet X.509 Public Key Infrastructure – Qualified Certificate Profile, March 2004 (siempre que no entre en conflicto con las normas ETSI EN 319 412).

17.2 Número de versión

Los certificados emitidos bajo esta Declaración de Prácticas de Certificación emplean el estándar X509, versión 3.

17.3 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.

17.4 Perfiles de Root y SubCA

17.4.1 Perfil de certificado de root CA para emisión de certificados cualificados

Campo	Crítico	Contenido
version		3
serialNumber		Número positivo único
signature		Sha256WithRSAEncryption o sha512WithRSAEncryption o ecdsa-with-SHA256 o ecdsa-with-SHA384
issuer		Igual que el campo Subject
validity		32 años
subject		
Country		País (ISO 3166-1 alpha 2 code)
Organization Identifier		<Código de 3 letras><Código de país de 2 letras>-<CIF organización>
Organization Name		Nombre completo de la organización
Common Name		Nombre de la CA
subjectPublicKeyInfo		RSA 2048, 4096 ó 8192 bits ECDSA 256 bits (prime256v1) ó 384 bits (secpr384r1)
Extensiones		
subjectKeyIdentifier		Derivada del resultado de aplicar el hash a la clave pública del sujeto
subjectAltName		rfc822 Name ca@eadtrust.eu URI: http://www.eadtrust.eu URI: http://ca.eadtrust.eu URI: http://policy.eadtrust.eu
basicConstraint	**Crítica**	CA:true
keyUsage	**Crítica**	Certificate signing, CRL signing

Existen cinco (5) certificados que se ajustan a este perfil, diferenciándose en el tamaño del algoritmo de HASH y la clave:

- RSA 2048 y SHA 256
- RSA 4096 y SHA 256
- RSA 8192 y SHA 512
- ECC 256 y SHA 256
- ECC 384 y SHA 384

17.4.2 Perfil de certificado de root CA para emisión de certificados web y PSD2

Campo	Crítico	Contenido
version		3
serialNumber		Número positivo único
signature		Sha256WithRSAEncryption o sha512WithRSAEncryption o ecdsa-with-SHA256 o ecdsa-with-SHA384
issuer		Igual que el campo Subject
validity		24 años
subject		
Country		País (ISO 3166-1 alpha 2 code)
Organization Name		Nombre completo de la organización
Common Name		Nombre de la CA
subjectPublicKeyInfo		RSA 4096 ó 8192 bits ECDSA 256 bits (prime256v1) ó 384 bits (secpr384r1)
Extensiones		
subjectKeyIdentifier		Derivada del resultado de aplicar el hash a la clave pública del sujeto
basicConstraint	**Crítica**	CA: true
keyUsage	**Crítica**	Certificate signing, CRL signing

Existen ocho (8) certificados que se ajustan a este perfil (QWAC), diferenciándose en el tamaño del algoritmo de HASH, de la clave y del tipo de validación definida por CA/B fórum:

- RSA 4096 y SHA 256 (Extended validation PSD2)
- RSA 4096 y SHA 256 (Domain validation y Organization validation)
- RSA 8192 y SHA 512 (Extended validation y PSD2)
- RSA 8192 y SHA 512 (Domain validation y Organization validation)
- ECC 256 y SHA 256 (Extended validation y PSD2)
- ECC 256 y SHA 256 (Domain validation y Organization validation)
- ECC 384 y SHA 384 (Extended validation y PSD2)
- ECC 384 y SHA 384 (Domain validation y Organization validation)

17.4.3 Perfil de certificado de root CA para emisión de certificados no cualificados

Campo	Crítico	Contenido
version		3
serialNumber		Número positivo único
signature		Sha256WithRSAEncryption
issuer		Igual que el campo Subject
validity		32 años
subject		
Country		País (ISO 3166-1 alpha 2 code)
Organization Identifier		<Código de 3 letras><Código de país de 2 letras>-<CIF organización>
Organization Name		Nombre completo de la organización
Common Name		Nombre de la CA
subjectPublicKeyInfo		RSA 2048 bits
Extensiones		
subjectKeyIdentifier		Derivada del resultado de aplicar el hash a la clave pública del sujeto
subjectAltName		rfc822 Name ca@eadtrust.eu URI: http://www.eadtrust.eu URI: http://ca.eadtrust.eu URI: http://policy.eadtrust.eu
basicConstraint	**Crítica**	CA:true
keyUsage	**Crítica**	Certificate signing, CRL signing

Existe un (1) certificado que se ajusta a este perfil:

- RSA 2048 y SHA 256

17.4.4 Perfil de certificado de subCA para emisión de certificados cualificados

Campo	Crítico	Contenido
version		3
serialNumber		Número positivo único
signature		Sha256WithRSAEncryption o sha512WithRSAEncryption o ecdsa-with-SHA256 o ecdsa-with-SHA384
issuer		Igual al campo Subject del certificado de la CA emisora
validity		16 años
subject		
Country		País (ISO 3166-1 alpha 2 code)
Organization Identifier		<Código de 3 letras><Código de país de 2 letras>-<CIF organización>
Organization Name		Nombre completo de la organización
Common Name		Nombre de la SubCA
Organizational Unit		Tipo de SubCA (Legal Person o Natural Person)
subjectPublicKeyInfo		RSA 2048, 4096 ó 8192 bits ECDSA 256 bits (prime256v1) ó 384 bits (secpr384r1)
Extensiones		
authorityKeyIdentifier		Derivada del resultado de aplicar el hash a la Clave pública de la AC emisora
basicConstraints	**Crítica**	CA=true, pathlen=0
subjectKeyIdentifier		Derivada del resultado de aplicar el hash a la clave pública del sujeto
issuerAltName		Igual al campo Subject Alternative Names de la CA Emisora
subjectAltName		rfc822 Name ca@eadtrust.eu URI: http://www.eadtrust.eu URI: http://ca.eadtrust.eu URI: http://policy.eadtrust.eu
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.1.401
cpsURI		http://policy.eadtrust.eu/
userNotice		Subordinate Certificate Authority. European Agency of Digital Trust, S.L.
policyIdentifier		2.5.29.32.0 (AnyPolicy)
cRLDistributionPoints		
distributionPoint		http://crl.eadtrust.eu/eadtrust-root-<algoritmo><longitud clave>eadq<año>.crl
authorityInfoAccess		
calssuers		http://ca.eadtrust.eu/eadtrust-root-<algoritmo><longitud clave>eadq<año>.crt
ocsp		http://ocsp.eadtrust.eu
keyUsage	**Crítica**	Digital Signature, Certificate signing, CRL signing

Existen once (11 certificados que se ajustan a este perfil, dos (2) por cada una de las cinco (5) CAs de tipo cualificado no web, diferenciándose en el tipo de certificado de entidad final: persona física y persona jurídica.

- RSA 2048 y SHA 256 (persona física)
- RSA 2048 y SHA 256 (persona jurídica)
- RSA 4096 y SHA 256 (persona física)
- RSA 4096 y SHA 256 (persona jurídica que incluye los certificados de sello de órgano)
- RSA 8192 y SHA 512 (persona física)
- RSA 8192 y SHA 512 (persona jurídica)
- ECC 256 y SHA 256 (persona física)
- ECC 256 y SHA 256 (persona jurídica)
- ECC 384 y SHA 384 (persona física)
- ECC 384 y SHA 384 (persona jurídica)

17.4.5 Perfil de certificado de subCA para emisión de certificados web y PSD2

Campo	Crítico	Contenido
version		3
serialNumber		Número positivo único
signature		Sha256WithRSAEncryption o sha512WithRSAEncryption o ecdsa-with-SHA256 o ecdsa-with-SHA384
issuer		Igual al campo Subject del certificado de la CA emisora
validity		12 años
subject		
Country		País (ISO 3166-1 alpha 2 code)
Organization Name		Nombre completo de la organización
Common Name		Nombre de la SubCA
subjectPublicKeyInfo		RSA 4096 ó 8192 bits ECDSA 256 bits (prime256v1) ó 384 bits (secpr384r1)
Extensiones		
authorityKeyIdentifier		Derivada del resultado de aplicar el hash a la Clave pública de la AC emisora
basicConstraints	**Crítica**	CA=true, pathlen=0
subjectKeyIdentifier		Derivada del resultado de aplicar el hash a la clave pública del sujeto
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.1.401
cpsURI		http://policy.eadtrust.eu/
policyIdentifier		2.5.29.32.0 (AnyPolicy)
cRLDistributionPoints		
distributionPoint		http://crl.eadtrust.eu/eadtrust-root-<algoritmo><longitud clave>ead<evpsd2 ó dvov><año>.crl
authorityInfoAccess		
calssuers		http://ca.eadtrust.eu/eadtrust-root-<algoritmo><longitud clave>ead<evpsd2 ó dvov><año>.crt
ocsp		http://ocsp.eadtrust.eu
keyUsage	**Crítica**	Digital Signature, Certificate signing, CRL signing
extendedKeyUsage		TSL Web Server Authentication, TSL Web Client Authentication

Existen diez (10) certificados que se ajustan a este perfil (QWAC), diferenciándose en el tamaño del SHA, de la clave y del tipo de validación definida por CA/B fórum:

- RSA 4096 y SHA 256 (Extended validation que incluye los certificados de sede electrónica de nivel alto y PSD2)
- RSA 4096 y SHA 256 (Domain validation y Organization validation, que incluye los certificados de sede electrónica de nivel medo/sustancial)
- RSA 8192 y SHA 512 (Extended validation y PSD2)
- RSA 8192 y SHA 512 (Domain validation y Organization validation)
- ECC 256 y SHA 256 (Extended validation y PSD2)

- ECC 256 y SHA 256 (Domain validation y Organization validation)
- ECC 384 y SHA 384 (Extended validation y PSD2)
- ECC 384 y SHA 384 (Domain validation y Organization validation)

17.4.6 Perfil de certificado de subCA para emisión de certificados no cualificados

Campo	Crítico	Contenido
version		3
serialNumber		Número positivo único
signature		Sha256WithRSAEncryption
issuer		Igual al campo Subject del certificado de la CA emisora
validity		16 años
subject		
Country		País (ISO 3166-1 alpha 2 code)
Organization Identifier		<Código de 3 letras><Código de país de 2 letras>-<CIF organización>
Organization Name		Nombre completo de la organización
Common Name		Nombre de la SubCA
subjectPublicKeyInfo		RSA 2048 bits
Extensiones		
authorityKeyIdentifier		Derivada del resultado de aplicar el hash a la Clave pública de la AC emisora
basicConstraints	**Crítica**	CA=true, pathlen=0
subjectKeyIdentifier		Derivada del resultado de aplicar el hash a la clave pública del sujeto
issuerAltName		Igual al campo Subject Alternative Names de la CA Emisora
subjectAltName		rfc822 Name ca@eadtrust.eu URI: http://www.eadtrust.eu URI: http://ca.eadtrust.eu URI: http://policy.eadtrust.eu
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.1.3161
cpsURI		http://policy.eadtrust.eu/
userNotice		Subordinate Certificate Authority. European Agency of Digital Trust, S.L.
policyIdentifier		2.5.29.32.0 (AnyPolicy)
cRLDistributionPoints		
distributionPoint		http://crl.eadtrust.eu/eadtrust-root-<algoritmo><longitud clave>eadnq<año>.crl
authorityInfoAccess		
calssuers		http://ca.eadtrust.eu/eadtrust-root-<algoritmo><longitud clave>eadnq<año>.crt
ocsp		http://ocsp.eadtrust.eu
keyUsage	**Crítica**	Digital Signature, Certificate signing, CRL signing

Existe un (1) certificado que se ajusta a este perfil:

- RSA 2048 y SHA 256

Los certificados no cualificados se utilizan en una variante de sello de tiempo cualificado.

17.5 Perfiles de certificados de Entidad Final

17.5.1 Perfil de certificado cualificado de persona jurídica para sello de tiempo cualificado

Campo	Crítico	Contenido
Versión		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		
CommonName		Nombre común
organizationIdentifier		<3 caracteres de tipo de identidad><país>- <identificador>. Ejemplo: VATES-B12312312
Organization		Nombre registrado completo
Country		País
OrganizationalUnit		Certificado de Sello de Tiempo
subjectPublicKeyInfo		RSA mínimo 2048 bits, ECDSA 256 bits (prime256v1) ó 384 bits (secpr384r1)
Extensiones		
issuerAltName		Igual al campo Subject Alternative Name de la CA Emisora
subjectAltName		email:ca@eadtrust.eu URI:http://www.eadtrust.eu URI:http://ca.eadtrust.eu URI:http://policy.eadtrust.eu
extendedKeyUsage		timeStamping
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
privateKeyUsagePeriod		Indica la fecha y la hora más tempranas en las que la clave privada podría usarse para firmar. notBefore / notAfter
certificatePolicies*		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.0.421
cpsURI		http://policy.eadtrust.eu
userNotice		European Agency of Digital Trust, S.L. Legal Person Qualified Certificate for Qualified TimeStamping
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		

Campo	Crítico	Contenido
caIssuers		http://ca.eadtrust.eu/ eadtrust-subca-<algoritmo><tamañoclave>eadlp<Año>.crt
ocsp		http://ocsp.eadtrust.eu
qcStatements **		
QcCompliance		Presente
QcType		id-etsi-qct-eseal
qcStatement-2		0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)
QcRetentionPeriod		15 años
keyUsage	**Crítica**	digitalSignature

* En caso de que la clave privada del certificado se encuentre en un **dispositivo cualificado de creación de sello** se cambia el OID 1.3.6.1.4.1.501.2.1.1.0.421 por 1.3.6.1.4.1.501.2.1.1.1.421 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 jerarquias cualificadas de personas jurídicas y admite diferentes variantes.

17.5.2 Perfil de certificado no cualificado de persona jurídica para sello de tiempo cualificado y no cualificado

Campo	Crítico	Contenido
Versión		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		
CommonName		Nombre común
organizationIdentifier		<3 caracteres de tipo de identidad><país>- <identificador>. Ejemplo: VATES-B12312312
Organization		Nombre registrado completo
Country		País
OrganizationalUnit		Certificado de Sello de Tiempo
subjectPublicKeyInfo		RSA mínimo 2048 bits ECDSA 256 bits (prime256v1) ó 384 bits (secpr384r1)
Extensiones		
issuerAltName		Igual al campo Subject Alternative Names de la CA Emisora
subjectAltName		email:ca@eadtrust.eu URI:http://www.eadtrust.eu

Campo	Crítico	Contenido
		URI:http://ca.eadtrust.eu URI:http://policy.eadtrust.eu
extendedKeyUsage		timeStamping
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		1.3.6.1.4.1.501.2.1.1.0.3161
cpsURI		http://policy.eadtrust.eu
userNotice		European Agency of Digital Trust, S.L.
cRLDistributionPoints		http://crl.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadnq<Año>.crl
authorityInfoAccess		
caIssuers		http://ca.eadtrust.eu/ eadtrust-subca-<algoritmo><tamañoclave>eadnq<Año>.crt
ocsp		http://ocsp.eadtrust.eu
keyUsage	**Crítica**	digitalSignature

Este tipo de certificados se expiden bajo la jerarquía no cualificada y admite diferentes variantes en función de la clave y el algoritmo de cifrado.

17.5.3 Perfil de certificado cualificado de persona física

Campo	Crítico	Contenido
version		3
serialNumber		Número positivo único
signature		Sha256WithRSAEncryption o ecdsa-with-SHA256 o ecdsa-with-SHA384
issuer		Igual al campo Subject del certificado de la CA emisora
validity		4 años
subject		
Country		País (ISO 3166-1 alpha 2 code)
Common Name		Nombre y Apellidos
Given Name		Nombre
Surname		Apellidos
serial number		<3 caracteres de tipo de identidad><país>- <identificador>. Ejemplo: IDCES-012345678R
Organizational Unit		Certificado de persona física
Organizational Unit	Opcional	Cuando está presente, indica la entidad jurídica a la que pertenece tal como figura en los registros oficiales.
subjectPublicKeyInfo		RSA mínimo 2048 bits ECDSA 256 bits (prime256v1) ó 384 bits (secpr384r1)
Extensiones		

authorityKeyIdentifier		Derivada del resultado de aplicar el hash a la Clave pública de la AC emisora
subjectKeyIdentifier		Derivada del resultado de aplicar el hash a la clave pública del sujeto
issuerAltName		Igual al campo Subject Alternative Names de la CA Emisora
subjectAltName		rfc822 Name Correo electrónico del titular opcional DirectoryName 1.3.6.1.4.1.501.1.1 Nombre 1.3.6.1.4.1.501.1.2 Primer Apellido 1.3.6.1.4.1.501.1.3 Segundo Apellido 1.3.6.1.4.1.501.1.4 DNI/NIE/NIF/ PASS
certificatePolicies*		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.0.41221
cpsURI		http://policy.eadtrust.eu/cps
userNotice		European Agency of Digital Trust, S.L. Natural Person Qualified Certificate
policyIdentifier		0.4.0.194112.1.0 (QCP-n)
policyIdentifier	**Opcional**	1.3.6.1.4.1.501.2.1.0.3
qcStatements**		
QcCompliance		Presente
QcType		id-etsi-qct-esign
QcRetentionPeriod		15 años
qcStatement-2		0.4.0.194121.1.1 (id-etsi-qcs-SemanticsId-Natural)
cRLDistributionPoints		
distributionPoint		http://crl.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadnp<Año>.crl
authorityInfoAccess		
caIssuers		http://ca.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadnp<Año>.crt
ocsp		http://ocsp.eadtrust.eu
extendedKeyUsage		clientAuth, emailProtection
keyUsage	**Crítica**	digitalSignature, nonRepudiation, keyEncipherment

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

Para el caso de que la identificación del sujeto se haga de manera remota los OIDs cuando la clave privada del certificado se encuentre en un dispositivo cualificado de creación de firma serán 1.3.6.1.4.1.501.2.1.1.4.41221 y 0.4.0.194112.1.2 y en caso contrario 1.3.6.1.4.1.501.2.1.1.3.41221 y OID 0.4.0.194112.1.0 respectivamente.

Cuando esté presente el OID de política 1.3.6.1.4.1.501.2.1.0.3, indica que el certificado se usará para sistemas de firma remota (firma on-behalf).

Los certificados de persona física "perteneciente a empresa" indican la denominación de la empresa en el campo OU (Organizational Unit) mientras que los de persona física "representante de empresa indican la denominación de la empresa en el campo O (OrganizationName).

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

Este tipo de certificados se expiden bajo las jerarquías cualificadas de personas físicas y admite diferentes variantes.

17.5.4 Perfil de certificado cualificado de representante de persona jurídica

Campo	Crítico	Contenido
version		3
serialNumber		Número positivo único
signature		Sha256WithRSAEncryption o ecdsa-with-SHA256 o ecdsa-with-SHA384
issuer		Igual al campo Subject del certificado de la CA emisora
validity		4 años
subject		
Country		País (ISO 3166-1 alpha 2 code)
Common Name		NIF, nombre y primer apellido del representante y (R: NIF de la Entidad representada)
Given Name		Nombre
Surname		Apellidos
serial number		DNI / NIE
organizationName		Razón Social, tal como figura en los registros oficiales.
organizationIdentifier		3 caracteres tipo -identidad + Country + - + identificador. Ejemplo VATES-B1234567
description		Codificación del documento público que acredita las facultades del firmante o los datos registrales
subjectPublicKeyInfo		RSA mínimo 2048 bits ó ECDSA 256 bits (prime256v1) ó 384 bits (secpr384r1)
Extensiones		
authorityKeyIdentifier		Derivada del resultado de aplicar el hash a la Clave pública de la AC emisora
subjectKeyIdentifier		Derivada del resultado de aplicar el hash a la clave pública del sujeto
issuerAltName		Igual al campo Subject Alternative Names de la CA Emisora
subjectAltName		rfc822 Name Correo electrónico del titular DirectoryName 1.3.6.1.4.1.501.1.1 Nombre del representante 1.3.6.1.4.1.501.1.2 Primer Apellido del representante 1.3.6.1.4.1.501.1.3 Segundo Apellido del representante 1.3.6.1.4.1.501.1.4 NIF del Representante 1.3.6.1.4.1.501.1.6 Razón Social de la Entidad 1.3.6.1.4.1.501.1.7 NIF de la Entidad Representada
certificatePolicies*		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.0.41222
cpsURI		http://policy.eadtrust.eu/cps
userNotice		European Agency of Digital Trust, S.L. Power of Attorney Qualified Certificate
policyIdentifier		0.4.0.194112.1.0 (QCP-n)

Campo	Crítico	Contenido
PolicyIdentifier		2.16.724.1.3.5.8 (OID MPR)
policyIdentifier	**Opcional**	1.3.6.1.4.1.501.2.1.0.3
qcStatements**		
QcCompliance		Presente
QcType		id-etsi-qct-esign
QcRetentionPeriod		15 años
qcStatement-2		0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)
cRLDistributionPoints		
distributionPoint		http://crl.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadnp<Año>.crl
authorityInfoAccess		
calssuers		http://ca.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadnp<Año>.crt
ocsp		http://ocsp.eadtrust.eu
extendedKeyUsage		clientAuth, emailProtection
keyUsage	**Crítica**	digitalSignature, nonRepudiation, keyEncipherment

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

Para el caso de que la identificación del sujeto se haga de manera remota los OIDs cuando la clave privada del certificado se encuentre en un dispositivo cualificado de creación de firma serían 1.3.6.1.4.1.501.2.1.1.4.41222 y 0.4.0.194112.1.2 y en caso contrario 1.3.6.1.4.1.501.2.1.1.3.41222 y OID 0.4.0.194112.1.0 respectivamente.

Cuando esté presente el OID de política 1.3.6.1.4.1.501.2.1.0.3, indica que el certificado se usará para sistemas de firma remota (firma on-behalf).

Los certificados de persona física "perteneciente a empresa" indican la denominación de la empresa en el campo OU (Organizational Unit) mientras que los de persona física "representante de empresa indican la denominación de la empresa en el campo O (OrganizationName).
** En caso de que la clave privada del certificado se encuentre en un **dispositivo cualificado de creación de firma** se añade el campo QSCD

Este tipo de certificados se expiden bajo las jerarquías cualificadas de personas físicas y admite diferentes variantes.

17.5.5 Perfil de certificado cualificado de web "domain validated" (QWAC)

Campos/Extensiones	Crítico	Contenido
Versión		3
serialNumber		Unique non-sequential positive number of minimum length 64 bits
Signature		Sha256WithRSAEncryption or Sha512WithRSAEncryption or ecdsa-with-SHA256 or

Campos/Extensiones	Crítico	Contenido
		ecdsa-with-SHA384
Issuer		Same as the Subject field of the issuing CA certificate
Validity		379 days
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		1.3.6.1.4.1.501.2.1.1.0.41241
cpsURI		http://policy.eadtrust.eu
policyIdentifier		0.4.0.194112.1.5 (ETSI QNCP-w)
policyIdentifier		2.23.140.1.2.1 (CAB/FORUM DV)
cRLDistributionPoints		http://crl.eadtrust.eu/eadtrust-subca-<algorithm><keylength>eaddvov<year>.crl
authorityInfoAccess		
caIssuers		http://ca.eadtrust.eu/eadtrust-subca-<algorithm><keylength>eaddvov<year>.crt
Ocsp		http://ocsp.eadtrust.eu
basicConstraint	Crítica	CA false
qcStatements		
QcRetentionPeriod		15 years
QcCompliance		Present
QcType		id-etsi-qct-web
keyUsage	Crítica	digitalSignature
CT RFC6962		Certificate Transparency

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

17.5.6 Perfil de certificado cualificado de web "organization validated" (QWAC)

Campos/Extensiones	Crítico	Contenido
version		3
serialNumber		Unique non-sequential positive number of minimum length 64 bits
signature		Sha256WithRSAEncryption or Sha512WithRSAEncryption or ecdsa-with-SHA256 or ecdsa-with-SHA384

Campos/Extensiones	Crítico	Contenido
issuer		Same as the Subject field of the issuing CA certificate
validity		379 days
subject		
OrganizationName		Organization Name
LocalityName		Locality Name
StateOrProvinceName		State or province name
CountryName		CountryName
subjectPublicKeyInfo		RSA 2048 bits minimum or ECDSA 256 bits (prime256v1) or 384 bits (secpr384r1)
Extensions		
subjectAltName		
dnsName		DNS name(s)
extendedKeyUsage		serverAuth, clientAuth
subjectKeyIdentifier		Derived from the result of applying the hash to the public key of the subject
authorityKeyIdentifier		Derived from the result of applying the hash to the Public key of the issuing CA
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.0.41242
cpsURI		http://policy.eadtrust.eu
policyIdentifier		0.4.0.194112.1.5 (ETSI QNCP-w)
policyIdentifier		2.23.140.1.2.2 (CAB/FORUM OV)
cRLDistributionPoints		http://crl.eadtrust.eu/eadtrust-subca-<algorithm><keylength>eaddvov<year>.crl
authorityInfoAccess		
caIssuers		http://ca.eadtrust.eu/eadtrust-subca-<algorithm><keylength>eaddvov<year>.crt
ocsp		http://ocsp.eadtrust.eu
basicConstraint	Crítica	CA false
qcStatements		
QcRetentionPeriod		15 years
QcCompliance		Present
QcType		id-etsi-qct-web
keyUsage	Crítica	digitalSignature
CT RFC6962		Certificate Transparency

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

17.5.7 Perfil de certificado cualificado de web “Extended Validation” (QWAC)

Campos/Extensiones	Crítico	Contenido
version		3
serialNumber		Unique non-sequential positive number of minimum length 64 bits
signature		Sha256WithRSAEncryption or Sha512WithRSAEncryption or ecdsa-with-SHA256 or ecdsa-with-SHA384
issuer		Same as the Subject field of the issuing CA certificate
validity		379 days
subject		
businessCategory		Private Organization, Government Entity, Business Entity or Non-Commercial Entity
jurisdictionCountryName		Country of Jurisdiction of Incorporation or Registration Field
jurisdictionStOrProvName		State or Province of Jurisdiction of Incorporation or Registration Field
jurisdictionLocalityName		Locality of Jurisdiction of Incorporation or Registration Field
OrganizationName		Organization Name
LocalityName		Locality Name
StateOrProvinceName		State or province name
CountryName		CountryName
OrganizationIdentifier		ETSI EN 319 412-1 and CA/B Forum format
serialNumber		Registration Number
subjectPublicKeyInfo		RSA 2048 bits minimum or ECDSA 256 bits (prime256v1) or 384 bits (secpr384r1)
Extensions		
subjectAltName		
dnsName		DNS name(s)
extendedKeyUsage		serverAuth, clientAuth
subjectKeyIdentifier		Derived from the result of applying the hash to the public key of the subject
authorityKeyIdentifier		Derived from the result of applying the hash to the Public key of the issuing CA
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.0.41244
cpsURI		http://policy.eadtrust.eu
policyIdentifier		0.4.0.194112.1.4 (ETSI QEVCP-w)
policyIdentifier		2.23.140.1.1 (CAB/FORUM EV)
cRLDistributionPoints		http://crl.eadtrust.eu/eadtrust-subca- <algorithm><keylength>eadevpsd2<year>.crl
authorityInfoAccess		
caIssuers		http://ca.eadtrust.eu/eadtrust-subca- <algorithm><keylength>eadevpsd2<year>.crt
ocsp		http://ocsp.eadtrust.eu
basicConstraint	Crítica	CA false
qcStatements		
QcCompliance		Present
QcType		id-etsi-qct-web

Campos/Extensiones	Crítico	Contenido
qcStatement-2		0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)
QcRetentiodPeriod		15
keyUsage	Crítica	digitalSignature
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.

17.5.8 Perfil de certificado no cualificado de web "domain validated"

Campos/Extensiones	Crítico	Contenido
Versión		3
serialNumber		Unique non-sequential positive number of minimum length 64 bits
Signature		Sha256WithRSAEncryption or Sha512WithRSAEncryption or ecdsa-with-SHA256 or ecdsa-with-SHA384
Issuer		Same as the Subject field of the issuing CA certificate
Validity		379 days
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		1.3.6.1.4.1.501.2.1.1.0.41247
cpsURI		http://policy.eadtrust.eu
policyIdentifier		0.4.0.2042.1.6 (ETSI DVCP)
policyIdentifier		2.23.140.1.2.1 (CAB/FORUM DV)
cRLDistributionPoints		http://crl.eadtrust.eu/eadtrust-subca-<algorithm><keylength>eaddvov<Año>.crl
authorityInfoAccess		
calssuers		http://ca.eadtrust.eu/eadtrust-subca-<algorithm><keylength>eaddvov<year>.crt
Ocsp		http://ocsp.eadtrust.eu
basicConstraint	Crítica	CA false
keyUsage	Crítica	digitalSignature
CT RFC6962		Certificate Transparency

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

17.5.9 Perfil de certificado no cualificado de web "organization validated"

Campos/Extensiones	Crítico	Contenido
version		3
serialNumber		Unique non-sequential positive number of minimum length 64 bits
signature		Sha256WithRSAEncryption or Sha512WithRSAEncryption or ecdsa-with-SHA256 or ecdsa-with-SHA384
issuer		Same as the Subject field of the issuing CA certificate
validity		379 days
subject		
OrganizationName		Organization Name
LocalityName		Locality Name
StateOrProvinceName		State or province name
CountryName		CountryName
subjectPublicKeyInfo		RSA 2048 bits minimum or ECDSA 256 bits (prime256v1) or 384 bits (secpr384r1)
Extensions		
subjectAltName		
dnsName		DNS name(s)
extendedKeyUsage		serverAuth, clientAuth
subjectKeyIdentifier		Derived from the result of applying the hash to the public key of the subject
authorityKeyIdentifier		Derived from the result of applying the hash to the Public key of the issuing CA
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.0.41248
cpsURI		http://policy.eadtrust.eu
policyIdentifier		0.4.0.2042.1.7 (ETSI OVCP)
policyIdentifier		2.23.140.1.2.2 (CAB/FORUM OV)
cRLDistributionPoints		http://crl.eadtrust.eu/eadtrust-subca- <algorithm><keylength>eaddvov<year>.crl
authorityInfoAccess		
calssuers		http://ca.eadtrust.eu/eadtrust-subca- <algorithm><keylength>eaddvov<year>.crt
ocsp		http://ocsp.eadtrust.eu
basicConstraint	Crítica	CA false
keyUsage	Crítica	digitalSignature
CT RFC6962		Certificate Transparency

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

17.5.10 Perfil de certificado no cualificado de web "Extended Validation"

Campos/Extensiones	Crítico	Contenido
version		3
serialNumber		Unique non-sequential positive number of minimum length 64 bits
signature		Sha256WithRSAEncryption or Sha512WithRSAEncryption or ecdsa-with-SHA256 or ecdsa-with-SHA384
issuer		Same as the Subject field of the issuing CA certificate
validity		379 days
subject		
businessCategory		Private Organization, Government Entity, Business Entity or Non-Commercial Entity
jurisdictionCountryName		Country of Jurisdiction of Incorporation or Registration Field
jurisdictionStOrProvName		State or Province of Jurisdiction of Incorporation or Registration Field
jurisdictionLocalityName		Locality of Jurisdiction of Incorporation or Registration Field
OrganizationName		Organization Name
LocalityName		Locality Name
StateOrProvinceName		State or province name
CountryName		CountryName
serialNumber		Registration Number
OrganizationIdentifier		ETSI EN 319 412-1 and CA/B Forum format
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		1.3.6.1.4.1.501.2.1.1.0.41249
cpsURI		http://policy.eadtrust.eu
policyIdentifier		0.4.0.2042.1.4 (ETSI EVCP)
policyIdentifier		2.23.140.1.1 (CAB/FORUM EV)
cRLDistributionPoints		http://crl.eadtrust.eu/eadtrust-subca- <algorithm><keylength>eadevpsd2<year>.crl
authorityInfoAccess		

Campos/Extensiones	Crítico	Contenido
calssuers		http://ca.eadtrust.eu/eadtrust-subca-<algorithm><keylength>eadevpsd2<year>.crt
ocsp		http://ocsp.eadtrust.eu
basicConstraint	Crítica	CA false
keyUsage	Crítica	digitalSignature
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.

17.5.11 Perfil de certificado cualificado de empleado público con nivel de aseguramiento sustancial/medio

Campos/Extensiones	Crítico	Contenido
Versión		3
serialNumber		Número positive único
signature		Sha256WithRSAEncryption ó ecdsa-with-SHA256 ó ecdsa-with-SHA384
Issuer		Igual que el subject de la CA C O OU OI CN
Validity		4 años
Subject		
CommonName		Nombre Apellido1 Apellido2 – DNI/NIE (Número de DNI/NIE)
Title	Opcional	Cargo
OrganizationalUnit	Opcional	Unidad dentro de la administración
OrganizationalUnit	Opcional	Código DIR3 de la unidad
OrganizationalUnit	Opcional	Número de identificación. (NRP o NIP)
OrganizationalUnit		CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO
OrganizationName		Organization Name
serialNumber		DNI/NIE semántica ETSI EN 319 412-1
Surname		Apellidos
Given Name		Nombre
CountryName		CountryName
subjectPublicKeyInfo		RSA 2048 bits
extensions		
subjectAltName		
rfc822Name	Opcional	Email del responsable
directoryName		
2.16.724.1.3.5.7.2.1		CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO
2.16.724.1.3.5.7.2.2		Entidad suscriptora
2.16.724.1.3.5.7.2.3		Número único de identificación de la entidad

Campos/Extensiones	Crítico	Contenido
2.16.724.1.3.5.7.2.4		DNI o NIE del firmante
2.16.724.1.3.5.7.2.5	Opcional	Número de identificación del firmante
2.16.724.1.3.5.7.2.6		Nombre (40 caracteres)
2.16.724.1.3.5.7.2.7		Apellido1 (40 caracteres)
2.16.724.1.3.5.7.2.8		Apellido2 (40 caracteres)
2.16.724.1.3.5.7.2.9	Opcional	Correo electrónico del firmante
2.16.724.1.3.5.7.2.10	Opcional	Unidad, dentro de la Administración, en la que está incluida el firmante
2.16.724.1.3.5.7.2.11	Opcional	Puesto desempeñado por el firmante dentro de la administración.
Othername: UPN	Opcional	UPN para smart card logon
extendedKeyUsage		clientAuth, emailProtection
subjectKeyIdentifier		Derivado de aplicar el hash a la clave del suscriptor
authorityKeyIdentifier		Derivado de aplicar el hash a la clave del emisor
certificatePolicies*		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.0.41223
cpsURI		http://policy.eadtrust.eu
userNotice		European Agency of Digital Trust, S.L. Certificado cualificado de empleado público
policyIdentifier		0.4.0.194112.1.0 (ETSI QCP-n)
policyIdentifier		2.16.724.1.3.5.7.2
policyIdentifier***	**Opcional**	1.3.6.1.4.1.501.2.1.0.3
cRLDistributionPoints		http://crl.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadnp<Año>.crl
authorityInfoAccess		
caIssuers		http://ca.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadnp<Año>.crt
ocsp		http://ocsp.eadtrust.eu
qcStatements**		
QcCompliance		Present
QcType		id-etsi-qct-esign
QcRetentiodPeriod		15
qcStatement-2		0.4.0.194121.1.1 (id-etsi-qcs-SemanticsId-Natural)
keyUsage	Crítica	digitalSignature, keyEncipherment,contentcommitment

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

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

***Cuando esté presente el OID de política 1.3.6.1.4.1.501.2.1.0.3, indica que el certificado se usará para sistemas de firma remota (firma on-behalf).

Se podrán emitir certificados con nivel de aseguramiento ALTO para empleado publico, siguiendo las directrices definidas en el documento “Perfiles de Certificados Electrónicos de la administración pública” que define los perfiles de certificados derivados de la aplicación del Real Decreto 203/2021, de 30 de marzo y está adaptado a las disposiciones de la Ley 39/2015 de 1 de Octubre, de Procedimiento

Administrativo Común de las Administraciones Públicas, la Ley 40/2015 de 1 de Octubre, de Régimen Jurídico del Sector Publico (LRJ) y al Reglamento (UE) 910/2014.

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

17.5.12 Perfil de certificado cualificado de empleado público con seudónimo con nivel de aseguramiento Alto (Firma)

Campos/Extensiones	Crítico	Contenido
Versión		3
serialNumber		Número positive único
signature		Sha256WithRSAEncryption
Issuer		Igual que el subject de la CA C O OU OI CN
Validity		4 años
Subject		
CommonName		(PUESTO o CARGO o literal SEUDONIMO) – SEUDONIMO – NOMBRE OFICIAL DEL ORGANISMO
Pseudonym		seudónimo
Title	Opcional	Nombre del puesto o cargo
OrganizationalUnit	Opcional	Unidad dentro de la administración
OrganizationalUnit	Opcional	Código DIR3 de la unidad
OrganizationalUnit		CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO
OrganizationName		Organization Name
CountryName		CountryName
subjectPublicKeyInfo		RSA 2048
extensions		
subjectAltName		
rfc822Name	Opcional	Email del responsable
directoryName		
2.16.724.1.3.5.4.1.1		CERTIFICADO CUALIFICADO DE FIRMA ELECTRONICA DE EMPLEADO PUBLICO CON SEUDONIMO, DE NIVEL ALTO
2.16.724.1.3.5.4.1.2		Entidad suscriptora
2.16.724.1.3.5.4.1.3		NIF suscriptora
2.16.724.1.3.5.4.1.9	Opcional	Correo electrónico de contacto
2.16.724.1.3.5.4.1.10	Opcional	Unidad
2.16.724.1.3.5.4.1.11	Opcional	Puesto
2.16.724.1.3.5.4.1.12		Seudónimo
subjectKeyIdentifier		Derivado de aplicar el hash a la clave del suscriptor
authorityKeyIdentifier		Derivado de aplicar el hash a la clave del emisor
certificatePolicies		

Campos/Extensiones	Crítico	Contenido
policyIdentifier		1.3.6.1.4.1.501.2.1.1.1.41224
cpsURI		http://policy.eadtrust.eu
userNotice		European Agency of Digital Trust, S.L. Certificado cualificado de empleado público con seudónimo nivel alto
policyIdentifier		0.4.0.194112.1.2 (ETSI QCP-n-qscd)
policyIdentifier		2.16.724.1.3.5.4.1
policyIdentifier**	**Opcional**	1.3.6.1.4.1.501.2.1.0.3
cRLDistributionPoints		http://crl.eadtrust.eu/eadtrust-subca- <algoritmo><tamañoclave>eadnp<Año>.crl
authorityInfoAccess		
caIssuers		http://ca.eadtrust.eu/eadtrust-subca- <algoritmo><tamañoclave>eadnp<Año>.crt
ocsp		http://ocsp.eadtrust.eu
qcStatements*		
QcCompliance		Present
QcType		id-etsi-qct-esign
QcRetentiodPeriod		15
QcSSCD		Presente
qcStatement-2		0.4.0.194121.1.1 (id-etsi-qcs-SemanticsId-Natural)
keyUsage	Crítica	contentCommitment
*Contempla el uso de dispositivo cualificado de creación de firma. **Cuando esté presente el OID de política 1.3.6.1.4.1.501.2.1.0.3, indica que el certificado se usará para sistemas de firma remota (firma on-behalf).		

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

17.5.13 Perfil de certificado cualificado de empleado público con seudónimo con nivel de aseguramiento Alto (Autenticación)

Campos/Extensiones	Crítico	Contenido
Versión		3
serialNumber		Número positive único
signature		Sha256WithRSAEncryption
Issuer		Igual que el subject de la CA C O OU OI CN
Validity		4 años
Subject		
CommonName		(PUESTO o CARGO o literal SEUDONIMO) – SEUDONIMO – NOMBRE OFICIAL DEL ORGANISMO
Pseudonym		seudónimo
Title	Opcional	Nombre del puesto o cargo
OrganizationalUnit	Opcional	Unidad dentro de la administración

Campos/Extensiones	Crítico	Contenido
OrganizationalUnit	Opcional	Código DIR3 de la unidad
OrganizationalUnit		CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO
OrganizationName		Organization Name
CountryName		CountryName
subjectPublicKeyInfo		RSA 2048
extensions		
subjectAltName		
rfc822Name	Opcional	Email del responsable
directoryName		
2.16.724.1.3.5.4.1.1		CERTIFICADO CUALIFICADO DE FIRMA ELECTRONICA DE EMPLEADO PUBLICO CON SEUDONIMO, DE NIVEL ALTO
2.16.724.1.3.5.4.1.2		Entidad suscriptora
2.16.724.1.3.5.4.1.3		NIF suscriptora
2.16.724.1.3.5.4.1.9	Opcional	Correo electrónico de contacto
2.16.724.1.3.5.4.1.10	Opcional	Unidad
2.16.724.1.3.5.4.1.11	Opcional	Puesto
2.16.724.1.3.5.4.1.12		Seudónimo
subjectKeyIdentifier		Derivado de aplicar el hash a la clave del suscriptor
authorityKeyIdentifier		Derivado de aplicar el hash a la clave del emisor
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.1.41225
cpsURI		http://policy.eadtrust.eu
userNotice		European Agency of Digital Trust, S.L. Certificado cualificado de empleado público con seudónimo nivel alto
policyIdentifier		0.4.0.194112.1.2 (ETSI QCP-n-qscd)
policyIdentifier		2.16.724.1.3.5.4.1
policyIdentifier**	**Opcional**	1.3.6.1.4.1.501.2.1.0.3
cRLDistributionPoints		http://crl.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadnp<Año>.crl
authorityInfoAccess		
calssuers		http://ca.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadnp<Año>.crt
ocsp		http://ocsp.eadtrust.eu
qcStatements*		
QcCompliance		Present
QcType		id-etsi-qct-esign
QcRetentiodPeriod		15
QcSSCD		Presente
qcStatement-2		0.4.0.194121.1.1 (id-etsi-qcs-SemanticsId-Natural)
extendedKeyUsage		clientAuth, emailprotection
keyUsage	Crítica	digitalSignature
*Contempla el uso de dispositivo cualificado de creación de firma		

Campos/Extensiones	Crítico	Contenido
**Cuando esté presente el OID de política 1.3.6.1.4.1.501.2.1.0.3, indica que el certificado se usará para sistemas de firma remota (firma on-behalf).		

Se podrán emitir certificados con otros niveles de aseguramiento para empleado publico con seudónimo en el futuro, siguiendo las directrices definidas en el documento Perfiles de Certificados Electrónicos de la administración pública que define los perfiles de certificados derivados del Real Decreto 203/2021, de 30 de marzo y está adaptado a las disposiciones de la Ley 39/2015 de 1 de Octubre, de Procedimiento Administrativo Común de las Administraciones Públicas, la Ley40/2015 de 1 de Octubre, de Régimen Jurídico del Sector Publico (LRJ) y al Reglamento (UE) 910/2014.

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

17.5.14 Perfil de certificado cualificado de empleado público de Justicia con seudónimo con nivel de aseguramiento sustancial/medio

Este certificado parte del perfil de certificado cualificado de empleado público con nivel de aseguramiento sustancial/medio.

Se consideran los siguientes aspectos:

En el campo **Organization (O)** se indica “ADMINISTRACIÓN DE JUSTICIA”.

En el campo **Organizational Unit (OU)** se indica “CONSEJO GENERAL DEL PODER JUDICIAL” o “ADMINISTRACIÓN DE JUSTICIA”).

En el campo **TITLE** se indica el CUERPO. Por ejemplo: Title=“CARRERA JUDICIAL“ o Title=“CARRERA FISCAL“ o Title=“C. LETRADOS DE LA ADMINISTRACIÓN DE JUSTICIA”)

En el campo **Common Name (CN)** se indica:

- CUERPO
- SÍMBOLO o CARÁCTER (-) de separación
- SEUDONIMO (Número de Personal del ámbito de la justicia precedido de los caracteres “JU:ES-“, según lo definido en la norma EN319 412-1). Ver regla más adelante.
- SÍMBOLO o CARÁCTER (-) de separación
- NOMBRE OFICIAL DEL ORGANISMO. Puede tener dos valores: ADMINISTRACIÓN DE JUSTICIA o CONSEJO GENERAL DEL PODER JUDICIAL.

Ejemplos:

- CARRERA JUDICIAL - JU:ES-J000001279 - CONSEJO GENERAL DEL PODER JUDICIAL
- C. AUXILIO JUDICIAL - JU:ES-A000000011N - ADMINISTRACIÓN DE JUSTICIA
- CARRERA FISCAL - JU:ES-F000002482E - ADMINISTRACIÓN DE JUSTICIA

En el campo **User notice** se indica: "Certificado cualificado de empleado público con seudónimo del ámbito de la Justicia"

En los campos **Subject Alternative Names** se indica:

- OID: 2.16.724.1.3.5.7.2.6) Nombre (40 caracteres)
- OID: 2.16.724.1.3.5.7.2.7) Apellido1 (40 caracteres)
- OID: 2.16.724.1.3.5.7.2.8) Apellido2 (40 caracteres)

Se podrá incluir opcionalmente un literal (AUTENTICACION, FIRMA o CIFRADO) que identifique la tipología del certificado. Este identificador siempre estará al final del CN y entre paréntesis. En el caso de un nivel de aseguramiento medio/sustancial, si se agrupan varios perfiles en un único certificado, no se deberá incluir esta opción.

No se podrá incluir el número de DNI/NIE.

El código de identificación de seudónimo (número profesional de la Administración de Justicia) está formado por una letra correspondiente al CARGO y CUERPO, un valor numérico de 9 caracteres y una letra de control. A este código se le anteponen las letras "JU:ES-"

Se asignará CARGO y una letra dependiendo del tipo de profesional atendiendo a la siguiente tabla:

Tipo Profesional	Letra Asignada
C. AUXILIO JUDICIAL	A
C. E. AYUDANTE DE LABORATORIO DEL INTCF	Y
C. E. FACULTATIVO DEL INTCF	X
CARRERA FISCAL	F
C. GESTIÓN PROCESAL Y ADMINISTRATIVA	G
CARRERA JUDICIAL	J
C. LETRADOS DE LA ADMINISTRACIÓN DE JUSTICIA	L
C. N. MÉDICOS FORENSES	I
C. E. TÉCNICO ESPECIALISTA DE LABORATORIO INTCF	E
C. TRAMITACIÓN PROCESAL Y ADMINISTRATIVA	T

Nota: las abreviaturas "C." corresponden a Cuerpo, "C. E." a Cuerpo Especial, "C. N." a Cuerpo Nacional e "INTCF" a Instituto Nacional de Toxicología y Ciencias Forenses.

El número profesional utiliza un dígito de control (una letra) al final del código para evitar posibles errores. Para calcular dicha letra se divide el número por 23, según la siguiente tabla:

RESTO	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22

DÍGITO DE CONTROL	R	W	A	G	M	Y	F	P	D	X	B	N	J	Z	S	Q	V	H	L	C	K	E	T

17.5.15 Perfil de certificado cualificado de empleado público de Justicia con seudónimo con nivel de aseguramiento Alto (Firma)

Este certificado parte del perfil de certificado cualificado de empleado público con seudónimo con nivel de aseguramiento Alto (Firma), con las consideraciones incluidas en el apartado 16.5.13 (Perfil de certificado cualificado de empleado público de Justicia con nivel de aseguramiento sustancial/medio)

17.5.16 Perfil de certificado cualificado de empleado público de Justicia con seudónimo con nivel de aseguramiento Alto (Autenticación)

Este certificado parte del perfil de certificado cualificado de empleado público con seudónimo con nivel de aseguramiento Alto (Autenticación), con las consideraciones incluidas en el apartado 16.5.13 (Perfil de certificado cualificado de empleado público de Justicia con nivel de aseguramiento sustancial/medio)

17.5.17 Perfil de certificado cualificado de web PSD2 (QWAC) Extended Validation

Campos/Extensiones	Crítico	Contenido
version		3
serialNumber		Unique non-sequential positive number of minimum length 64 bits
signature		Sha256WithRSAEncryption or Sha512WithRSAEncryption or ecdsa-with-SHA256 or ecdsa-with-SHA384
issuer		Same as the Subject field of the issuing CA certificate
validity		379 days
subject		
OrganizationIdentifier		ETSI EN 319 412-1 and CA/B Forum format
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

Campos/Extensiones	Crítico	Contenido
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
policyIdentifier		0.4.0.194112.1.4 (ETSI QEVCP-w)
policyIdentifier		2.23.140.1.1 (CAB/FORUM EV)
cRLDistributionPoints		http://crl.eadtrust.eu/eadtrust-subca-<algorithm><keylength>eadevpsd2<year>.crl
authorityInfoAccess		
caIssuers		http://ca.eadtrust.eu/eadtrust-subca-<algorithm><keylength>eadevpsd2<year>.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
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.

17.5.18 Perfil de certificado cualificado de sello electrónico para persona jurídica

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 2048 mínimo 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		1.3.6.1.4.1.501.2.1.1.0.41231
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
policyIdentifier***	**Opcional**	1.3.6.1.4.1.501.2.1.0.3
cRLDistributionPoints		http://crl.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadlp<Año>.crl

Campos/Extensiones	Crítico	Contenido
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)
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 1.3.6.1.4.1.501.2.1.1.0.41231 por 1.3.6.1.4.1.501.2.1.1.1.41231 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 Cuando esté presente el OID de política 1.3.6.1.4.1.501.2.1.0.3, indica que el certificado se usará para sistemas de firma remota (firma on-behalf).		

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

En el caso de los certificados EPREL se tendrán en cuenta las especificaciones publicadas.[62]

17.5.19 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>.

62 https://ec.europa.eu/info/sites/default/files/energy_climate_change_environment/suppliers_verification_guide_v1.05_0.pdf

Campos/Extensiones	Crítico	Contenido
		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
policyIdentifier***	**Opcional**	1.3.6.1.4.1.501.2.1.0.3
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

***Cuando esté presente el OID de política 1.3.6.1.4.1.501.2.1.0.3, indica que el certificado se usará para sistemas de firma remota (firma on-behalf).

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

17.5.20 Perfil de certificado cualificado de sede electrónica administrativa "Extended Validation" (QWAC) con nivel de aseguramiento Alto

Campos/Extensiones	Crítico	Contenido
version		3
serialNumber		integer positivo, no mayor 20 octetos
signature		SHA-2 con RSA.
issuer		Mismo Subject que el del certificado emisor. Campos Country Common Name Organization
validity		372 days
subject		
OrganizationalUnit		OU= "SEDE ELECTRONICA"
OrganizationalUnit		El nombre descriptivo de la sede. OU= p. ej: PUNTO DE ACCESO GENERAL
businessCategory		businessCategory = "Government Entity"
jurisdictionCountryName		jurisdictionCountryName= "ES"
jurisdictionStOrProvName		State or Province of Jurisdiction of Incorporation or Registration Field
jurisdictionLocalityName		Locality of Jurisdiction of Incorporation or Registration Field
OrganizationName		Denominación (nombre "oficial" de la organización) del suscriptor de servicios de certificación (custodio del certificado)
Common Name		Denominación de nombre de dominio (DNS) donde residirá el certificado. CN= p. ej: administracion.gob.es
LocalityName		Ciudad
StateOrProvinceName		State or province name
CountryName		Estado cuya ley rige el nombre, que será ES ("España") por tratarse de entidades públicas.
serialNumber		El NIF de la entidad responsable. SerialNumber = p. ej: S2833002. Size [RFC 5280] 64
Organization Identifier		Identificador de la organización. Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad) OrganizationIdentifier p. ej: VATES-S2833002.
subjectPublicKeyInfo		RSA 2048 bits
Extensions		
subjectAltName		
dnsName		DNS name(s)

Campos/Extensiones	Crítico	Contenido
extendedKeyUsage		serverAuth
subjectKeyIdentifier		Identificador de la clave pública del suscriptor o poseedor de claves (derivada de utilizar la función de Hash sobre la clave pública del sujeto). Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.
authorityKeyIdentifier		Medio para identificar la clave pública correspondiente a la clave privada utilizada para firmar un certificado, por ejemplo en los casos en que el emisor tiene múltiples claves de firma.
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.0.41246
cpsURI		http://policy.eadtrust.eu
userNotice		P. ej: "Certificado cualificado de sede electrónica, nivel alto. Consulte las condiciones de uso en " + URL de la DPC o, en su caso, documento legal de tercero
policyIdentifier		0.4.0.194112.1.4 (ETSI QEVCP-w) / *0.4.0.194112.1.5 (ETSI QNCP -w)*
policyIdentifier		2.23.140.1.1 (CAB/FORUM EV) / *2.23.140.1.2.1 (CAB/FORUM DV) — 2.23.140.1.2.2 (CAB/FORUM OV)*
policyIdentifier		2.16.724.1.3.5.5.1 (alto) / *2.16.724.1.3.5.5.2 (medio/sustancial)*
cRLDistributionPoints		http://crl.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadevpsd2<Año>.crl
authorityInfoAccess		
calssuers		http://ca.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadevpsd2<Año>.crt
ocsp		http://ocsp.eadtrust.eu
basicConstraint	Crítica	CA false
qcStatements		
QcCompliance		Indicación de certificado cualificado
QcType		id-etsi-qct-web
QcRetentiodPeriod		Integer:=15 ([ETSI EN 319 412-5] describe el periodo de conservación de toda la información relevante para el uso de un certificado, tras la caducidad de este) OID 0.4.0.1862.1.3
QcPDS		Lugar donde se encuentra la declaración PDS
semanticsId-Legal		Para indicar semántica de persona jurídica definida por la EN 319 412-1
keyUsage	Crítica	digitalSignature
CT RFC6962		Certificate Transparency (cuando estemos en CA/B Forum)
cabfOrganizationIdentifier		(OID: 2.23.140.3.1) If the subject: organizationIdentifier is present, this field MUST be present.

Los certificados EV pueden ser multidominio, pero NO se pueden emitir con calificadores de subdominio de tipo “wildcard” (*). Son de política **QEVCP-w** (certificate policy for EU qualified website authentication certificates based on EVCP). OID: `itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-web (4)`

Se podrán emitir certificados Wildcard cuando estén alineados con la política **QNCP-w** (certificate policy for EU qualified website authentication certificates based on NCP and PTC) según el CA/Browser Forum: "Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates". OID: `itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qncp-web (5)`

17.5.21 Perfil de certificado cualificado de sello de órgano Nivel Medio/Sustancial

Campos/Extensiones	Crítico	Contenido
version		3
serialNumber		Número positivo único (menor de 20 octetos)
signature		Sha256WithRSAEncryption
issuer		Igual al campo Subject del certificado de la CA emisora Country Organization Organizational Unit Organization Identifier Common Name
validity		5 años (o menos)
subject		
serialNumber	Opcional	Número único de identificación de la entidad, aplicable de acuerdo con la legislación del país. En España, NIF. SerialNumber = p. ej: S2833002. Número secuencial único asignado por el prestador (Printable String)) Size [RFC 5280] 64
Surname	Opcional	Primer y segundo apellido, de acuerdo con documento de identidad (DNI/Pasaporte), así como su DNI (Ver Criterios de Composición del campo CN para un empleado público). Primer apellido, espacio en blanco, segundo apellido del responsable del certificado (titular del órgano) de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 80 p. ej: "DE LA CAMARA ESPAÑOL - DNI 00000000G"
Givenname	Opcional	Nombre de pila, de acuerdo con documento de identidad (DNI/Pasaporte) Nombre de pila del responsable del certificado (titular del órgano) de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 p. ej: "JUAN ANTONIO"
CommonName		Denominación de sistema o aplicación de proceso automático. CN= p. ej: "PLATAFORMA DE VALIDACION Y FIRMA ELECTRONICA. @FIRMA. Nombre descriptivo del sistema automático. Asegurando que dicho nombre tenga sentido y no dé lugar a ambigüedades.
organizationIdentifier		Identificador de la organización distinto del nombre Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)

Campos/Extensiones	Crítico	Contenido
Organization Name		Denominación (nombre “oficial” de la organización) del creador del sello.
Country		Estado cuya ley rige el nombre, que será "España" por tratarse de entidades públicas.
OrganizationalUnit		SELLO ELECTRONICO
OrganizationalUnit		Denominación oficial de la unidad p. ej: SUBDIRECCION DE EXPLOTACION
OrganizationalUnit		Código DIR3 de la unidad p. ej: E04976701
subjectPublicKeyInfo		RSA 2048 mínimo
extensions		
issuerAltName		Igual al campo SubjectAlternativeNames de la CA Emisora
Subject Alternate Names		
Rfc822Name		Correo electrónico de contacto de la entidad suscriptora del sello. P. ej: soporte.afirma5@minhap.es
Directory Name		Tipo de certificado Tipo= SELLO ELECTRONICO DE NIVEL MEDIO (String UTF8) Size = 31 2.16.724.1.3.5.6.2.1 **Nombre de la entidad suscriptora** Entidad Suscriptora = p. ej: MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS (String UTF8) Size = 80 OID: 2.16.724.1.3.5.6.2.2 **NIF entidad suscriptora** NIF suscriptora = NIF entidad suscriptora, p. ej: S2833002 (String UTF8) Size = 9 OID: 2.16.724.1.3.5.6.2.3 **DNI/NIE del responsable (titular del órgano)** DNI/NIE responsable= p. ej: 00000000G (String UTF8) Size = 9 OID: 2.16.724.1.3.5.6.2.4 **Denominación de sistema o componente** Nombre descriptivo del sistema de sellado automático, asegurando que dicho nombre tenga sentido y no dé lugar a ambigüedades. Denominación sistema = p. ej: “PLATAFORMA DE VALIDACION Y FIRMA ELECTRONICA. @FIRMA”. (String UTF8) Size = 128 OID: 2.16.724.1.3.5.6.2.5 **Nombre de pila (titular del órgano)** N = Nombre de pila del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 OID: 2.16.724.1.3.5.6.2.6

Campos/Extensiones	Crítico	Contenido
		Ej: “JUAN ANTONIO” **Primer apellido (titular del órgano)** SN1 = Primer apellido del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 OID: 2.16.724.1.3.5.6.2.7 Ej: “DE LA CAMARA” **Segundo apellido (titular del órgano)** SN2 = Segundo apellido del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 En caso de no existir el segundo apellido, se dejará en blanco (sin ningún carácter). OID: 2.16.724.1.3.5.6.2.8 Ej: “ESPAÑOL” **Correo electrónico** Correo electrónico de la persona responsable del sello, p. ej: juanantonio.delacamara.espanol@mpr.es (String) Size [RFC 5280] 255 OID: 2.16.724.1.3.5.6.2.9
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		1.3.6.1.4.1.501.2.1.1.0.41233
cpsURI		http://policy.eadtrust.eu
userNotice		Ej: "Certificado cualificado de sello electrónico de Administración, órgano o entidad de derecho público, nivel Medio/Sustancial. Consulte las condiciones de uso en " + URL de la DPC o, en su caso, documento legal de tercero.
policyIdentifier		0.4.0.194112.1.1 (OID ETSI QCP-l)
userNotice		European Telecommunications Standards Institute. eIDAS European Regulation Compliant
policyIdentifier		2.16.724.1.3.5.6.2
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

Campos/Extensiones	Crítico	Contenido
ocsp		http://ocsp.eadtrust.eu
basicConstraint	Crítica	CA false
qcStatements		
QcCompliance		Presente
QcType		id-etsi-qct-eseal
QcRetentiodPeriod		Integer:=15 ([ETSI EN 319 412-5] describe el periodo de conservación de toda la información relevante para el uso de un certificado, tras la caducidad de este) OID 0.4.0.1862.1.3
qcStatement-2		0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)
QcPDS		
keyUsage	Crítica	digitalSignature, nonRepudiation, keyEncipherment

17.5.22 Perfil de certificado cualificado de sello de órgano Nivel Alto

Campos/Extensiones	Crítico	Contenido
version		3
serialNumber		Número positivo único (menor de 20 octetos)
signature		Sha256WithRSA Encryption.
issuer		Igual al campo Subject del certificado de la CA emisora Country Organization Organizational Unit Organization Identifier Common Name
validity		5 años (o menos)
subject		
serialNumber	Opcional	Número único de identificación de la entidad, aplicable de acuerdo con la legislación del país. En España, NIF. SerialNumber = p. ej: S2833002. Número secuencial único asignado por el prestador (Printable String)) Size [RFC 5280] 64
Surname	Opcional	Primer y segundo apellido, de acuerdo con documento de identidad (DNI/Pasaporte), así como su DNI (Ver Criterios de Composición del campo CN para un empleado público).

Campos/Extensiones	Crítico	Contenido
		Primer apellido, espacio en blanco, segundo apellido del responsable del certificado (titular del órgano) de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 80 p. ej: "DE LA CAMARA ESPAÑOL - DNI 00000000G"
Givenname	Opcional	Nombre de pila, de acuerdo con documento de identidad (DNI/Pasaporte) Nombre de pila del responsable del certificado (titular del órgano) de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 p. ej: "JUAN ANTONIO"
CommonName		Denominación de sistema o aplicación de proceso automático. CN= p. ej: "PLATAFORMA DE VALIDACION Y FIRMA ELECTRONICA. @FIRMA. Nombre descriptivo del sistema automático. Asegurando que dicho nombre tenga sentido y no dé lugar a ambigüedades.
organizationIdentifier		Identificador de la organización distinto del nombre Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)
Organization Name		Denominación (nombre "oficial" de la organización) del creador del sello.
Country		Estado cuya ley rige el nombre, que será "España" por tratarse de entidades públicas.
OrganizationalUnit		SELLO ELECTRONICO
OrganizationalUnit		Denominación oficial de la unidad p. ej: SUBDIRECCION DE EXPLOTACION
OrganizationalUnit		Código DIR3 de la unidad p. ej: E04976701
subjectPublicKeyInfo		RSA 2048 mínimo
extensions		
issuerAltName		Igual al campo SubjectAlternativeNames de la CA Emisora
Subject Alternate Names		
Rfc822Name		Correo electrónico de contacto de la entidad suscriptora del sello. P. ej: soporte.afirma5@minhap.es
Directory Name		**Tipo de certificado** Tipo= SELLO ELECTRONICO DE NIVEL ALTO (String UTF8) Size = 31 2.16.724.1.3.5.6.1.1 **Nombre de la entidad suscriptora**

Campos/Extensiones	Crítico	Contenido
		Entidad Suscriptora = p. ej: MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS (String UTF8) Size = 80 OID: 2.16.724.1.3.5.6.1.2 **NIF entidad suscriptora** NIF suscriptora = NIF entidad suscriptora, p. ej: S2833002 (String UTF8) Size = 9 OID: 2.16.724.1.3.5.6.1.3 **DNI/NIE del responsable (titular del órgano)** DNI/NIE responsable= p. ej: 00000000G (String UTF8) Size = 9 OID: 2.16.724.1.3.5.6.1.4 **Denominación de sistema o componente** Nombre descriptivo del sistema de sellado automático, asegurando que dicho nombre tenga sentido y no dé lugar a ambigüedades. Denominación sistema = p. ej: "PLATAFORMA DE VALIDACION Y FIRMA ELECTRONICA. @FIRMA". (String UTF8) Size = 128 OID: 2.16.724.1.3.5.6.1.5 **Nombre de pila (titular del órgano)** N = Nombre de pila del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 OID: 2.16.724.1.3.5.6.1.6 Ej: "JUAN ANTONIO" **Primer apellido (titular del órgano)** SN1 = Primer apellido del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 OID: 2.16.724.1.3.5.6.1.7 Ej: "DE LA CAMARA" **Segundo apellido (titular del órgano)** SN2 = Segundo apellido del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 En caso de no existir el segundo apellido, se dejará en blanco (sin ningún carácter). OID: 2.16.724.1.3.5.6.1.8 Ej: "ESPAÑOL" **Correo electrónico** Correo electrónico de la persona responsable del sello, p. ej: juanantonio.delacamara.espanol@mpr.es (String) Size [RFC 5280] 255 OID: 2.16.724.1.3.5.6.1.9
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		1.3.6.1.4.1.501.2.1.1.1.41233

Campos/Extensiones	Crítico	Contenido
cpsURI		http://policy.eadtrust.eu
userNotice		Ej: "Certificado cualificado de sello electrónico de Administración, órgano o entidad de derecho público, nivel alto. Consulte las condiciones de uso en " + URL de la DPC o, en su caso, documento legal de tercero
policyIdentifier		0.4.0.194112.1.3 (OID ETSI QCP-l-qscd)
userNotice		European Telecommunications Standards Institute. eIDAS European Regulation Compliant
policyIdentifier		2.16.724.1.3.5.6.1
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		Indicación de certificado cualificado
QcType		id-etsi-qct-eseal
QcRetentiodPeriod		Integer:=15 ([ETSI EN 319 412-5] describe el periodo de conservación de toda la información relevante para el uso de un certificado, tras la caducidad de este) OID 0.4.0.1862.1.3
qcStatement-2		0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)
QcSSCD		
QcPDS		
keyUsage	Crítica	digitalSignature, nonRepudiation, keyEncipherment

17.6 Perfil de CRL (Certificate Revocation List)

Las CRL's emitidas por EADTrust se emiten de conformidad con las siguientes normas:

- RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile - abril 2002.
- RFC 4325: Internet X.509 Public Key Infrastructure Authority Information Access Certificate Revocation List (CRL) Extension -diciembre 2005.
- RFC 4630: Update to DirectoryString Processing in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile -agosto 2006.

17.7 Perfil de certificado para respondedor OCSP

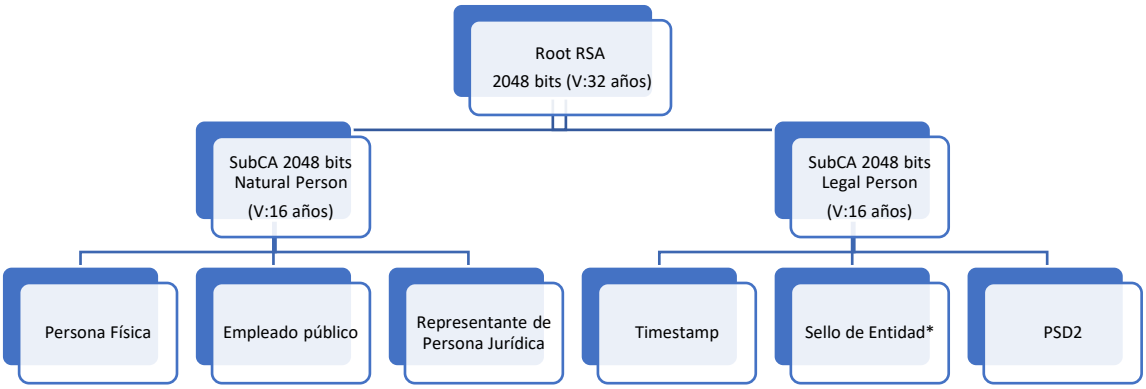
Los certificados emitidos por EADTrust para Respondedores OCSP, son conformes con la norma:

- RFC 6960: Internet X.509 Public Key Infrastructure Online Certificate Status Protocol-OCSP.

Campo	Crítico	Contenido
version		3
serialNumber		Número positivo único
signature		Sha256WithRSAEncryption
issuer		Igual al campo Subject del certificado de la CA emisora
validity		1 año
Subject		
Country		País (ISO 3166-1 alpha 2 code)
Common Name		Nombre del OCSP Responder + Nombre de la CA que delega
Organization Name		European Agency of Digital Trust, S.L.
Organizational Unit		OCSP Responder
subjectPublicKeyInfo		RSA 1024, 2048 bits, 4096 bits
Extensiones		
authorityKeyIdentifier		Derivada del resultado de aplicar el hash a la Clave pública de la AC emisora
subjectKeyIdentifier		Derivada del resultado de aplicar el hash a la clave pública del sujeto
issuerAltName		Igual al campo Subject Alternative Names de la CA Emisora
subjectAltName		email: ca@eadtrust.eu URI: http://www.eadtrust.eu URI: http://ca.eadtrust.eu URI: http://policy.eadtrust.eu
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.0.6960
cpsURI		http://policy.eadtrust.eu/cps
userNotice		European Agency of Digital Trust, S.L. OCSP Certificate
OCSP No Check		
Basic Constraints		CA false
extendedKeyUsage		OCSP Stamping
keyUsage	**Crítica**	digitalSignature

Este tipo de certificados se expiden para servidores OCSP externos. El servidor OCSP interno firma las respuestas OCSP con el certificado de la CA subordinada correspondiente.

17.8 Listado completo de los certificados vigentes de EADTrust (Root CA y Sub-CA)



17.8.1 EADTrust RSA 2048 Root CA For Qualified Certificates 2019

Sha256:
15032DE1C99D402B30B83A98FA9644135BF350F0D1C55788CD7DBA2279D01E1A

-----BEGIN CERTIFICATE-----
MIIEZzCCA0+gAwIBAgIIU2BoCBlIgyQwDQYJKoZIhvcNAQELBQAwgZwxQjBABgNV
BAMMOUVBRFRydXN0IFJTQSAyMDQ4IFJvb3QgQ0EgRm9yIFF1YWxpZmllZCBDZXJ0
aWZpY2F0ZXMgMjAxOTEvMC0GA1UECgwmRXVyb3BlYW4gQWdlbmN5IG9mIERpZ2l0
YWwgVHJ1c3QsIFMuTC4xCzAJBgNVBAYTAkVTMRgwFgYDVQRhDA9WQVRFUy1CODU2
MjYyNDAwIBcNMTkwNjA2MTA1NjE4WhgPMjA1MTA1MjkxMDU2MThaMIGcMUIwQAYD
VQQDDDlFQURUcnVzdCBSU0EgMjA0OCBSb290IENBIEZvciBRdWFsaWZpZWQgQ2Vy
dGlmaWNhdGVzIDIwMTkxLzAtBgNVBAoMJkV1cm9wZWFuIEFnZW5jeSBvZiBEaWdp
dGFsIFRydXN0LCBTLkwuMQswCQYDVQQGEwJFUzEYMBYGA1UEYQwPVkFURVMtQjg1
NjI2MjQwMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxH50WSvmyaP2
TqEN/WI6VtuYjI5TjHaotSjgUGz72z0Z1dA7liX082iF/JGcvIovMbb0ayUNULz1
ezKkoTxCvPzNobvnNFrxPtkySAS5BVtxoD/0xZlgMwsyse892rEl/FIOiUucPzc2
HxWB10dDAhxhYlWcBAecsjYA0czh98s2ulNlWPAinFBcr0wmWD3P5qfz8TCzpk4r
4NStZFeg+ScdYbXLzcCGGU33V+8yEsMzppUyztRbtJrwPD/k/yumIXtStbWXup+d
Snbii5JiUhcTn3hXipjypIu3VFRBFzXY8Be6IVjpR24GG7tDVHyhbvJONGCK5CjD
umhFVOMS9QIDAQABo4GoMIGlMA8GA1UdEwEB/wQFMAMBAf8wDgYDVR0PAQH/BAQD
AgEGMGMGA1UdEQRcMFqBDmNhQGVhZHRydXN0LmV1hhZodHRwOi8vd3d3LmVhZHRy
dXN0LmV1hhVodHRwOi8vY2EuZWFkdHJ1c3QuZXWGGWh0dHA6Ly9wb2xpY3kuZWFk
dHJ1c3QuZXUwHQYDVR0OBBYEFB/Ua7BjhgwLCYxCbjPdeh0UMSuZMA0GCSqGSIb3
DQEBCwUAA4IBAQC/7aPGae9raByQdwTQCrfJZB8NCyKxWP847BGznHFh83k9hH4D
gQay13qnFRF7cxhv7DZ9p7u0Rrn89HQGEDp9zzlu3+PBa5rhh4ftZmAk5qL/0Wws
0IYZjwfuns+AnfUZdroLtWsVqpN0sgzrR73RksO0h2L1/Xm+1blPB8bcJcu0siaT
5BW6yb+sD/Whal51ZVayNcSX6vF5g0OoXjeojk2e1offACMAhpy5iTWW1jtcpjf3

R4F62ITsOdTtWzshdu7Bi4bHHwbSoLDlxLZmgmiZBg8In1EA0qb5zCR5Cdsy4w+6
Vi9PBz6ImVmgJmvsv+ojGjHpv0vCdU9ML/1j
-----END CERTIFICATE-----

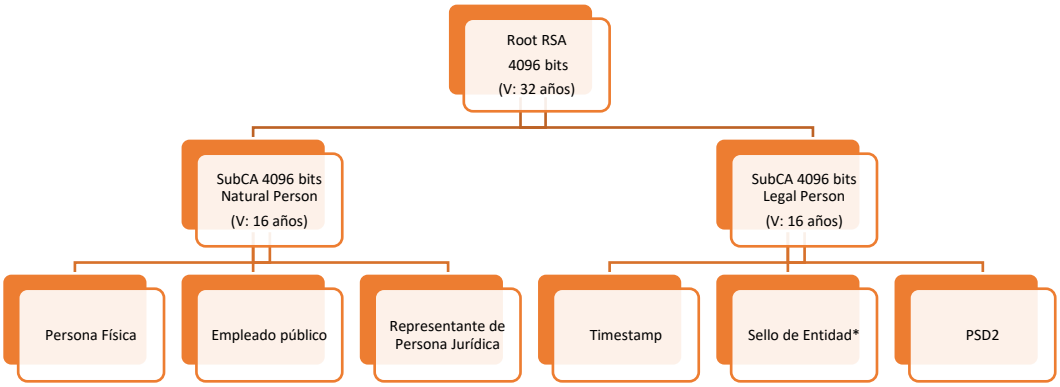
17.8.1 EADTrust RSA 2048 SubCA For Qualified Certificates 2019 – Natural Person

-----BEGIN CERTIFICATE-----
MIIGdTCCBV2gAwIBAgIIdGgFWUGBFicwDQYJKoZIhvcNAQELBQAwgZwxQjBABgNV
BAMMOUVBRFRydXN0IFJTQSAyMDQ4IFJvb3QgQ0EgRm9yIFF1YWxpZmllZCBDZXJ0
aWZpY2F0ZXMgMjAxOTEvMC0GA1UECgwmRXVyb3BlYW4gQWdlbmN5IG9mIERpZ2l0
YWwgVHJ1c3QsIFMuTC4xCzAJBgNVBAYTAkVTMRgwFgYDVQRhDA9WQVRFUy1CODU2
MjYyNDAwHhcNMTkwNjA2MTA1NjIzWhcNMzUwNjAyMTA1NjIzWjCBsTFAMD4GA1UE
Aww3RUFEVHJ1c3QgUlNBIDIwNDggU3ViQ0EgRm9yIFF1YWxpZmllZCBDZXJ0aWZp
Y2F0ZXMgMjAxOTEvMC0GA1UECgwmRXVyb3BlYW4gQWdlbmN5IG9mIERpZ2l0YWwg
VHJ1c3QsIFMuTC4xCzAJBgNVBAYTAkVTMRgwFgYDVQRhDA9WQVRFUy1CODU2MjYy
NDAxFTATBgNVBAsMDExlZ2FsIFBlcnNvbjCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAPBQEUtUdXNGvxaYBi9k1Te3sYjYRwRLzCqLeOcUzE6adEvcTSVN
MMzxu4hL+YSgm+2WrJDSbjLKVTlUJXIWGr1b3YzdYMyfKaZw6in76MNO0gUm1BFS
f7catMHzyqkQJ9GBUF0iEecERo1SFOeFltpXemXK5d1eApNchjQLDS7GduRgDb6r
gX+54yeLqh4opLsVEnYhO0umb5XXcO8m/tDhhUNqPWQZhUBubN3oPqdAM9CO5Q+n
Y2tVqKp3HtC2W0Mc6rvUit1KtopIwVjvNDTnwSWxDdtpy5pWmA42Ko4+a5fRNDBJ
55JT4FgPyjHsi5PZTtiSIF60y38ys7feoMUCAwEAAaOCAqIwggKeMIGoBgNVHSAE
gaAwgZ0wBgYEVR0gADCBkgYNKwYBBAGDdQIBAQGDETCBgDAlBggrBgEFBQcCARYZ
aHR0cDovL3BvbGljeS5lYWR0cnVzdC5ldTBXBggrBgEFBQcCAjBLDElTdWJvcmRp
bmF0ZSBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkuIEV1cm9wZWFuIEFnZW5jeSBvZiBE
aWdpdGFsIFRydXN0LCBTLkwuMBIGA1UdEwEB/wQIMAYBAf8CAQAwDgYDVR0PAQH/
BAQDAgGGMB0GA1UdDgQWBBT62Qqiacv/aK/ymon/VpRUG7OZjzBjBgNVHRIEXDBa
gQ5jYUBlYWR0cnVzdC5ldYYWaHR0cDovL3d3dy5lYWR0cnVzdC5ldYYVaHR0cDov
L2NhLmVhZHRydXN0LmV1hhlodHRwOi8vcG9saWN5LmVhZHRydXN0LmV1MGMGA1Ud
EQRcMFqBDmNhQGVhZHRydXN0LmV1hhZodHRwOi8vd3d3LmVhZHRydXN0LmV1hhVo
dHRwOi8vY2EuZWFkdHJ1c3QuZXWGGWh0dHA6Ly9wb2xpY3kuZWFkdHJ1c3QuZXUw
HwYDVR0jBBgwFoAUH9RrsGOGDAsJjEJuM916HRQxK5kwSQYDVR0fBEIwQDA+oDyg
OoY4aHR0cDovL2NybC5lYWR0cnVzdC5ldS9lYWR0cnVzdC1yb290LXJzYTIwNDhl
YWRxMjAxOS5jcmwweAYIKwYBBQUHAQEEbDBqMEMGCCsGAQUFBzAChjdodHRwOi8v
Y2EuZWFkdHJ1c3QuZXUvZWFkdHJ1c3Qtcm9vdC1yc2EyMDQ4ZWFkcTIwMTkuY3J0
MCMGCCsGAQUFBzABhhdodHRwOi8vb2NzcC5lYWR0cnVzdC5ldTANBgkqhkiG9w0B
AQsFAAOCAQEAUI5MNqYKLh2Is3HPs6xy0E4AYTmWqdlvNJRI9syz1PcEt5UxTk24
M7qzJ1wlC7I+xyJl1vR8FNTCXKHnCS0rgDXTIVl3YhxvvfhwxcXYITUPzK1LTte5
sJ4cyaAE5c701XWZFPhicRxZCPN1vgjD5CMuHB31LwbDzda28kpuvv247+WudKbG
XoHw6dyM5MJEU0f4q7X/Tw+EiV917+zIcfCn5A9hS3RSYb023DrqKQkrQoH/zhoH
EdBWdG1dCHMfy/nox/RhfSy5YCZyY38OhzfO1RB/i25hHsMBZpLjN673d3a2nsOQ
ShUd/8socvS7/YbN09fOuEcSZItak8uZyA==
-----END CERTIFICATE-----

17.8.2 EADTrust RSA 2048 SubCA For Qualified Certificates 2019 – Legal Person

82340EA4D7ACD80DF97DC7598C9495588CC8873EC9506DAD0C11EA119433399D

-----BEGIN CERTIFICATE-----
MIIGeDCCBWCgAwIBAgIJAJYIF4d0g4kSMA0GCSqGSIb3DQEBCwUAMIGcMUIwQAYD
VQQDDDlFQURUcnVzdCBSU0EgMjA0OCBSb290IENBIEZvciBRdWFsaWZpZWQgQ2Vy
dGlmaWNhdGVzIDIwMTkxLzAtBgNVBAoMJkV1cm9wZWFuIEFnZW5jeSBvZiBEaWdp
dGFsIFRydXN0LCBTLkwuMQswCQYDVQQGEwJFUzEYMBYGA1UEYQwPVkFURVMtQjg1
NjI2MjQwMB4XDTE5MDYwNjEwNTYyMVoXDTM1MDYwMjEwNTYyMVowgbMxQDA+BgNV
BAMMN0VBRFRydXN0IFJTQSAyMDQ4IFN1YkNBIEZvciBRdWFsaWZpZWQgQ2VydGlm
aWNhdGVzIDIwMTkxLzAtBgNVBAoMJkV1cm9wZWFuIEFnZW5jeSBvZiBEaWdpdGFs
IFRydXN0LCBTLkwuMQswCQYDVQQGEwJFUzEYMBYGA1UEYQwPVkFURVMtQjg1NjI2
MjQwMRcwFQYDVQQLDA5OYXR1cmFsIFBlcnNvbjCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAPEz8MX8+TRSvmYqS/OpZ6VootOuD4eLdm4Krz8AFwdUAvzu
u5ckSIINcwdjxP3wcoAlDtP5PKLoPEniDQ+LABxKPzR+IbTJw3MRoJMCxyd3FoZG
riqorsVPH9SD8wM/ppNULtdW+K1WD6KTy6vwRJ+f4tLCW8/DmCFbOYYAnAeiATP5
oCLdl5JU62DeKDj085n31q0STN2wu6B9bqLer85FuhpoJagGVMW4r4sGAhH8mLGC
B+/o+kNQLXENXmf/U8gSnfixB6QDRGuwS7i6QUnrig3O1fYYluPNl4CqLnWwVGlM
L5AtCGQYFEIdE89ixmQ9H/osuewN/tDzuqCAAiMCAwEAAaOCAqIwggKeMIGoBgNV
HSAEgaAwgZ0wBgYEVR0gADCBkgYNKwYBBAGDdQIBAQGDETCBgDAlBggrBgEFBQcC
ARYZaHR0cDovL3BvbGljeS5lYWR0cnVzdC5ldTBXBggrBgEFBQcCAjBLDElTdWJv
cmRpbmF0ZSBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkuIEV1cm9wZWFuIEFnZW5jeSBv
ZiBEaWdpdGFsIFRydXN0LCBTLkwuMBIGA1UdEwEB/wQIMAYBAf8CAQAwDgYDVR0P
AQH/BAQDAgGGMB0GA1UdDgQWBBRr3pOyqvu62v7vRk7JZ9w9/nundTBjBgNVHRIE
XDBagQ5jYUBlYWR0cnVzdC5ldYYWaHR0cDovL3d3dy5lYWR0cnVzdC5ldYYVaHR0
cDovL2NhLmVhZHRydXN0LmV1hhlodHRwOi8vcG9saWN5LmVhZHRydXN0LmV1MGMG
A1UdEQRcMFqBDmNhQGVhZHRydXN0LmV1hhZodHRwOi8vd3d3LmVhZHRydXN0LmV1
hhVodHRwOi8vY2EuZWFkdHJ1c3QuZXWGGWh0dHA6Ly9wb2xpY3kuZWFkdHJ1c3Qu
ZXUwHwYDVR0jBBgwFoAUH9RrsGOGDAsJjEJuM916HRQxK5kwSQYDVR0fBEIwQDA+
oDygOoY4aHR0cDovL2NybC5lYWR0cnVzdC5ldS9lYWR0cnVzdC1yb290LXJzYTIw
NDhlYWRxMjAxOS5jcmwweAYIKwYBBQUHAQEEbDBqMEMGCCsGAQUFBzAChjdodHRw
Oi8vY2EuZWFkdHJ1c3QuZXUvZWFkdHJ1c3Qtcm9vdC1yc2EyMDQ4ZWFkcTIwMTku
Y3J0MCMGCCsGAQUFBzABhhdodHRwOi8vb2NzcC5lYWR0cnVzdC5ldTANBgkqhkiG
9w0BAQsFAAOCAQEAdBpKcP8Acq/FqeeytxZPPJpJ78EygUtnOoSmt4KSmQ8OteG8
kBKd+ZQp7z3bsfxywShRXJjbFXq/ulzXBbClTrw6jWyCF6HbQKBdv6pE8g6vw3h/
Zv2QB48PjbcJx8pyTos6bd8qTb99m5XPZPdx5pxQv6gjZ33seizHpsOv+PvCXRlQ
65OnvbrNIZpgmteqAb/Uj7swKuW2TkF7jeadbsA1tb5W7Vs2D1Jf+FvWx4asqpCC
Od8Ec1LBiaVeQ3fzP41/Se/p1E3YhqlAckr8hGmz4ILCNksePtORbFdR3jh4FtU
cka3JrUxJgQ0PEk2lCdWrtRrJywKValDWs0E3w==
-----END CERTIFICATE-----



17.8.1 EADTrust RSA 4096 Root CA For Qualified Certificates 2019

17571DF0BB0ABEDAB83693C6CBACA5653371F0E499401CD07375172BF2433B11

```
-----BEGIN CERTIFICATE-----
MIIGZzCCBE+gAwIBAgIIIQlJZjUjZJIwDQYJKoZIhvcNAQELBQAwgZwxQjBABgNV
BAMMOUVBRFRydXN0IFJTQSA0MDk2IFJvb3QgQ0EgRm9yIFF1YWxpZmllZCBDZXJ0
aWZpY2F0ZXMgMjAxOTEvMC0GA1UECgwmRXVyb3BlYW4gQWdlbmN5IG9mIERpZ2l0
YWwgVHJ1c3QsIFMuTC4xCzAJBgNVBAYTAkVTMRgwFgYDVQRhDA9WQVRFUy1CODU2
MjYyNDAwIBcNMTkwNjA2MTA1NjMzWhgPMjA1MTA1MjkxMDU2MzNaMIGcMUIwQAYD
VQQDDDlFQURUcnVzdCBSU0EgNDA5NiBSb290IENBIEZvciBRdWFsaWZpZWQgQ2Vy
dGlmaWNhdGVzIDIwMTkxLzAtBgNVBAoMJkV1cm9wZWFuIEFnZW5jeSBvZiBEaWdp
dGFsIFRydXN0LCBTLkwuMQswCQYDVQQGEwJFUzEYMBYGA1UEYQwPVkFURVMtQjg1
NjI2MjQwMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAqQYfy0Vrc8SK
L6Saw5s1UQ4CztHwWDmyHKp5otL/7Ldp6i1R6CDW/Nd2E4Pfd5HCms5tqloc6cqk
npNheWLHrMOWCxOJagcuDFa3ISmEpLtnNQvOlJTF2sBevzRNhFSdrEExsGJ4W6Or
7diR495e5DlnifF3LI/vPIk8RLEPGMNp74fcrPM2ML28Nx9VvhvzhsYsiGFNZKgw
e3nqueAUC3TIUi/d8jS+VS4Bty1B1zFD3VrsTQ14NACTQNl1DQB9TN07XyOyP7A8
f+GWNs7LCyO1Y0lpk8X/jcz4RkBXAYETY6QNr/ome+abmSs7Nu7JVa6TCy1cXQgC
B5InQD18V077wFvH0WidkLJvN5MqO2MyVkzVzFk8q3CeVcWj8c8f0wYtptU3SNiN
QyVkahlAFyaMt4spancQjTY/eQ1jf5wjtQdnC48AJtgp46bbt0HAYEMgxB6JWpkJ
7GRr5REL+rqRTFZNPWqs1+nrcXS3NeZSgrtWKxDAA3w9t+aC/l9HrwWAAXH8MnB5
Ym8+0z50YEMTI9GNs4lbkdZe5DvkwYldxIawBhdXGWTFiFGlPuz5TGr0k4h85ko9
EusOCs2Ix8CGl3Y5dSdKWMPkAerVRuclwG0eLP+wCKf5jPo2RFjC6qcUIqGFJsS8
U15iJmYGkgpxRVq9EpKkmduhIeahOIkCAwEAAaOBqDCBpTAPBgNVHRMBAf8EBTAD
AQH/MA4GA1UdDwEB/wQEAwIBBjBjBgNVHREEXDBagQ5jYUBlYWR0cnVzdC5ldYYW
aHR0cDovL3d3dy5lYWR0cnVzdC5ldYYVaHR0cDovL2NhLmVhZHRydXN0LmV1hhlo
dHRwOi8vcG9saWN5LmVhZHRydXN0LmV1MB0GA1UdDgQWBBTjwjA0RwPADxeyY7BQ
E+UUsQxZ9DANBgkqhkiG9w0BAQsFAAOCAgEAgMlFhhM2dRMxE8vl4Rkq7X1MIOt9
```

t0DwJnxGZZLZaAX+FgzggHNWygWUbSeGZDrYQP/u1rWWffsGvCmd7WioRHhhzLs8
N9tr5cToapCElfOh7L++Cx8yVRP9dkoAgKeCAfDsg3uLcLlnn+32NFXD3sFkhBMY
8FbP1MOfFNYFQ0pMm9rbsLMR27qyCPyBt1kLjfJX1ylRJVmP9Q9Isc9LOpcG7rSf
T4lIH/NOa2RDfZXL0yuYGVHyPnREvGamI17OGXVWvirmpfWKvdMPi1Z12mEktOLn
paXBbrAHHjtGgB3wT8ujTo8Tkv0nEWrlrpuqjd+mo8Nd2OqGk5Rya8yQ93OFuMT+
fHbdCEs0M7xy7DNeoAEuQIFVmC2FpeYhmc6ZSPzFCjey/8ojWz7+zLRqlnmjIcwr
m7cLDgKmNoNOWy5HM0XEAZtzns7sgE7LLQICWScDzGPi7OE8K+hWqzV0L5v36hOm
cr9udcjcW9u83VuusPp/OuKLyRXiqRobYOZbpM/1wQIlG8csuaq1l8R3BWxDEuR6
SiGZVfx8xTlxCgIbG2udvuBrExntPIhFdWi7VjIIOQkI7lvYwLprCvhbRYD9Sm1R
19kIyD3eE2esLEPto0bLu3AETQtcadOQZqsQG+qLmzZfU3KTRzvbAHtAK4Y5qE+U
CmHHuZU44qXdGEI=
-----END CERTIFICATE-----

17.8.1 EADTrust RSA 4096 SubCA For Qualified Certificates 2019 – Natural Person

04BF1DA6D0168BDD3F2DEC2E22C50D558BDE5C7CC9516C83CB6393352A9F0F9C

-----BEGIN CERTIFICATE-----
MIIIdzCCBl+gAwIBAgIISHZjZSJoMyIwDQYJKoZIhvcNAQELBQAwgZwxQjBABgNV
BAMMOUVBRFRydXN0IFJTQSA0MDk2IFJvb3QgQ0EgRm9yIFF1YWxpZmllZCBDZXJ0
aWZpY2F0ZXMgMjAxOTEvMC0GA1UECgwmRXVyb3BlYW4gQWdlbmN5IG9mIERpZ2l0
YWwgVHJ1c3QsIFMuTC4xCzAJBgNVBAYTAkVTMRgwFgYDVQRhDA9WQVRFUy1CODU2
MjYyNDAwHhcNMTkwNjA2MTA1NjM1WhcNMzUwNjAyMTA1NjM1WjCBszFAMD4GA1UE
Aww3RUFEVHJ1c3QgUlNBIDQwOTYgU3ViQ0EgRm9yIFF1YWxpZmllZCBDZXJ0aWZp
Y2F0ZXMgMjAxOTEvMC0GA1UECgwmRXVyb3BlYW4gQWdlbmN5IG9mIERpZ2l0YWwg
VHJ1c3QsIFMuTC4xCzAJBgNVBAYTAkVTMRgwFgYDVQRhDA9WQVRFUy1CODU2MjYy
NDAxFzAVBgNVBAsMDk5hdHVyYWwgUGVyc29uMIICIjANBgkqhkiG9w0BAQEFAAOC
Ag8AMIICCgKCAgEAv4Lh3uZWD1QyEEpjSrPdYiZ5dVY8BqFjx2hvNlodk8q0R9/I
8AXxtTR2AmqgsDdVXOPCg3hRr+lxaY+fslWkyfknTZTjXEy9dxXd9Z0MPlRLI3A9
oZNkFLuQcu/qq19bLV1igRWGwgRJXPyY9T0rAdShfO+1pun5UXRlZAsjtFBM8FCQ
Uu+8g0yEhRf8yJfjhlaQvTRCtt6305aBsUwyjkSSZl10L3IxgUCs9Kzv2iQXn8te
B6Gsc38OBpgDT3lppS1grRUwzc3nlYw7+NisRxMvjZ0xCdyMl24+PgZ99fKGzDIk
OoKwIJLLUa3ecxgA4xslkcq/F5c4PfbJnUu8oWsp6MO7Z9U09MHAl8IFUrw6y5q0
5aQORm3qLqOXCUO+A6B7EVdJ5VtQZeZsS713G9u5QlA5xA28KAuqxpIqSEAXWsDu
nx3j5KKvObIZjVD11iPcXupqn2VoANphS2PHR1pkJIkTbQFoYmEz7pw6VSz4rCMp
1tE6uwHKPyehXBUenIEbHLyOWlXUEd4teNUB+WZpEFC7RyLYdJRKjfpNXC++shc4
tSsmBzH6CRWcdyxEbgNfaLV82zCGk0wY9OXsQfQZMqAAE/kYDCZelKr5GlJh/DR8
SdHet9EuBT92AspFkBvBHoeE2qU1yMG/1X9apNq44P+z3t1aQ8z0m7GOJ7UCAwEA
AaOCAqIwggKeMIGoBgNVHSAEgaAwgZ0wBgYEVR0gADCBkgYNKwYBBAGDdQIBAQGD
ETCBgDAlBggrBgEFBQcCARYZaHR0cDovL3BvbGljeS5lYWR0cnVzdC5ldTBXBggr
BgEFBQcCAjBLDElTdWJvcmRpbmF0ZSBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkuIEV1
cm9wZWFuIEFnZW5jeSBvZiBEaWdpdGFsIFRydXN0LCBTLkwuMBIGA1UdEwEB/wQI
MAYBAf8CAQAwDgYDVR0PAQH/BAQDAgGGMB0GA1UdDgQWBBQGM9orzumBUU9p3c3I
r98sLz2+XjBjBgNVHRIEXDBagQ5jYUBlYWR0cnVzdC5ldYYWaHR0cDovL3d3dy5l
YWR0cnVzdC5ldYYVaHR0cDovL2NhLmVhZHRydXN0LmV1hhlodHRwOi8vcG9saWN5
LmVhZHRydXN0LmV1MGMGA1UdEQRcMFqBDmNhQGVhZHRydXN0LmV1hhZodHRwOi8v
d3d3LmVhZHRydXN0LmV1hhVodHRwOi8vY2EuZWFkdHJ1c3QuZXWGGWh0dHA6Ly9w
b2xpY3kuZWFkdHJ1c3QuZXUwHwYDVR0jBBgwFoAU48IwNEcDwA8XsmOwUBPlFLEM

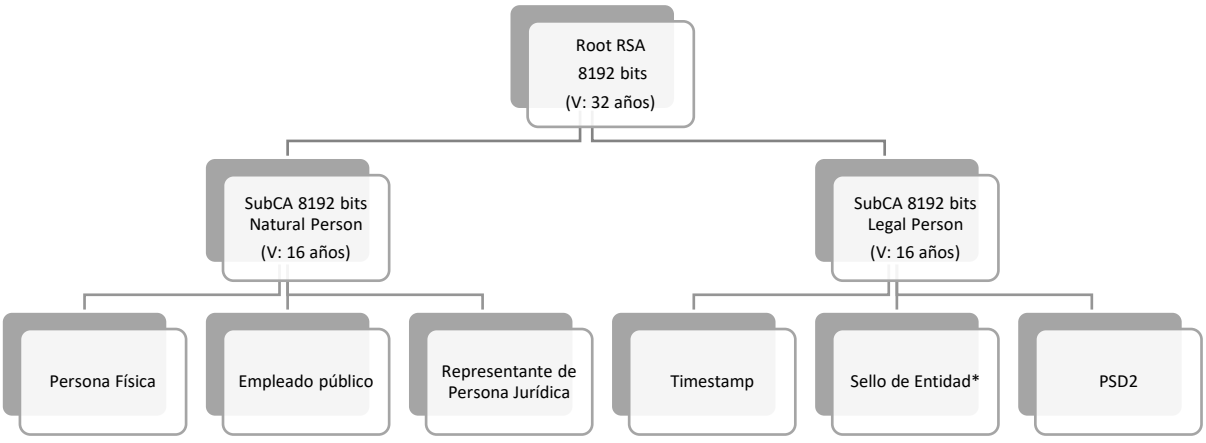
WfQwSQYDVR0fBEIwQDA+oDygOoY4aHR0cDovL2NybC5lYWR0cnVzdC5ldS9lYWR0
cnVzdC1yb290LXJzYTQwOTZlYWRxMjAxOS5jcmwweAYIKwYBBQUHAQEEbDBqMEMG
CCsGAQUFBzAChjdodHRwOi8vY2EuZWFkdHJ1c3QuZXUvZWFkdHJ1c3Qtcm9vdC1y
c2E0MDk2ZWFkcTIwMTkuY3J0MCMGCCsGAQUFBzABhhdodHRwOi8vb2NzcC5lYWR0
cnVzdC5ldTANBgkqhkiG9w0BAQsFAAOCAgEAcpvyo/49EIRP4e0YD9FdeJoBWGIm
WWFuEIGnw9wizXj7JDISUk/UXZo7ogmpGe4aB219gnJkZhHTAQ4gEIW4yKCUwbyG
efmhwwmcYoxz/Z9emWzRadrOUXGjO+bvvEFDr0Azbu0WOtR+aWwp0H6RhUJyZPdT
e+r26PskmPxAljbXLrb1JYYbfbEPX13u0jZBQm7BNjGcp5vgjIWTwRt5q8mA3RaK
hiI1+uv4E7prkO5CeSEdbwQz7aJo7snGw2RLO0RmvoPMQe+utRZMYNjWlEyh0ejv
ivFGcZ5vjiLO1fuqHV1O+TcZuC27zHgpB046XF79rnSpslkeL9MA+7pmUTNLisqT
KSVY6LXZjpiudEReMe3q5zdRvfYZAW1arUOMGFNwam/NJswxtPtCxh0Y3QhvBjxL
OTzkP+ruxkoKhjUKLHIuW1bRqGlLg9CNGG14Db16fvwUlyRRqaJH/aRKTZTgNHzR
Pt6gFxPO3q6YIy4TE/+odcIqlIrJNbth5FiqOt2D82WQjTKIGbgy+BqtdG40xh/B
aXMVkxO8VjJHiETKpombbm6gUedEXhqFcXle3V3H8hoq0AS48YId5GndkZJxww/p
A7Hx2d9J1IgpsP1QGdYC3fAtxCMB/RoeMklzgRIlG9mT5pkBK3epxZA+oEamXcIX
zfLLzmCrrerEILw=
-----END CERTIFICATE-----

17.8.1 EADTrust RSA 4096 SubCA For Qualified Certificates 2019 - Legal person

7FD0FFDF3AA0C96993DC6D1ADAD779226381AC7B5C48A01D1A2E4AFC6C2F777A

-----BEGIN CERTIFICATE-----
MIIIdTCCBl2gAwIBAgIIZDAGdySXc3IwDQYJKoZIhvcNAQELBQAwgZwxQjBABgNV
BAMMOUVBRFRydXN0IFJTQSA0MDk2IFJvb3QgQ0EgRm9yIFF1YWxpZmllZCBDZXJ0
aWZpY2F0ZXMgMjAxOTEvMC0GA1UECgwmRXVyb3BlYW4gQWdlbmN5IG9mIERpZ2l0
YWwgVHJ1c3QsIFMuTC4xCzAJBgNVBAYTAkVTMRgwFgYDVQRhDA9WQVRFUy1CODU2
MjYyNDAwHhcNMTkwNjA2MTA1NjU3WhcNMzUwNjAyMTA1NjU3WjCBsTFAMD4GA1UE
Aww3RUFEVHJ1c3QgUlNBIDQwOTYgU3ViQ0EgRm9yIFF1YWxpZmllZCBDZXJ0aWZp
Y2F0ZXMgMjAxOTEvMC0GA1UECgwmRXVyb3BlYW4gQWdlbmN5IG9mIERpZ2l0YWwg
VHJ1c3QsIFMuTC4xCzAJBgNVBAYTAkVTMRgwFgYDVQRhDA9WQVRFUy1CODU2MjYy
NDAxFTATBgNVBAsMDExlZ2FsIFBlcnNvbjCCAiIwDQYJKoZIhvcNAQEBBQADggIP
ADCCAgoCggIBAKsZ4po900f2BEfKsZB1FhlIgfqXksUEDv+aj+QSQkdxhmU3XYIg
t2vd2PtjUNrglCyuxr8ix9x90yEhz1wMWVRVRs10btEN4Aw9qzSZrQyKewx5SY7Y
7YSYa4P4SYrVZSWO/4RxLFcAec9Q4eM3owyuYFTfFFyGHJE43hKu+THfHw0bghPy
DjqGe+15/xh7JCdVlMc56kOU/tcKQd7ack3FQqiV9v+D+ki70f2E2pbUY1zhCvx9
/vTAPOVOzQ977IqzW0CsU51VnSjsxwph4XI3HdTQot4FKY7/U72/oDQGajg6Dzd2
awfBRQSLfASL1rfHSLCo18ycEog9OMiG0wJ0dL82gU+sCdFxSja6clc/tDpa6A4k
feTHHJOcHmbhkkBttXw55CdUSdymmb6+c0brqotKiCBm2NPINtLGNAAwERW0N2gM
mbgq13tQlY4FvGU9oIk1FzFfWpiP7ELOEAa+7f+3YscaoQ7zlVvcZ17xF/gi/KnE
EjB0UBL10K8naU61FXS0fakgG7JF0Tt5GSGDiNX/HE8p+0VOu6GOKKoGtvkthgs+
K1h66tHoa3sUA3aMo1IgMifOzwR7sfzkKttuTvDFRptvifx7/svtCjOu5k7sPxU4
vNgULtWHcwe9glkgdf0p79+SjoBDAc+kPMIIMaSTAr4m70EdlWU1mBD3AgMBAAGj
ggKiMIICnjCBqAYDVR0gBIGgMIGdMAYGBFUdIAAwgZIGDSsGAQQBg3UCAQEBgxEw
gYAwJQYIKwYBBQUHAgEWGWh0dHA6Ly9wb2xpY3kuZWFkdHJ1c3QuZXUwVwYIKwYB
BQUHAgIwSwxJU3Vib3JkaW5hdGUgQ2VydGlmaWNhdGUgQXV0aG9yaXR5LiBFdXJv
cGVhbiBBZ2VuY3kgb2YgRGlnaXRhbCBUcnVzdCwgUy5MLjASBgNVHRMBAf8ECDAG

AQH/AgEAMA4GA1UdDwEB/wQEAwIBhjAdBgNVHQ4EFgQUMS5X72kv2esv2yA4CeOE
pyxJ/0UwYwYDVR0SBFwwWoEOY2FAZWFkdHJ1c3QuZXWGFmh0dHA6Ly93d3cuZWFk
dHJ1c3QuZXWGFWh0dHA6Ly9jYS5lYWR0cnVzdC5ldYYZaHR0cDovL3BvbGljeS5l
YWR0cnVzdC5ldTBjBgNVHREEXDBagQ5jYUBlYWR0cnVzdC5ldYYWaHR0cDovL3d3
dy5lYWR0cnVzdC5ldYYVaHR0cDovL2NhLmVhZHRydXN0LmV1hhlodHRwOi8vcG9s
aWN5LmVhZHRydXN0LmV1MB8GA1UdIwQYMBaAFOPCMDRHA8APF7JjsFAT5RSxDFn0
MEkGA1UdHwRCMEAwPqA8oDqGOGh0dHA6Ly9jcmwuZWFkdHJ1c3QuZXUvZWFkdHJ1
c3Qtcm9vdC1yc2E0MDk2ZWFkcTIwMTkuY3JsMHgGCCsGAQUFBwEBBGwwajBDBggr
BgEFBQcwAoY3aHR0cDovL2NhLmVhZHRydXN0LmV1L2VhZHRydXN0LXJvb3QtcnNh
NDA5NmVhZHEyMDE5LmNydDAjBggrBgEFBQcwAYYXaHR0cDovL29jc3AuZWFkdHJ1
c3QuZXUwDQYJKoZIhvcNAQELBQADggIBAB5p4UleQ5K3+sw0s2TPQLbleanJmCEx
MjeNkv4wpxndMXcKI6x7qkZvwtp/vW6a8OhpTeRR2pmQwbhh4vFTI1GeHGxSDF6N
hJi71K5xy7lYL/P4etc5P12MlycKAtdFPSJoN1+utmXhADZQ4r65riNTwhJHCqq3
abXd13fkoJzqouqOpy8ndFY5tuVDMXU9ih4l1gV5dMs2pVgre/gS7U4nPA3OFRSV
mxZR+u7Q6YPmXoq06iG5F6uAhQGibiaUf4pUYcTJTQFx5hLSEMfHs2fwkFs70YBF
wlVdpDSpWLieYtZlpKvQcOWWpC1wujklxOzBlUWB/0ohm9Qw6ykw+2MUYFcZcqRT
C/Fn9UqAlFyUMT0F5hIvZ4w9YvqsBJXI2taPg1dMgM5TvXa41pjPAqN7+1BgtDH0
gfEmERpQpbbfILCYvl/uoVn25ZoEr6SKSCfBV1MFRr7Fm0G23x5vARR82cHfOVF4
c8MVAsfCKJZKmirQLLedf8cSMPB4pkFRtKPkXPjs8RsHLBOQONt9pNm/DVSD7xwe
Y+qqfoHEiD3vNqiQXTFvUNlkcbhAGZqAMZC2GGejoASNq9VQACu6vNww1nd/CPIl
PPPCnJKPKLbYQPWqndA24K9ZlrpOECg0YGfqxW5mbv4uWD5dAYC/bokXPeZxajyv
eVNwq7shidsX
-----END CERTIFICATE-----



17.8.1 EADTrust RSA 8192 Root CA For Qualified Certificates 2019

-----BEGIN CERTIFICATE-----
MIIKZzCCBk+gAwIBAgIIJhCHiXdYiREwDQYJKoZIhvcNAQENBQAwgZwxQjBABgNV
BAMMOUVBRFRydXN0IFJTQSA4MTkyIFJvb3QgQ0EgRm9yIFF1YWxpZmllZCBDZXJ0
aWZpY2F0ZXMgMjAxOTEvMC0GA1UECgwmRXVyb3BlYW4gQWdlbmN5IG9mIERpZ2l0
YWwgVHJ1c3QsIFMuTC4xCzAJBgNVBAYTAkVTMRgwFgYDVQRhDA9WQVRFUy1CODU2
MjYyNDAwIBcNMTkwNjA2MTExNDA4WhgPMjA1MTA1MjkxMTE0MDhaMIGcMUIwQAYD
VQQDDDlFQURUcnVzdCBSU0EgODE5MiBSb290IENBIEZvciBRdWFsaWZpZWQgQ2Vy

dGlmaWNhdGVzIDIwMTkxLzAtBgNVBAoMJkV1cm9wZWFuIEFnZW5jeSBvZiBEaWdp
dGFsIFRydXN0LCBTLkwuMQswCQYDVQQGEwJFUzEYMBYGA1UEYQwPVkFURVMtQjg1
NjI2MjQwMIIEIjANBgkqhkiG9w0BAQEFAAOCBA8AMIIECgKCBAEA0alN5WQu/Tlf
n8tANw/5+cJ8qOjtuSBUTCctyleW6Q11w9OS4Wdz2wj263OaCrxRjfyGso/dDpVi
tGrq9g7zL81kPYW2tqgNkB+IGAJ9VVB3Vu/8j1DIKPYwGEfAV/HwZV3RAFz71Hnm
IPZH5qAmme1E2ioPcg2q8beisJYYO3Avap8cjTXUxsAtyOcVA0E3osa1Gak45Njs
ucH6xfUKeokelPbnDxa2QiYpYioGEkghqXQkumH6mJ/RCnLOGYMYokN21YR/ec56
K7Ri6Q53qPU9IRcPktZubew5R9ePyFopPycwEGqcgObimDDC+XZfXpZ+0qsqRRrN
5PiZjs5jDX++xXIfoomnnDTxgXMSQnCkdf/g1bChhEbGIckjT7rz6GJpFRWdTbH1
8MQyBa3Ikrozv5h0ngUfGGTOau/8vCSCAj/Ow6TmTcTejM9/qXohRjuLi8/EnBf2
YJEMhFVWcFtgS64DOvA5X/X+QpY4t1r9MRjuBfaJ454NGM1IORoyUXPf4jF5XNm8
FIqDT3083PDRXQxYimBHsGrJ607oUNW4xItJUl0SjoLQfSab6mviIBnO+V/w7IER
IrqBe6Pnju8vTPmnrn23dXj8pMteTCTJ3bjyCCNVYXVKB4cfXGhWdytnEY442lvo
dGuc4ucbZIPc+YuPecRuQKkrpYk+gpAw0iF757PIC0yykqRX9fc2I739RvsR8OaV
Y/sAXYF3yKX7TF+MX6kGmL2GLtWnVIbDJLKtr5DCFvo+m6yt+z1AcG1UuYKP+3/l
Kn++6U68RtWyEZThMLI96mX0PMy1j2nAvnBZHHkM+o5cFD5qwQLxYuNCocJ7YYFR
J+3Y3qfJPJg+G0wwNMztV9TSC4n4J58ac82do0GcccWdGoyr/yEnlte9jJ/NQ61P
FKo/499m3UbfrwmBHeKIfhXW3LA0VHmkapfxTPGQSwTDewjwqo1HwPG1skCa3SII
i0xwUcXqK5/5ZPFnYV9TrxOUOv+y+UfOk6U2wE4cXnEllYkrdOKFV4DuL5yplbTM
bJ+MlUI3cy693DdVjyF5V5VoJzZW2vFFA+N4pG9mkyICIuLEwUjmNoFcwxCHjkDl
VBUYZIH25MA9o7HS1dsGA4InNtIl5Lt0aR8xR6a1x/Vgu7i26mQ+t/9m1BxEyDEd
6WN9kjnhe/ijEmdv5gjwAu0pPUHsDc1I+2YGtSKJD3ZWWk/RiwAmgVkrdicK50Ii
Xk67Ypj25JBXLfj5OfAnFJawNmCcjCv/BdQBMDmlPxMnyXmUZpf8Vua5mvncdcPT
zi2WTtDvq4kpvQwkXBuWySLQWv1f1PY6HZIYwqWEJXQptlM4DuhpgJyM+g1hqsDn
UyoXjbb2nQIDAQABo4GoMIGlMA8GA1UdEwEB/wQFMAMBAf8wDgYDVR0PAQH/BAQD
AgEGMGMGA1UdEQRcMFqBDmNhQGVhZHRydXN0LmV1hhZodHRwOi8vd3d3LmVhZHRy
dXN0LmV1hhVodHRwOi8vY2EuZWFkdHJ1c3QuZXWGGWh0dHA6Ly9wb2xpY3kuZWFk
dHJ1c3QuZXUwHQYDVR0OBBYEFAbmc9lROUCn0VeMNn/H7dB53ffLMA0GCSqGSIb3
DQEBDQUAA4IEAQCq6yOyzhD3p8j+R8cMwqtd2sJepky1JGcz7pN0o50TtP2zSZL/
+ZNs7cI30cg97YWc8JE7yRA+ppcLss25N1UlRUL8t1JTG0Xbf9fIovjlLjU3hA0z
RhzdtfGz5cdH0LS2rU6r893tX/yjW4KUyYI24XUrt0OZpcfKrtuZnSa2YHhmWOO9
KYrVqpIpNVU4P92Gr91H9Ro9IW6kg29/zpgjVr8SrNqkmaxhDEFuzLVphKbf+RZx
PzYZ7p5kobYSLNpzzgnhPkylc5ytkxTpQBXa79OZp7bwIEoRqYNfucTqIhY77wWL
7YUc2gq9HQM5FFaCUSb2Ik3HlgujBVk4euccvgRrOJXi9j2DL5ICHTdG7GW6F+xG
MrThkzevQoG4HHIvB/tQwQDHATEuTghzD2cFavIhnX0A97plPMEPlUwV7edJMum6
b/NaNRFJCIWhs9x6cORAQPfGDdyUwyaWWrq9VgcS2L+Yk/fs6nkhZdLtZ97F167i
pv11c3V89QOx2Iv+9JD5Nm+VqnaI5Z9vgrfYDDR5OM1i+EakKBDs7nDySPWd3F4l
1yuQu99FsBlQCE0k6C3TK8XgATqzwRW205YIc6NcSo3Byz4HMSarfHBK4utP3vI1
3KKzsImHmpJ/483xSPHxUYT4sD2FtynillSR0JIeyHZuhMGAK5Ix/JnTQNmCxC6C
M//Vq3IJN8ofFBMFCFxn/Kx0p8LZAHIQVsy8ttQBA2jnzlU98VDwS5sBsENCr927
hSaWw3XlWWUdZWbx0qu6wQSkiSlrVm3zyWSeFpv74ibM8VYMwRLiAL65m9nTxMyA
lfvcWgupv9RQbvrX2GU4KHhJN0vi6yUHOGugaGXvnnsOEllF49nop7zrA0N9QFoD
Jf530D9/U4mw0LS0Cli5eWKctCxDYMQXs/RTNOgOx0fy0yFNIGOlXBodLtswZPXw
sNcvo5H74dJLrbPWi6ZlaYOoEDq78XuP7kx0n7940Qrq7Ks6FGbhrNHYbb7Apm80
uYKKkw4qjBXlQUNqDd3wc8ug+y1abLZnHnmuW+dfGBKJD6M+hr6zDJXqcNz6xCWb
DzbBnxiiR/2zCP9rbHx1Af2bL2MCrvmwfaKtRHnNWS1vbfmu025p+Vr7yerin5+J
fyAs2hLJEO/G7Ef3EcMG6sH//z55EJw+ziqbExb0OPVsRLZqVv84H/vT4VxVsS8G
1RDxuEKSy9gg9iESq0a0VMVxk2Fypim6rvxFGAZceEWXy+XUP6G8zkXF3lqjl2/3
UJpVg+Z96CideS4DGHjVpFW/tu6J1NFK139KS6QFke9wP6g/bzrN+Q6OizSCc7v6
wjup+COimIMePMHiseuA4TKzEZD0U2lHjoiz

```
-----END CERTIFICATE-----
```

17.8.1 EADTrust RSA 8192 SubCA For Qualified Certificates 2019 – Natural Person

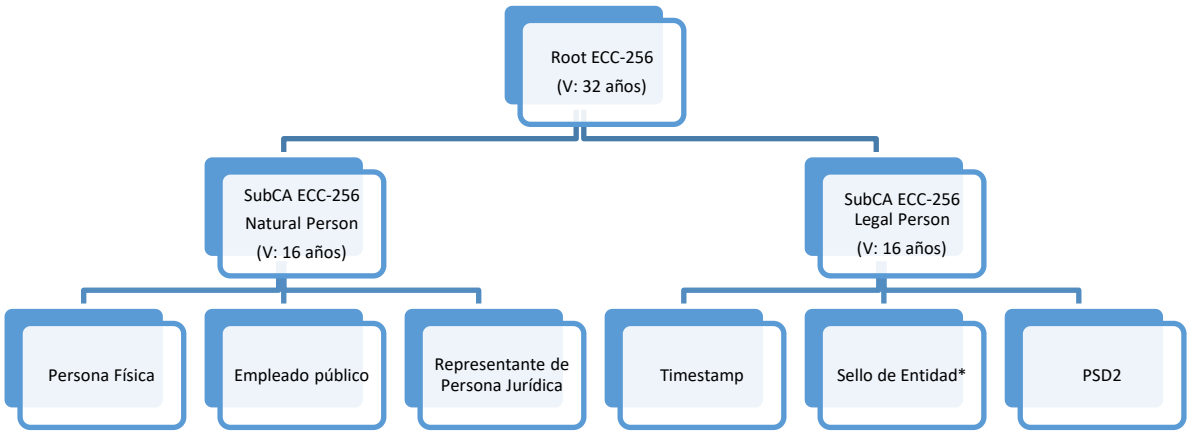
```
-----BEGIN CERTIFICATE-----
MIIMdzCCCF+gAwIBAgIIURY4c0dWMFkwDQYJKoZIhvcNAQENBQAwgZwxQjBABgNV
BAMMOUVBRFRydXN0IFJTQSA4MTkyIFJvb3QgQ0EgRm9yIFF1YWxpZmllZCBDZXJ0
aWZpY2F0ZXMgMjAxOTEvMC0GA1UECgwmRXVyb3BlYW4gQWdlbmN5IG9mIERpZ2l0
YWwgVHJ1c3QsIFMuTC4xCzAJBgNVBAYTAkVTMRgwFgYDVQRhDA9WQVRFUy1CODU2
MjYyNDAwHhcNMTkwNjA2MTEyMDUxWhcNMzUwNjAyMTEyMDUxWjCBszFAMD4GA1UE
Aww3RUFEVHJ1c3QgUlNBIDgxOTIgU3ViQ0EgRm9yIFF1YWxpZmllZCBDZXJ0aWZp
Y2F0ZXMgMjAxOTEvMC0GA1UECgwmRXVyb3BlYW4gQWdlbmN5IG9mIERpZ2l0YWwg
VHJ1c3QsIFMuTC4xCzAJBgNVBAYTAkVTMRgwFgYDVQRhDA9WQVRFUy1CODU2MjYy
NDAxFzAVBgNVBAsMDk5hdHVyYWwgUGVyc29uMIIEIjANBgkqhkiG9w0BAQEFAAOC
BA8AMIIECgKCBAEAvdbc3AjQjlTTpjUs7iwmyPFGJRP6OCW+Y3/+xPX7tK0EVbyC
IFKoM7XX1Iwt2YJkO53r1v2MoCekjI9xGT3LHFfWAlHJx6IFzc0lwLfdeH/fbt3T
0XPg+stZEa4cWtjtm8U0Aihi9XHRD5d+0PnTG2PyjYrWE2wSUqqOnYUSHPl7WJV7
DD37ZQFCFlBOyVk8XCJbQoxFoBSnC+SSODzvkKzR1a2L4YyDzL/ytPIDfpgP0qWI
mUyNGayvVAkSQ8jxOn3C7XgtwvTmAFS+TJsO4mkmLS03E9ausLHZVEVogqQdtgL1
dFeOJFKUONqlcDv9U80J5/D7DrgwBzUYz4Xx/lLVxmTk7A/7bu+qmnKi+y1NltIK
CMWMSQkZZMePwYGG/T82nxR4ln+AyWYJWpMP93O0XP8/SMBk5d3xl+aNl5pdzTUP
EKGQ8JGAF+HNfyZppFNpBEpXz9LRiTdQdcJHVpJ7E7dwdEfbM44YCiz8FZMLHxRA
gfvwRKEUmWWR26HB+CgdqjC6lBxZRH+e2n6QwJl7U26kv3dY9bCDtWs4qu8BFjNn
gEEwQ8G/zOhlp50888TKnzZwZEYV6zasz/3I37hAHKhfi0ke6KdhT0fERGvr1UBg
7jpmQNYzLHShOCs+Tq2qBwYlOEOIGFICaUC7gvXKtzhyroqL8Gbz4L3VxsqlsVmr
e5KOzV5eEHhBKjEF9KZFyBxDAwa65TNZcbSGGq3kc4NARUWdmkFMtQHF6GHUIxKe
xfQYPu/U3pFqwFG4SGxyPCcFCGa0tqIjCuIIBQpcORKTvR+DhBAS/l8o+5N4rE8g
qY1hn0//vxzQZ58DQtf0QrdEQYUjAP/VZrJq2bmjVWdfeF3UJQ6/XYKkMmlJrabq
Kv5pBHPAFVbUpitOU0CK+1rY0UKWLWUJldgx+/TcnLK/vAnevAcTdKyVqQzKCYKs
v7ZwUxpZVUwAeJHMTpY0EnhbVzz/5JnHHNqyU937cyRfyOMGovQfhoNc/RbkbWwC
0WY8+IAC41kBPSq64oA6Y5yKQizzogyp6+4WGHqyhhuR7OHi41sXgSPOggI3oEfT
s3I/NzsXyKi1bCQsye4y0oHPd4BRuzafRIP63FAhiyJ7AlSH+BGIgDDzqqpknYbd
aysAyQdwjPqfh6PO6D80FPf+Wf1rtTt/mUMLIIgTTJHWRF1cpC47Bc+Tx3b/j5rh
/X4d8jHLUDf4vzdowj1Gg2qdwJuGo0ikbUa2PafYmaDkfb70WgnHA/jV8+jPTz9A
RgEcPY/IGS522KdVQivE449EP33SMY/Mfb6Q2h6n+TUpI5u8SLsvDPTugvwVU0Wi
Upp2te3wcY2xj7diV0gKwsxT6sS7AvezdLisKQIDAQABo4ICojCCAp4wgagGA1Ud
IASBoDCBnTAGBgRVHSAAMIGSBg0rBgEEAYN1AgEBAYMRMIGAMCUGCCsGAQUFBwIB
FhlodHRwOi8vcG9saWN5LmVhZHRydXN0LmV1MFcGCCsGAQUFBwICMEsMSVN1Ym9y
ZGluYXRlIENlcnRpZmljYXRlIEF1dGhvcml0eS4gRXVyb3BlYW4gQWdlbmN5IG9m
IERpZ2l0YWwgVHJ1c3QsIFMuTC4wEgYDVR0TAQH/BAgwBgEB/wIBADAOBgNVHQ8B
Af8EBAMCAYYwHQYDVR0OBBYEFOqZz2sBGPmBRGn9yJpordU303OYMGMGA1UdEgRc
MFqBDmNhQGVhZHRydXN0LmV1hhZodHRwOi8vd3d3LmVhZHRydXN0LmV1hhVodHRw
Oi8vY2EuZWFkdHJ1c3QuZXWGGWh0dHA6Ly9wb2xpY3kuZWFkdHJ1c3QuZXUwYwYD
VR0RBFwwWoEOY2FAZWFkdHJ1c3QuZXWGFmh0dHA6Ly93d3cuZWFkdHJ1c3QuZXWG
FWh0dHA6Ly9jYS5lYWR0cnVzdC5dYYZaHR0cDovL3BvbGljeS5lYWR0cnVzdC5l
dTAfBgNVHSMEGDAWgBQG5nPZUTlAp9FXjDZ/x+3Qed33yzBJBgNVHR8EQjBAMD6g
PKA6hjhodHRwOi8vY3JsLmVhZHRydXN0LmV1L2VhZHRydXN0LXJvb3QtcnNhODE5
MmVhZHEyMDE5LmNybDB4BggrBgEFBQcBAQRsMGowQwYIKwYBBQUHMAKGN2h0dHA6
```

Ly9jYS5lYWR0cnVzdC5ldS9lYWR0cnVzdC1yb290LXJzYTgxOTJlYWRxMjAxOS5j
cnQwIwYIKwYBBQUHMAGGF2h0dHA6Ly9vY3NwLmVhZHRydXN0LmV1MA0GCSqGSIb3
DQEBDQUAA4IEAQBCe2VS5kD4qKddyF5XuTCAuyHeXXx9YUp3bmm+blEgSET/83BW
UNeuwamsxPzkBhyejvGn8hNR0ncej073Rlfai03qlXo6K8jwVjwNwDzgtB4oYMBw
vvKlnmuPRGd6qYdPtWMw6boMa2KQcEXqp0kp8F7yIY3agvt5wARRRMlK9Pgl+Fdd
8xFpKRS2WFqONV4V3gIIhOuCjzUGKkTmsoH1DGJYwc3mI36bJe6kVLwFEEnqm28t
vF86BygX11zUz9MnZx5obFGSGqdlewWnQCGINOLI052ovyCiQIOG6TE9Lcs0PzcE
9BqdWpxbGfnDK40U/05UCWDwIIa9qcSa4SWtrt6VEe5gtkpnPVx07nYaFVY85fDN
wz0LxzWM6zMucx85F3jtxuhaA+s9E6/qlxmFP8bnEDnb7HtYAKPF1pB98Beavpu9
mxTVc4GiTdmG6NFzly25p33qTmw5yBwLdmijvtlZWyrC6DwDx144KPYg63jT+FVI
oWoWReKvD+c/t5pkOmfd+UCIAyMwnMExABku549pR/3RBB/WfYjSwCUNN3VlxN8f
uPPTv89tGW+kZ2WO2o4cUsd2vM2du9eFYhGEsY0/KpUUS17IsmeW+EKUPWzsopv5
hlR6DXW/nj2bYrYp5A81hP8kk2sco8hIrKDqInHF6UhQDUhcYmFcsKOmJFkC+xVR
qQhFtB3o2CuNNiC/NNw1WRVJKPv5gS0QI0tzLvukLiL7uiyrHYP80ExHWSy+/+1n
bI3yjBaZc+bkJTz0jDemDSap+vT3x56dip2x+SBMfrgOxVuf2j3ex/y/udSvAseS
x3e9PmyNRTca6x2DZhcbAwlT8kZwJtjN0GCk8FoAYXmJuPD2XXaDWauYU2Tx1ixb
6OCol0OfThXxcx0Ai5MSC8QMVIsN/1Zuyd14C+N4Z9mcZJcghH3gCaWodHA3lgQk
TiVyhs7JHt0b/pemXrmRfzzVl3hgP9FgmIYV/YkDwdRbS9R3wuHYJ46RMUpKhHv5
LK+fem163RuNthF7Cc+nrOczdflrv6G6dR08nQlIAMMvfN0Rr6QnnC8sp2A+rAMD
xN2U6JjZVecc/UB7I4Rkin1z83Ta9qPjkXwikGts3BwbaH6IFU5Y80wgqGRSSeIt
aOIXjoH/1AqMEWaKpKzqtkap71r2JB6D9bw6Ke8yrVaiAZHCKaEFXzqwmJr0HnpL
jrHJ2lIu4OewtvDSEWBbbu+RjDc2T9+evbunu0Mtkh9Bb+OriFVyuYbSFhw2pdZc
jdT6lQzA8C+/qsMH2Ln+K6iDXGPGECC3+ASU5m7HscwhAGKJK+SgW1ZWW+ZxRh9s
+lXxDATUzQotlFTxtQWKnU4FO4CIbo2acjTS
-----END CERTIFICATE-----

17.8.1 EADTrust RSA 8192 SubCA For Qualified Certificates 2019 – Legal Person

-----BEGIN CERTIFICATE-----
MIIMdjCCCF6gAwIBAgIJAJmJVFEJM1SBMA0GCSqGSIb3DQEBDQUAMIGcMUIwQAYD
VQQDDDlFQURUcnVzdCBSU0EgODE5MiBSb290IENBIEZvciBRdWFsaWZpZWQgQ2Vy
dGlmaWNhdGVzIDIwMTkxLzAtBgNVBAoMJkV1cm9wZWFuIEFnZW5jeSBvZiBEaWdp
dGFsIFRydXN0LCBTLkwuMQswCQYDVQQGEwJFUzEYMBYGA1UEYQwPVkFURVMtQjg1
NjI2MjQwMB4XDTE5MDYwNjExMjMwMVoXDTM1MDYwMjExMjMwMVowgbExQDA+BgNV
BAMMN0VBRFRydXN0IFJTQSA4MTkyIFN1YkNBIEZvciBRdWFsaWZpZWQgQ2VydGlm
aWNhdGVzIDIwMTkxLzAtBgNVBAoMJkV1cm9wZWFuIEFnZW5jeSBvZiBEaWdpdGFs
IFRydXN0LCBTLkwuMQswCQYDVQQGEwJFUzEYMBYGA1UEYQwPVkFURVMtQjg1NjI2
MjQwMRUwEwYDVQQLDAxMZWdhbCBQZXJzb24wggQiMA0GCSqGSIb3DQEBAQUAA4IE
DwAwggQKAoIEAQC9wXqa6rIiOTC51CZWZ7o0Ct9DqsMnWyxQzymtdI2S43S4Cfdd
EtpUG7/CndjP12gZjHK7JbED+byfEWClqRQAc+ttIptjEBy+wHwkaHKD7qucawjJ
qS0fie2fPhiJwpF/1fsZ4XmSekaw3R0Hl1K0zcMrgdvXeB9BWe0HNFKapcMBxXrv
Ud5h0u610saSkWC51VKxRrfMuR7FWYA7pcHFjDxZnsZhaBQ1J27QGvRdrvrS52L8
8rqdBTLCSKleNjnkORaQ0GQtRqXhxnggFHi7BlQNhuZ84Evhm4nZ3JvjGPGPMBzh
wHiU08sTh4nD3doYymOyn9+DkF7mrXjT1sJaNHPId9in9R0KViurbjUhI1JNBuIu
4zs2pNRWM6GAgx7Pdcv85dPpWF0jGZTFqx8pKJskdrny/CngKMHMDCss7YOjMoqx
5Pwk2nFPxC6PynFmTGAhY09w68SQoRVY2Eh9MBM1CrDnvMj+f17To/RLsukV9uCR
xwX1NfzPxTRqSMXIdm8MZcjoCs2XLXuQSUP4I5zyWlVEpICMzCGV4E6T3Obt2mAC
x+tOx9mDayor0DmWwfE2bbCwNoOtK8S/ZvOVdTPPLF/5h1nNnwhKxe+62UwYBWnY
qAN2YNbUJuFjjmk2uOuYX0AyQACmxJzKPS+ChtzpeI++dlw5/gH2sSm4x28T2ZQK

l13kqKTC0tEHIDo9/b+Zpr7/H69my3Jh14VKSHgcBByjA2anHbnbjSUNCgvcqESC
rQ/KxxHgkQP2RcbRuMaRLNxjWwgeyc9Ohv1+Tdo7mlorNbj53hW6N0LSjEZOiZJo
bThFnP19SvBGCuaF5nT0LuKt2gek0BOkeqcQPhBcPEY9u5cUTMJO0P7wfArzZ60J
tf/hBjLrLKRoCvAkxureCPCb3EF7v0xjrXEYSgXktq4uUBtW0HeUsBrgY/T8mlKI
B9vzlxLT7NdwPsPyoIsQEHeYOOuIe8yQHs/u1Elro32bHEauxqmnmkOKSC4VlinK
OhdrLr9N4K825QewzkPKK0Ki8E5zCOzFVIseas6OHe/e/PHPXhNQyGJpkMyCeYXz
MS6bXfd94pRiKJFBX4Ac+vL9cp2/4/6ycj6WIHphiMoQ2aHM4On8jKI1xSvPw+aX
bRFAsHzq1B7DHJCzgv4S6U1VJgZJjYjlcQBbbPwfhKY8Ibz5GhuLDsfj7HoE1FoS
ivv7BOAp8pdYmhU+MeQZ1jQTB0GtuhyGc5pJIdnnvKvyxDoNAVN9+wIXYSnDwwgY
jNKa41PP8IwaEkMkyP60guJaZWZsIP8Xh/T+CLWWAMVfgHjhIAaxD13wvE4X18QG
lVGf2o4QEZnWb21AzUFJlyJJ4zs3i046aXETAgMBAAGjggKiMIICnjCBqAYDVR0g
BIGgMIGdMAYGBFUdIAAwgZIGDSsGAQQBg3UCAQEBgxEwgYAwJQYIKwYBBQUHAgEW
GWh0dHA6Ly9wb2xpY3kuZWFkdHJ1c3QuZXUwVwYIKwYBBQUHAgIwSwxJU3Vib3Jk
aW5hdGUgQ2VydGlmaWNhdGUgQXV0aG9yaXR5LiBFdXJvcGVhbiBBZ2VuY3kgb2Yg
RGlnaXRhbCBUcnVzdCwgUy5MLjASBgNVHRMBAf8ECDAGAQH/AgEAMA4GA1UdDwEB
/wQEAwIBhjAdBgNVHQ4EFgQUjEij9L8KVkDKzpNdej0m2BSUps8wYwYDVR0SBFww
WoEOY2FAZWFkdHJ1c3QuZXWGFmh0dHA6Ly93d3cuZWFkdHJ1c3QuZXWGFWh0dHA6
Ly9jYS5lYWR0cnVzdC5ldYYZaHR0cDovL3BvbGljeS5lYWR0cnVzdC5ldTBjBgNV
HREEXDBagQ5jYUBlYWR0cnVzdC5ldYYWaHR0cDovL3d3dy5lYWR0cnVzdC5ldYYV
aHR0cDovL2NhLmVhZHRydXN0LmV1hhlodHRwOi8vcG9saWN5LmVhZHRydXN0LmV1
MB8GA1UdIwQYMBaAFAbmc9lROUCn0VeMNn/H7dB53ffLMEkGA1UdHwRCMEAwPqA8
oDqGOGh0dHA6Ly9jcmwuZWFkdHJ1c3QuZXUvZWFkdHJ1c3Qtcm9vdC1yc2E4MTky
ZWFkcTIwMTkuY3JsMHgGCCsGAQUFBwEBBGwwajBDBggrBgEFBQcwAoY3aHR0cDov
L2NhLmVhZHRydXN0LmV1L2VhZHRydXN0LXJvb3QtcnNhODE5MmVhZHEyMDE5LmNy
dDAjBggrBgEFBQcwAYYXaHR0cDovL29jc3AuZWFkdHJ1c3QuZXUwDQYJKoZIhvcN
AQENBQADggQBALUKGYkyYwhrLkXj1rsoSmnNWd5GlzOS2j2H7i4/4mu1qExONAed
UXXM0PHiXkmAehuXNzMRkXsFvRw0Po3F7Ol+Wn/fJ53vQnrVMKrk0xdpyuXZ9tkm
0J2Po/VJ0I0+cPn8TD9MSC/ITt9O5UMCE+Ct0Ene9g9nFSaPL4Y5b6IVyUPV9Eec
GNpYjpRMnf9bBH+lC5+oxpAVCmoT4GqHkDPrvYbdbGX6TQ5GXv4UnQVImN0mNgGE
6uhDeG6zn8HhgIFkpvsPRBRfDSKnmvjXg0HPBsVUUjUMFboGy0J9ZHyKhv+/260D
89Gmj4CwmI7mdHP04pCDMrIcKYHsH4FvLQP3Wp2uVwWWvA3A6eDPcsVXFdFEOZrj
itmsArWNpAjUlkfj+DpYRAeYh6wsWM7mzVbp1Taf2vz1RKsqkphKnuGaD8jtzUx4
9YV/9+IHnAICuX1z483f8R4n94Mz2hJingUvGZxopY811ypASJ/2gQ7l/3Dut7Ez
kCOTXNcSjcV8hFVuSFMR9+dMdBz1TX1dHvw8BtwEhGkvtGHkdMIX+2AKw3Nan89f
ZPK1r8n0oRaFufiE7uRAMSDmPVISThyWds81K0NX04j7im47wpS41VOIGvXHWYNR
N24y+jSkqtCtFbxryFXsaQKVNm77zwjSm+zTvPBJVo2JLX7itPxo9vYCDyLtMR6o
boF4GYYV1YdSqJRdRoMMApRjdHhOwGkUZ9GgDqvRElFIDa85kf+eOuiXKFUt9eTH
tg5HLLhUrplq+G2GIYIi8XV0IoZpUOQnf3zSufQr/0OUduTaKsybDBntiYjQUriM
17zlj6QPG7h3MGkF6sdLGlMFE8KeUosIEKJyvcDtHDuvJv4CuqNEZuR6pP8T29xv
I+JcTBcb8boPKioo2f0tLUOf2SpT+hNnBVrPwKetZyFZPAkxwhYrX/z7DyVK95s+
vzoWH/tmNSDfH97wdTOONfQfgR80B2RpZ6bpN5TCxX2IKyKdA4DpPk3nV15Z3oG9
MfYFMYb18ZsQedpZYPnKrSRjtG+ZnRYLiY7H/4nRX1ciL25pVQu6hbvFgQ3sHXQK
GXeatTxCJLRvFMduDST9henlgkol9UQIcu4/vT3R87f1/sWX9IB7KVIApInVKaE9
8xm9o2FQBROiyFeLfsKyLOLXA0e1BKOu2BOepOeDpX7dr4EhF4806m8Eu7qh4eNu
Q8xyuXu9pD9+3TH8czvN4WJVq466BYE/NlCWPxTcB1oqx56NlvGGgnT4LZVMhHb8
BkSBlNeGmEXAia+lauABuYZNE+OcVDh3TjiSZi1GU0auCzbilwp/Zr1xM+VPaG1A
WoWcVv7rQ+bAVw78nULnJQNPRIoK9gkvZOA=
-----END CERTIFICATE-----



17.8.1 EADTrust ECC 256 Root CA For Qualified Certificates 2019

Sha256: DD6E8746ED97DFECF6A7244B37DB4BDD0588C1F6242151152E5C0DF1D0BB2574

```
-----BEGIN CERTIFICATE-----
MIIC2TCCAn+gAwIBAgIIVIg0cUCCeFAwCgYIKoZIzj0EAwIwgZsxQTA/BgNVBAMM
OEVBRFRydXN0IEVDQyAyNTYgUm9vdCBDQSBGb3IgUXVhbGlmaWVkIENlcnRpZmlj
YXRlcyAyMDE5MS8wLQYDVQQKDCZFdXJvcGVhbiBBZ2VuY3kgb2YgRGlnaXRhbCBU
cnVzdCwgUy5MLjELMAkGA1UEBhMCRVMxGDAWBgNVBGEMD1ZBVEVTLUI4NTYyNjI0
MDAgFw0xOTA2MDYxMTIzMTFaGA8yMDUxMDUyOTExMjMxMVowgZsxQTA/BgNVBAMM
OEVBRFRydXN0IEVDQyAyNTYgUm9vdCBDQSBGb3IgUXVhbGlmaWVkIENlcnRpZmlj
YXRlcyAyMDE5MS8wLQYDVQQKDCZFdXJvcGVhbiBBZ2VuY3kgb2YgRGlnaXRhbCBU
cnVzdCwgUy5MLjELMAkGA1UEBhMCRVMxGDAWBgNVBGEMD1ZBVEVTLUI4NTYyNjI0
MDBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABCmRZ006jBfLIwycHIDiBAMTbiue
EHu7uBeWLfSEFE1OSrhSAYShQgX9Z5BxGXnIXblTlrjdmRYTvgYzDzy1s3yjgagw
gaUwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwYwYDVR0RBFwwWoEO
Y2FAZWFkdHJ1c3QuZXWGFmh0dHA6Ly93d3cuZWFkdHJ1c3QuZXWGFWh0dHA6Ly9j
YS5lYWR0cnVzdC5ldYYZaHR0cDovL3BvbGljeS5lYWR0cnVzdC5ldTAdBgNVHQ4E
FgQUAWeahMSZxoHtPFgEdK8ko9deQQ0wCgYIKoZIzj0EAwIDSAAwRQIgDt6bdlhA
NUyIgWUbwq7b7Dsq8/aGGpr3n96x4fwZdLUCIQCJEPIqtElTsfjc0kc8fW5/LVZ+
ZTomWaLy4q7/TaBxkA==
-----END CERTIFICATE-----
```

17.8.2 EADTrust ECC 256 SubCA For Qualified Certificates 2019 – Natural Person

Sha256: E5F78053300C169D79A7FB387361AD2A8D1A9BB750B9183C7BB19734D542F07C

```
-----BEGIN CERTIFICATE-----
MIIE5zCCBI2gAwIBAgIIRXRDCCFQI5gwCgYIKoZIzj0EAwIwgZsxQTA/BgNVBAMM
OEVBRFRydXN0IEVDQyAyNTYgUm9vdCBDQSBGb3IgUXVhbGlmaWVkIENlcnRpZmlj
```

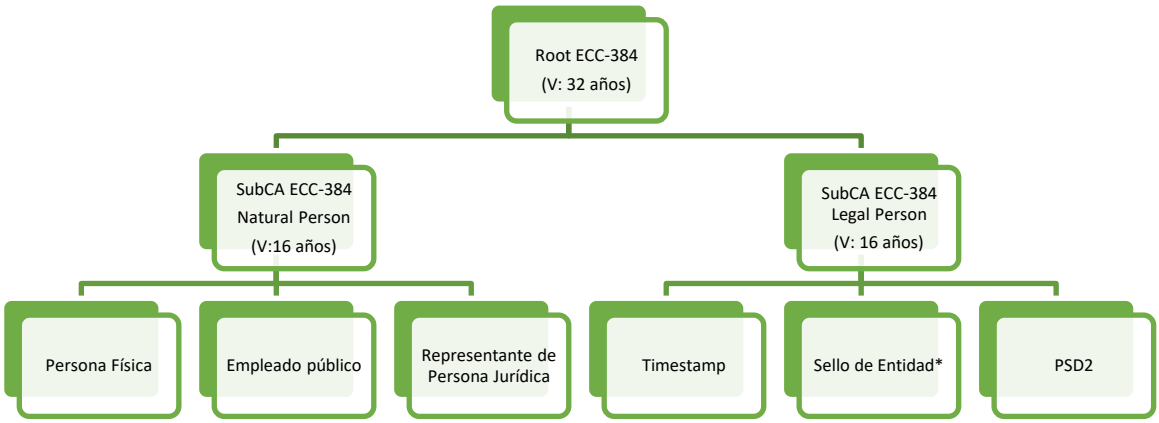
YXRlcyAyMDE5MS8wLQYDVQQKDCZFdXJvcGVhbiBBZ2VuY3kgb2YgRGlnaXRhbCBU
cnVzdCwgUy5MLjELMAkGA1UEBhMCRVMxGDAWBgNVBGEMD1ZBVEVTLUI4NTYyNjI0
MDAeFw0xOTA2MDYxMTIzMTJaFw0zNTA2MDIxMTIzMTJaMIGyMT8wPQYDVQQDDDZF
QURUcnVzdCBFQ0MgMjU2IFN1YkNBIEZvciBRdWFsaWZpZWQgQ2VydGlmaWNhdGVz
IDIwMTkxLzAtBgNVBAoMJkV1cm9wZWFuIEFnZW5jeSBvZiBEaWdpdGFsIFRydXN0
LCBTLkwuMQswCQYDVQQGEwJFUzEYMBYGA1UEYQwPVkFURVMtQjg1NjI2MjQwMRcw
FQYDVQQLDA5OYXR1cmFsIFBlcnNvbjBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IA
BIvhQDKEvOGURiGfC4WgrptHxeQsvHdo1lcoQtGO/ElyWoYx0vS6mIb9KUePFb5s
3bvFuNbDyyIFO0PM5lF3yOijggKgMIICnDCBqAYDVR0gBIGgMIGdMAYGBFUdIAAw
gZIGDSsGAQQBg3UCAQEBgxEwgYAwJQYIKwYBBQUHAgEWGWh0dHA6Ly9wb2xpY3ku
ZWFkdHJ1c3QuZXUwVwYIKwYBBQUHAgIwSwxJU3Vib3JkaW5hdGUgQ2VydGlmaWNh
dGUgQXV0aG9yaXR5LiBFdXJvcGVhbiBBZ2VuY3kgb2YgRGlnaXRhbCBUcnVzdCwg
Uy5MLjASBgNVHRMBAf8ECDAGAQH/AgEAMA4GA1UdDwEB/wQEAwIBhjAdBgNVHQ4E
FgQUw+LbEe82PGqASYsjRo07pzNrmQwwYwYDVR0SBFwwWoEOY2FAZWFkdHJ1c3Qu
ZXWGFmh0dHA6Ly93d3cuZWFkdHJ1c3QuZXWGFWh0dHA6Ly9jYS5lYWR0cnVzdC5l
dYYZaHR0cDovL3BvbGljeS5lYWR0cnVzdC5ldTBjBgNVHREEXDBagQ5jYUBlYWR0
cnVzdC5ldYYWaHR0cDovL3d3dy5lYWR0cnVzdC5ldYYVaHR0cDovL2NhLmVhZHRy
dXN0LmV1hhlodHRwOi8vcG9saWN5LmVhZHRydXN0LmV1MB8GA1UdIwQYMBaAFAFn
moTEmcaB7TxYBHSvJKPXXkENMEgGA1UdHwRBMD8wPaA7oDmGN2h0dHA6Ly9jcmwu
ZWFkdHJ1c3QuZXUvZWFkdHJ1c3Qtcm9vdC1lY2MyNTZlYWRxMjAxOS5jcmwwdwYI
KwYBBQUHAQEEazBpMEIGCCsGAQUFBzAChjZodHRwOi8vY2EuZWFkdHJ1c3QuZXUv
ZWFkdHJ1c3Qtcm9vdC1lY2MyNTZlYWRxMjAxOS5jcnQwIwYIKwYBBQUHMAGGF2h0
dHA6Ly9vY3NwLmVhZHRydXN0LmV1MAoGCCqGSM49BAMCA0gAMEUCIGp+6oK32Jsu
+fGmgaszbcsuhvgItZIGHNWQxtX44SN2AiEAjj8rAaWdPjX9KPDsCIjTyNY0UeE3
heqjNssNsXJzCVY=
-----END CERTIFICATE-----

17.8.1 EADTrust ECC 256 SubCA For Qualified Certificates 2019 – Legal Person

Sha256: 360993593406E5AA311663EDFF5A3409A8DD1E30708C9CABE34EFD8E5392733D

-----BEGIN CERTIFICATE-----
MIIE5jCCBIugAwIBAgIIBJeJkUGCQIMwCgYIKoZIzj0EAwIwgZsxQTA/BgNVBAMM
OEVBRFRydXN0IEVDQyAyNTYgUm9vdCBDQSBGb3IgUXVhbGlmaWVkIENlcnRpZmlj
YXRlcyAyMDE5MS8wLQYDVQQKDCZFdXJvcGVhbiBBZ2VuY3kgb2YgRGlnaXRhbCBU
cnVzdCwgUy5MLjELMAkGA1UEBhMCRVMxGDAWBgNVBGEMD1ZBVEVTLUI4NTYyNjI0
MDAeFw0xOTA2MDYxMTIzMTJaFw0zNTA2MDIxMTIzMTJaMIGwMT8wPQYDVQQDDDZF
QURUcnVzdCBFQ0MgMjU2IFN1YkNBIEZvciBRdWFsaWZpZWQgQ2VydGlmaWNhdGVz
IDIwMTkxLzAtBgNVBAoMJkV1cm9wZWFuIEFnZW5jeSBvZiBEaWdpdGFsIFRydXN0
LCBTLkwuMQswCQYDVQQGEwJFUzEYMBYGA1UEYQwPVkFURVMtQjg1NjI2MjQwMRUw
EwYDVQQLDAxMZWdhbCBQZXJzb24wWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATW
uOl18JPJcTxF2ttbytstqBRGYZB6sMGqHRYRpEJommoO6orLRmzV9cGFI8lDjffh
fRN0wBYEigucsELa6n0uo4ICoDCCApwwgagGA1UdIASBoDCBnTAGBgRVHSAAMIGS
Bg0rBgEEAYN1AgEBAYMRMIGAMCUGCCsGAQUFBwIBFhlodHRwOi8vcG9saWN5LmVh
ZHRydXN0LmV1MFcGCCsGAQUFBwICMEsMSVN1Ym9yZGluYXRlIENlcnRpZmljYXRl
IEF1dGhvcml0eS4gRXVyb3BlYW4gQWdlbmN5IG9mIERpZ2l0YWwgVHJ1c3QsIFMu
TC4wEgYDVR0TAQH/BAgwBgEB/wIBADAOBgNVHQ8BAf8EBAMCAYYwHQYDVR0OBBYE
FNNMbDq9Nv5whyOHOu49kM/Lm/chMGMGA1UdEgRcMFqBDmNhQGVhZHRydXN0LmV1
hhZodHRwOi8vd3d3LmVhZHRydXN0LmV1hhVodHRwOi8vY2EuZWFkdHJ1c3QuZXWG

GWh0dHA6Ly9wb2xpY3kuZWFkdHJ1c3QuZXUwYwYDVR0RBFwwWoEOY2FAZWFkdHJ1
c3QuZXWGFmh0dHA6Ly93d3cuZWFkdHJ1c3QuZXWGFWh0dHA6Ly9jYS5lYWR0cnVz
dC5ldYYZaHR0cDovL3BvbGljeS5lYWR0cnVzdC5ldTAfBgNVHSMEGDAWgBQBZ5qE
xJnGge08WAR0rySj115BDTBIBgNVHR8EQTA/MD2gO6A5hjdodHRwOi8vY3JsLmVh
ZHRydXN0LmV1L2VhZHRydXN0LXJvb3QtZWNjMjU2ZWFkcTIwMTkuY3JsMHcGCCsG
AQUFBwEBBGswaTBCBggrBgEFBQcwAoY2aHR0cDovL2NhLmVhZHRydXN0LmV1L2Vh
ZHRydXN0LXJvb3QtZWNjMjU2ZWFkcTIwMTkuY3J0MCMGCCsGAQUFBzABhhdodHRw
Oi8vb2NzcC5lYWR0cnVzdC5ldTAKBggqhkjOPQQDAgNJADBGAiEAo3kjVg5x0Nx2
Vl5H86QV1mB0g4miZn1xrt7SQV+8ggUCIQCOjpmf3+3shoTYYNZkUlv0aWfjV//5
lps4eXGPqoaeaQ==
-----END CERTIFICATE-----



17.8.1 EADTrust ECC 384 Root CA For Qualified Certificates 2019

-----BEGIN CERTIFICATE-----
MIIDFzCCApygAwIBAgIIJ5cWUAlhiIgwCgYIKoZIzj0EAwMwgZsxQTA/BgNVBAMM
OEVBRFRydXN0IEVDQyAzODQgUm9vdCBDQSBGb3IgUXVhbGlmaWVkIENlcnRpZmlj
YXRlcyAyMDE5MS8wLQYDVQQKDCZFdXJvcGVhbiBBZ2VuY3kgb2YgRGlnaXRhbCBU
cnVzdCwgUy5MLjELMAkGA1UEBhMCRVMxGDAWBgNVBGEMD1ZBVEVTLUI4NTYyNjI0
MDAgFw0xOTA2MDYxMTIzMTVaGA8yMDUxMDUyOTExMjMxNVowgZsxQTA/BgNVBAMM
OEVBRFRydXN0IEVDQyAzODQgUm9vdCBDQSBGb3IgUXVhbGlmaWVkIENlcnRpZmlj
YXRlcyAyMDE5MS8wLQYDVQQKDCZFdXJvcGVhbiBBZ2VuY3kgb2YgRGlnaXRhbCBU
cnVzdCwgUy5MLjELMAkGA1UEBhMCRVMxGDAWBgNVBGEMD1ZBVEVTLUI4NTYyNjI0
MDB2MBAGByqGSM49AgEGBSuBBAAiA2IABJpUpFLZZZkWHv7hxNgamqv9qlL4uZZc
/TFfnrnJEBoXssZyad/kLD+906Watn5F8e5PhwufanG6wTMd4SEuPH9vC8xmb1+m
aKUtEJBgF9pl6qlRdM8Sg+9oHlulZz73jaOBqDCBpTAPBgNVHRMBAf8EBTADAQH/
MA4GA1UdDwEB/wQEAwIBBjBjBgNVHREEXDBagQ5jYUBlYWR0cnVzdC5ldYYWaHR0
cDovL3d3dy5lYWR0cnVzdC5ldYYVaHR0cDovL2NhLmVhZHRydXN0LmV1hhlodHRw
Oi8vcG9saWN5LmVhZHRydXN0LmV1MB0GA1UdDgQWBBR4FP3u0QlgXHWnZ24mSIHk
6sSSATAKBggqhkjOPQQDAwNpADBmAjEApeqkkNMGW8neYsXLzPy2XytMX9Jf7oxN
Z7I1oonC4XXl0cDVsW5u4KP02+CO0/trAjEA29yWuzRywABtXZlVisrvsSJAhFvC
E/WD7KUyKb4inlL9R7ssEt6VrzpYdqDLyiqn
-----END CERTIFICATE-----

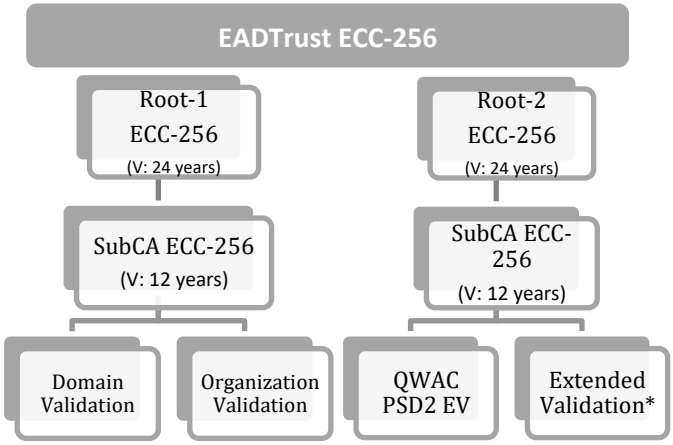
17.8.1 EADTrust ECC 384 SubCA For Qualified Certificates 2019 – Natural Person


```
-----BEGIN CERTIFICATE-----
MIIFJDCCBKugAwIBAgIJAJA2BpFoYohBMAoGCCqGSM49BAMDMIGbMUEwPwYDVQQD
DDhFQURUcnVzdCBFQ0MgMzg0IFJvb3QgQ0EgRm9yIFF1YWxpZmllZCBDZXJ0aWZp
Y2F0ZXMgMjAxOTEvMC0GA1UECgwmRXVyb3BlYW4gQWdlbmN5IG9mIERpZ2l0YWwg
VHJ1c3QsIFMuTC4xCzAJBgNVBAYTAkVTMRgwFgYDVQRhDA9WQVRFUy1CODU2MjYy
NDAwHhcNMTkwNjA2MTEyMzE2WhcNMzUwNjAyMTEyMzE2WjCBsjE/MD0GA1UEAww2
RUFEVHJ1c3QgRUNDIDM4NCBTdWJDQSBGb3IgUXVhbGlmaWVkIENlcnRpZmljYXRl
cyAyMDE5MS8wLQYDVQQKDCZFdXJvcGVhbiBBZ2VuY3kgb2YgRGlnaXRhbCBUcnVz
dCwgUy5MLjELMAkGA1UEBhMCRVMxGDAWBgNVBGEMD1ZBVEVTLUI4NTYyNjI0MDEX
MBUGA1UECwwOTmF0dXJhbCBQZXJzb24wdjAQBgcqhkjOPQIBBgUrgQQAIgNiAATZ
zrGktCAEuUZV2ZqHDfb7uiaQRwTpzALrdQHT4DHCAuTGINfLIOdodPkktVdMaVMb
ZmDzOBHfD2uJs1xEI6v4ztnSXh3Ib0nK7/0DNjtK1gfF8BpRgQsbwLP1Vm42mD6j
ggKgMIICnDCBqAYDVR0gBIGgMIGdMAYGBFUdIAAwgZIGDSsGAQQBg3UCAQEBgxEw
gYAwJQYIKwYBBQUHAgEWGWh0dHA6Ly9wb2xpY3kuZWFkdHJ1c3QuZXUwVwYIKwYB
BQUHAgIwSwxJU3Vib3JkaW5hdGUgQ2VydGlmaWNhdGUgQXV0aG9yaXR5LiBFdXJv
cGVhbiBBZ2VuY3kgb2YgRGlnaXRhbCBUcnVzdCwgUy5MLjASBgNVHRMBAf8ECDAG
AQH/AgEAMA4GA1UdDwEB/wQEAwIBhjAdBgNVHQ4EFgQUj7roZnJ0IkzMJ4lICDFz
Cx6bS4IwYwYDVR0SBFwwWoEOY2FAZWFkdHJ1c3QuZXWGFmh0dHA6Ly93d3cuZWFk
dHJ1c3QuZXWGFWh0dHA6Ly9jYS5lYWR0cnVzdC5ldYYZaHR0cDovL3BvbGljeS5l
YWR0cnVzdC5ldTBjBgNVHREEXDBagQ5jYUBlYWR0cnVzdC5ldYYWaHR0cDovL3d3
dy5lYWR0cnVzdC5ldYYVaHR0cDovL2NhLmVhZHRydXN0LmV1hhlodHRwOi8vcG9s
aWN5LmVhZHRydXN0LmV1MB8GA1UdIwQYMBaAFHgU/e7RCWBcdadnbiZIgeTqxJIB
MEgGA1UdHwRBMD8wPaA7oDmGN2h0dHA6Ly9jcmwuZWFkdHJ1c3QuZXUvZWFkdHJ1
c3Qtcm9vdC1lY2MzODRlYWRxMjAxOS5jcmwwdwYIKwYBBQUHAQEEazBpMEIGCCsG
AQUFBzAChjZodHRwOi8vY2EuZWFkdHJ1c3QuZXUvZWFkdHJ1c3Qtcm9vdC1lY2Mz
ODRlYWRxMjAxOS5jcnQwIwYIKwYBBQUHMAGGF2h0dHA6Ly9vY3NwLmVhZHRydXN0
LmV1MAoGCCqGSM49BAMDA2cAMGQCMH6hKBIXDD6FtWe0lgEKCo+eqz91aZCzIf6t
W7kWgBB6nXAR/iwpO52l3d7uDzP9SAIwf/zs2GCNsqLLLTaFiuk/pVy69WAhNqUd
/mL7Qh36ObWETT46WU/q5PbcJlRDbMmC
-----END CERTIFICATE-----
```


17.8.1 EADTrust ECC 384 SubCA For Qualified Certificates 2019 – Legal Person


```
-----BEGIN CERTIFICATE-----
MIIFIjCCBKigAwIBAgIIWCYiWAgIdgEwCgYIKoZIzj0EAwMwgZsxQTA/BgNVBAMM
OEVBRFRydXN0IEVDQyAzODQgUm9vdCBDQSBGb3IgUXVhbGlmaWVkIENlcnRpZmlj
YXRlcyAyMDE5MS8wLQYDVQQKDCZFdXJvcGVhbiBBZ2VuY3kgb2YgRGlnaXRhbCBU
cnVzdCwgUy5MLjELMAkGA1UEBhMCRVMxGDAWBgNVBGEMD1ZBVEVTLUI4NTYyNjI0
MDAeFw0xOTA2MDYxMTIzMTZaFw0zNTA2MDIxMTIzMTZaMIGwMT8wPQYDVQQDDDZF
QURUcnVzdCBFQ0MgMzg0IFN1YkNBIEZvciBRdWFsaWZpZWQgQ2VydGlmaWNhdGVz
IDIwMTkxLzAtBgNVBAoMJkV1cm9wZWFuIEFnZW5jeSBvZiBEaWdpdGFsIFRydXN0
LCBTLkwuMQswCQYDVQQGEwJFUzEYMBYGA1UEYQwPVkFURVMtQjg1NjI2MjQwMRUw
EwYDVQQLDAxMZWdhbCBQZXJzb24wdjAQBgcqhkjOPQIBBgUrgQQAIgNiAAT16y8u
3RP+c73LiVVIx3fsNqxqYmu7Xj2TxDNQhibTh64f+OfQB2HmmPcavFeYhdks6LmP
qt+kgY30W9A43fVSfjyBBqVDrNnaqJyYkfHEe4q6lNZETLCAZUu6inZDqWajggKg
MIICnDCBqAYDVR0gBIGgMIGdMAYGBFUdIAAwgZIGDSsGAQQBg3UCAQEBgxEwgYAw
JQYIKwYBBQUHAgEWGWh0dHA6Ly9wb2xpY3kuZWFkdHJ1c3QuZXUwVwYIKwYBBQUH
```

AgIwSwxJU3Vib3JkaW5hdGUgQ2VydGlmaWNhdGUgQXV0aG9yaXR5LiBFdXJvcGVh
biBBZ2VuY3kgb2YgRGlnaXRhbCBUcnVzdCwgUy5MLjASBgNVHRMBAf8ECDAGAQH/
AgEAMA4GA1UdDwEB/wQEAwIBhjAdBgNVHQ4EFgQUXBniqx22uD1FEpGSG4wUcdjo
9fYwYwYDVR0SBFwwWoEOY2FAZWFkdHJ1c3QuZXWGFmh0dHA6Ly93d3cuZWFkdHJ1
c3QuZXWGFWh0dHA6Ly9jYS5lYWR0cnVzdC5ldYYZaHR0cDovL3BvbGljeS5lYWR0
cnVzdC5ldTBjBgNVHREEXDBagQ5jYUBlYWR0cnVzdC5ldYYWaHR0cDovL3d3dy5l
YWR0cnVzdC5ldYYVaHR0cDovL2NhLmVhZHRydXN0LmV1hhlodHRwOi8vcG9saWN5
LmVhZHRydXN0LmV1MB8GA1UdIwQYMBaAFHgU/e7RCWBcdadnbiZIgeTqxJIBMEgG
A1UdHwRBMD8wPaA7oDmGN2h0dHA6Ly9jcmwuZWFkdHJ1c3QuZXUvZWFkdHJ1c3Qt
cm9vdC1lY2MzODRlYWRxMjAxOS5jcmwwdwYIKwYBBQUHAQEEazBpMEIGCCsGAQUF
BzAChjZodHRwOi8vY2EuZWFkdHJ1c3QuZXUvZWFkdHJ1c3Qtcm9vdC1lY2MzODRl
YWRxMjAxOS5jcnQwIwYIKwYBBQUHMAGGF2h0dHA6Ly9vY3NwLmVhZHRydXN0LmV1
MAoGCCqGSM49BAMDA2gAMGUCMDqqc9gguSfkl51ohpQPBevyklWcm1FLTwsO8r5g
KccXtsVJ6W3Z1QnCGCsfYzyF8wIxAIHxWbeFz94DJo4mv53RLthhFkLdLMnPtdeC
6FFHuJFMZwTsJDFZotTF2D/y7gLUbQ==
-----END CERTIFICATE-----



17.8.2 EADTrust ECC 256 Root CA For Qualified Web DV/OV Cert 2019

-----BEGIN CERTIFICATE-----
MIICQDCCAeagAwIBAgIIUgcyMxmBF3kwCgYIKoZIzj0EAwIwgYMxQzBBBgNVBAMM
OkVBRFRydXN0IEVDQyAyNTYgUm9vdCBDQSBGb3IgUXVhbGlmaWVkIFdlYiBEVi9P
ViBDZXJ0IDIwMTkxLzAtBgNVBAoMJkV1cm9wZWFuIEFnZW5jeSBvZiBEaWdpdGFs
IFRydXN0LCBTLkwuMQswCQYDVQQGEwJFUzAeFw0xOTA2MDYxMTM1NTJaFw00MzA1
MzExMTM1NTJaMIGDMUMwQQYDVQQDDDpFQURUcnVzdCBFQ0MgMjU2IFJvb3QgQ0Eg
Rm9yIFF1YWxpZmllZCBXZWIgRFYvT1YgQ2VydCAyMDE5MS8wLQYDVQQKDCZFdXJv
cGVhbiBBZ2VuY3kgb2YgRGlnaXRhbCBUcnVzdCwgUy5MLjELMAkGA1UEBhMCRVMw
WTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASmsvUbOfnnKs3E/Ax/DsRZeCTWd/sE
MrM/afOWgFWh30mNWFmhNEZvT6sICq42qRM35y/aVbTZRdrf9bxu6v+po0IwQDAP
BgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBBjAdBgNVHQ4EFgQUvCvHW+Nq
2n3RqEatR97jRcDD/bIwCgYIKoZIzj0EAwIDSAAwRQIgecIKoOw2jGf3xLbnBLXd
NCvlE5yqXefogNF10FlSTkECIQC+5T1TjlQl4BKUk4QFehy4B96aDIH5WoVV+Fbu
dcOIFA==
-----END CERTIFICATE-----

17.8.1 EADTrust ECC 256 SubCA For Qualified Web DV/OV Cert 2019

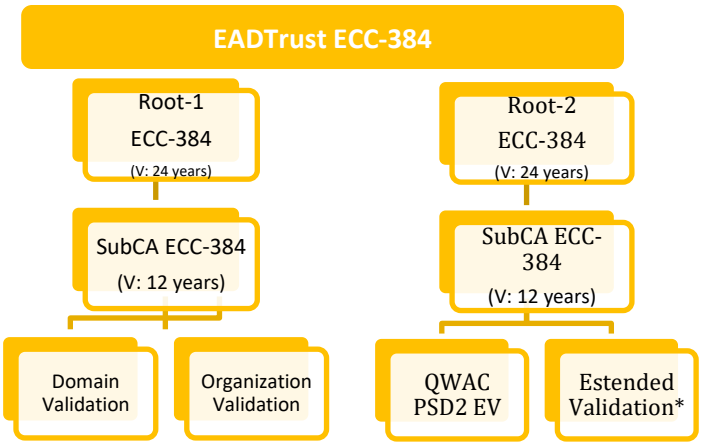

```
-----BEGIN CERTIFICATE-----
MIIDnDCCA0GgAwIBAgIIEXWHRlgglDkwCgYIKoZIzj0EAwIwgYMxQzBBBgNVBAMM
OkVBRFRydXN0IEVDQyAyNTYgUm9vdCBDQSBGb3IgUXVhbGlmaWVkIFdlYiBEVi9P
ViBDZXJ0IDIwMTkxLzAtBgNVBAoMJkV1cm9wZWFuIEFnZW5jeSBvZiBEaWdpdGFs
IFRydXN0LCBTLkwuMQswCQYDVQQGEwJFUzAeFw0xOTA2MDYxMTM1NTJaFw0zMTA2
MDMxMTM1NTJaMIGBMUEwPwYDVQQDDDhFQURUcnVzdCBFQ0MgMjU2IFN1YkNBIEZv
ciBRdWFsaWZpZWQgV2ViIERWL09WIENlcnQgMjAxOTEvMC0GA1UECgwmRXVyb3Bl
YW4gQWdlbmN5IG9mIERpZ2l0YWwgVHJ1c3QsIFMuTC4xCzAJBgNVBAYTAkVTMFkw
EwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEQmqP2YJyJACaPj9Mu1FeH2UTDK5U6zrX
oPr/+1cA0VayagC9JFB02g/xej3X9tv55c9V8iUfw5LA70VoFbNMjaOCAZ0wggGZ
MEsGA1UdIAREMEIwBgYEVR0gADA4Bg0rBgEEAYN1AgEBAYMRMCcwJQYIKwYBBQUH
AgEWGWh0dHA6Ly9wb2xpY3kuZWFkdHJ1c3QuZXUwEgYDVR0TAQH/BAgwBgEB/wIB
ADAOBgNVHQ8BAf8EBAMCAYYwHQYDVR0OBBYEFOCbgvBLf7ZoiOqft6Av/hWlrJVk
MB8GA1UdIwQYMBaAFLwrx1vjatp90ahGrUfe40XAw/2yMEsGA1UdHwREMEIwQKA+
oDyGOmh0dHA6Ly9jcmwuZWFkdHJ1c3QuZXUvZWFkdHJ1c3Qtcm9vdC1lY2MyNTZl
YWRkdm92MjAxOS5jcmwwegYIKwYBBQUHAQEEbjBsMEUGCCsGAQUFBzAChjlodHRw
Oi8vY2EuZWFkdHJ1c3QuZXUvZWFkdHJ1c3Qtcm9vdC1lY2MyNTZlYWRkdm92MjAx
OS5jcnQwIwYIKwYBBQUHMAGGF2h0dHA6Ly9vY3NwLmVhZHRydXN0LmV1MB0GA1Ud
JQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjAKBggqhkjOPQQDAgNJADBGAiEA+xsp
1y3d0b/kLk+9bqHxlTXznZQSSjYmiBQCpv8kabsCIQCaLjx5plNhyGTWMRoaSNw0
fSAkivbPUopn53pcCu8Cjg==
-----END CERTIFICATE-----
```


17.8.2 EADTrust ECC 256 Root CA For Qualified Web EV/PSD2 Cert 2019


```
-----BEGIN CERTIFICATE-----
MIICRDCCAeqgAwIBAgIIImMDVYeTMkgwCgYIKoZIzj0EAwIwgYUxRTBDBgNVBAMM
PEVBRFRydXN0IEVDQyAyNTYgUm9vdCBDQSBGb3IgUXVhbGlmaWVkIFdlYiBFVi9Q
U0QyIENlcnQgMjAxOTEvMC0GA1UECgwmRXVyb3BlYW4gQWdlbmN5IG9mIERpZ2l0
YWwgVHJ1c3QsIFMuTC4xCzAJBgNVBAYTAkVTMB4XDTE5MDYwNjExNDkyNFoXDTQz
MDUzMTExNDkyNFowgYUxRTBDBgNVBAMMPEVBRFRydXN0IEVDQyAyNTYgUm9vdCBD
QSBGb3IgUXVhbGlmaWVkIFdlYiBFVi9QU0QyIENlcnQgMjAxOTEvMC0GA1UECgwm
RXVyb3BlYW4gQWdlbmN5IG9mIERpZ2l0YWwgVHJ1c3QsIFMuTC4xCzAJBgNVBAYT
AkVTMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAE0EISu3kfw9Uasnh4Y7vNtkWG
UvCkCAA45lWFPbvIH668463fRfObNL9jCuRryOAj5ws2/XnVx03P/iEBhCvsNKNC
MEAwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFNN3
zVrao5Nci0pMZdKaDAHVmT8TMAoGCCqGSM49BAMCA0gAMEUCIQDxOmhZS7u3FlKC
tGQDCDs0rzvaW9mO03YP/Y0GSi2JQAIgdwgCgMc42H3u2Apo7uubqUIIY+Ebo3MT
9wwf4X0aTRg=
-----END CERTIFICATE-----
```

17.8.3 EADTrust ECC 256 SubCA For Qualified Web EV/PSD2 Cert 2019


```
-----BEGIN CERTIFICATE-----
MIIDpDCCA0mgAwIBAgIIMiJzWEZDQEQwCgYIKoZIzj0EAwIwgYUxRTBDBgNVBAMM
PEVBRFRydXN0IEVDQyAyNTYgUm9vdCBDQSBGb3IgUXVhbGlmaWVkIFdlYiBFVi9Q
U0QyIENlcnQgMjAxOTEvMC0GA1UECgwmRXVyb3BlYW4gQWdlbmN5IG9mIERpZ2l0
YWwgVHJ1c3QsIFMuTC4xCzAJBgNVBAYTAkVTMB4XDTE5MDYwNjExNDkyNFoXDTMx
MDYwMzExNDkyNFowgYMxQzBBBgNVBAMMOkVBRFRydXN0IEVDQyAyNTYgU3ViQ0Eg
Rm9yIFF1YWxpZmllZCBXZWIgRVYvUFNEMiBDZXJ0IDIwMTkxLzAtBgNVBAoMJkV1
cm9wZWFuIEFnZW5jeSBvZiBEaWdpdGFsIFRydXN0LCBTLkwuMQswCQYDVQQGEwJF
UzBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABCoD0KVinA0yE58PK9jtDhp24ao1
77XI+uEN1ek+PYZhgDZZeD5TkjDrGIC2UchXhw24U1/plMMbZNVVf4KhBzWjggGh
MIIBnTBLBgNVHSAERDBCMAYGBFUdIAAwOAYNKwYBBAGDdQIBAQGDETAnMCUGCCsG
AQUFBwIBFhlodHRwOi8vcG9saWN5LmVhZHRydXN0LmV1MBIGA1UdEwEB/wQIMAYB
Af8CAQAwDgYDVR0PAQH/BAQDAgGGMB0GA1UdDgQWBBQJdR5ZrQBosRSSVUEGb7Nm
MDkgczAfBgNVHSMEGDAWgBTTd81a2qOTXItKTGXSmgwB1Zk/EzBNBgNVHR8ERjBE
MEKgQKA+hjxodHRwOi8vY3JsLmVhZHRydXN0LmV1L2VhZHRydXN0LXJvb3QtZWNj
MjU2ZWFkZXZwc2QyMjAxOS5jcmwwfAYIKwYBBQUHAQEEcDBuMEcGCCsGAQUFBzAC
hjtodHRwOi8vY2EuZWFkdHJ1c3QuZXUvZWFkdHJ1c3Qtcm9vdC1lY2MyNTZlYWRl
dnBzZDIyMDE5LmNydDAjBggrBgEFBQcwAYYXaHR0cDovL29jc3AuZWFkdHJ1c3Qu
ZXUwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMAoGCCqGSM49BAMCA0kA
MEYCIQC26I5aeV5Y/bM0ZDI6w43s7lbd86MlqAvrX8yciDv+6AIhAPPNHzRucILM
LzkpHGqvNFIpa1AzzB3ryo3TE5Af2Lyy
-----END CERTIFICATE-----
```



17.8.4 EADTrust ECC 384 Root CA For Qualified Web DV/OV Cert 2019

```
-----BEGIN CERTIFICATE-----
MIICfjCCAgOgAwIBAgIIQkhkc3QlBBIwCgYIKoZIzj0EAwMwgYMxQzBBBgNVBAMM
OkVBRFRydXN0IEVDQyAzODQgUm9vdCBDQSBGb3IgUXVhbGlmaWVkIFdlYiBEVi9P
ViBDZXJ0IDIwMTkxLzAtBgNVBAoMJkV1cm9wZWFuIEFnZW5jeSBvZiBEaWdpdGFs
IFRydXN0LCBTLkwuMQswCQYDVQQGEwJFUzAeFw0xOTA2MDYxMTM1NTVaFw00MzA1
MzExMTM1NTVaMIGDMUMwQQYDVQQDDDpFQURUcnVzdCBFQ0MgMzg0IFJvb3QgQ0Eg
Rm9yIFF1YWxpZmllZCBXZWIgRFYvT1YgQ2VydCAyMDE5MS8wLQYDVQQKDCZFdXJv
cGVhbiBBZ2VuY3kgb2YgRGlnaXRhbCBUcnVzdCwgUy5MLjELMAkGA1UEBhMCRVMw
djAQBgcqhkjOPQIBBgUrgQQAIgNiAAS7oySQYb7uQT6YONuFW8H+DKiMY3K5eaRE
IRYQiYdfvM52nDrMGI3ne422tQXthT3LNaWK+JYvPiO5S+0tkJnPMVN/FcS2YmOx
aD9E5LUi9yCX+6Iglt8c7rTM/SjEE2ujQjBAMA8GA1UdEwEB/wQFMAMBAf8wDgYD
VR0PAQH/BAQDAgEGMB0GA1UdDgQWBBQclNgSlEl/161Dcbsusroz0sD0RjAKBggq
hkjOPQQDAwNpADBmAjEAu/UWRl5XlmTgSsSmGBkNw4u5i/pXvdDW9pn8dGw4RBie
wb75uu50eH0xxrdv8pInAjEAix9xKDwCNClzYZDGlMFvldSG3PlsJqgJ6pB9kOwV
Ono9W0VX13P+QB9G4ixZ4j0B
-----END CERTIFICATE-----
```

17.8.1 EADTrust ECC 384 SubCA For Qualified Web DV/OV Cert 2019

```
-----BEGIN CERTIFICATE-----
MIID1zCCA16gAwIBAgIIUCAycVlJY2gwCgYIKoZIzj0EAwMwgYMxQzBBBgNVBAMM
OkVBRFRydXN0IEVDQyAzODQgUm9vdCBDQSBGb3IgUXVhbGlmaWVkIFdlYiBEVi9P
ViBDZXJ0IDIwMTkxLzAtBgNVBAoMJkV1cm9wZWFuIEFnZW5jeSBvZiBEaWdpdGFs
IFRydXN0LCBTLkwuMQswCQYDVQQGEwJFUzAeFw0xOTA2MDYxMTM1NTVaFw0zMTA2
MDMxMTM1NTVaMIGBMUEwPwYDVQQDDDhFQURUcnVzdCBFQ0MgMzg0IFN1YkNBIEZv
ciBRdWFsaWZpZWQgV2ViIERWL09WIENlcnQgMjAxOTEvMC0GA1UECgwmRXVyb3Bl
YW4gQWdlbmN5IG9mIERpZ2l0YWwgVHJ1c3QsIFMuTC4xCzAJBgNVBAYTAkVTMHYw
EAYHKoZIzj0CAQYFK4EEACIDYgAE6o4xOzPzH2Ht9WK476vEYj6nkC3GiYomL9YS
Ru0gzdi2oSlm8eZcGEuD7pe0Gd3Y8JL7A1ygRzIUa+TUuftPjB4MfWLz79VcHZCR
```

xtFZrxRuesh4HN61haPqkk7sFSUxo4IBnTCCAZkwSwYDVR0gBEQwQjAGBgRVHSAA
MDgGDSsGAQQBg3UCAQEBgxEwJzAlBggrBgEFBQcCARYZaHR0cDovL3BvbGljeS5l
YWR0cnVzdC5ldTASBgNVHRMBAf8ECDAGAQH/AgEAMA4GA1UdDwEB/wQEAwIBhjAd
BgNVHQ4EFgQUZj/V6yyw0c/kc+YXwGjFc+pv9kowHwYDVR0jBBgwFoAUHJTYEpRJ
f9etQ3G7LrK6M9LA9EYwSwYDVR0fBEQwQjBAoD6gPIY6aHR0cDovL2NybC5lYWR0
cnVzdC5ldS9lYWR0cnVzdC1yb290LWVjYzM4NGVhZGR2b3YyMDE5LmNybDB6Bggr
BgEFBQcBAQRuMGwwRQYIKwYBBQUHMAKGOWh0dHA6Ly9jYS5lYWR0cnVzdC5ldS9l
YWR0cnVzdC1yb290LWVjYzM4NGVhZGR2b3YyMDE5LmNydDAjBggrBgEFBQcwAYYX
aHR0cDovL29jc3AuZWFkdHJ1c3QuZXUwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsG
AQUFBwMCMAoGCCqGSM49BAMDA2cAMGQCMFqnk4zWsC5s5l+6abjGtJHRJBkaGeCJ
zs7CXXWBDFEF3Wci9b1zKCjr2IZb8hkLZAIwRDNBSURcXnoz1GgWrmW/dazQkIc+
VTQ7t15/sSrmczCUUmBTjo5llrCWFbMV/HgS
-----END CERTIFICATE-----

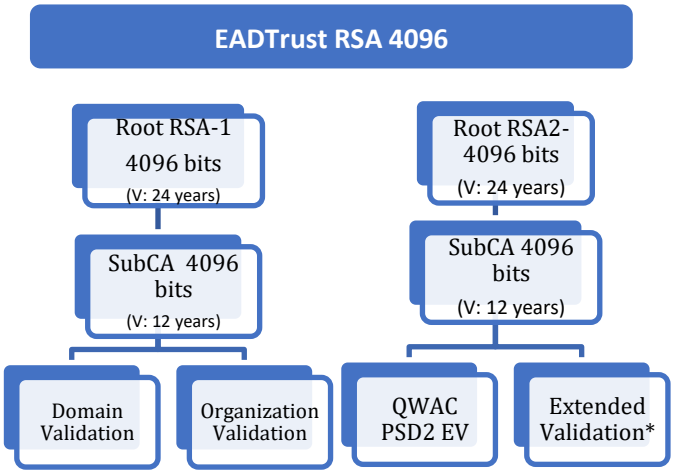
17.8.2 EADTrust ECC 384 Root CA For Qualified Web EV/PSD2 Cert 2019

-----BEGIN CERTIFICATE-----
MIICgTCCAgigAwIBAgIJAJWBAHV3mAKHMAoGCCqGSM49BAMDMIGFMUUwQwYDVQQD
DDxFQURUcnVzdCBFQ0MgMzg0IFJvb3QgQ0EgRm9yIFF1YWxpZmllZCBXZWIgRVYv
UFNEMiBDZXJ0IDIwMTkxLzAtBgNVBAoMJkV1cm9wZWFuIEFnZW5jeSBvZiBEaWdp
dGFsIFRydXN0LCBTLkwuMQswCQYDVQQGEwJFUzAeFw0xOTA2MDYxMTQ5MjZaFw00
MzA1MzExMTQ5MjZaMIGFMUUwQwYDVQQDDDxFQURUcnVzdCBFQ0MgMzg0IFJvb3Qg
Q0EgRm9yIFF1YWxpZmllZCBXZWIgRVYvUFNEMiBDZXJ0IDIwMTkxLzAtBgNVBAoM
JkV1cm9wZWFuIEFnZW5jeSBvZiBEaWdpdGFsIFRydXN0LCBTLkwuMQswCQYDVQQG
EwJFUzB2MBAGByqGSM49AgEGBSuBBAAiA2IABJwJZClPg5KoeHhGqUtuv8o8DUYD
+FuNm4szFx+stoo6Bn8IQjbQaRdj+BXP008keggIoKjeKUfaOGebcot2BLirNhYo
u5xbN6fsVCoerHfAFz5/pOev4FQRh/m4pHaicaNCMEAwDwYDVR0TAQH/BAUwAwEB
/zAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFOrpUOSzk0k/BQQ1pfBHVxF+XhEZ
MAoGCCqGSM49BAMDA2cAMGQCMBBxKbl4mBx9pWki6DLVPCSloHBSSM7kdPxQUwQY
v9kCEBnkt5kF8ZFYGbinSSkKDQIwA7qPHhRyKSDD2X1hCQKtauv5FT3ufStwDOQP
33uSJ7F8aprXuUd2t0bFdIvWKRWz
-----END CERTIFICATE-----

17.8.3 EADTrust ECC 384 SubCA For Qualified Web EV/PSD2 Cert 2019

-----BEGIN CERTIFICATE-----
MIID3zCCA2agAwIBAgIIBFExZXBGYzUwCgYIKoZIzj0EAwMwgYUxRTBDBgNVBAMM
PEVBRFRydXN0IEVDQyAzODQgUm9vdCBDQSBGb3IgUXVhbGlmaWVkIFdlYiBFVi9Q
U0QyIENlcnQgMjAxOTEvMC0GA1UECgwmRXVyb3BlYW4gQWdlbmN5IG9mIERpZ2l0
YWwgVHJ1c3QsIFMuTC4xCzAJBgNVBAYTAkVTMB4XDTE5MDYwNjExNDkyNloXDTMx
MDYwMzExNDkyNlowgYMxQzBBBgNVBAMMOkVBRFRydXN0IEVDQyAzODQgU3ViQ0Eg
Rm9yIFF1YWxpZmllZCBXZWIgRVYvUFNEMiBDZXJ0IDIwMTkxLzAtBgNVBAoMJkV1
cm9wZWFuIEFnZW5jeSBvZiBEaWdpdGFsIFRydXN0LCBTLkwuMQswCQYDVQQGEwJF
UzB2MBAGByqGSM49AgEGBSuBBAAiA2IABA/E/MZip8kQYbCd6ULS02ZFHo3mMWXN
PX2TgKPzHlkRvEO6W25XPT7kHgaJQkBXbN3runWSrd0jO+VOTpXZRizLMrwpwL4f
HqO/CzZNiryxd0BsSscTDAwsdSlN+c3apaOCAaEwggGdMEsGA1UdIAREMEIwBgYE
VR0gADA4Bg0rBgEEAYN1AgEBAYMRMCcwJQYIKwYBBQUHAgEWGWh0dHA6Ly9wb2xp
Y3kuZWFkdHJ1c3QuZXUwEgYDVR0TAQH/BAgwBgEB/wIBADAOBgNVHQ8BAf8EBAMC
AYYwHQYDVR0OBBYEFHG7WKA8L1SHXQt7UUg4q2DXqqnjMB8GA1UdIwQYMBaAFOrp

UOSzk0k/BQQ1pfBHVxF+XhEZME0GA1UdHwRGMEQwQqBAoD6GPGh0dHA6Ly9jcmwu
ZWFkdHJ1c3QuZXUvZWFkdHJ1c3Qtcm9vdC1lY2MzODRlYWRldnBzZDIyMDE5LmNy
bDB8BggrBgEFBQcBAQRwMG4wRwYIKwYBBQUHMAKGO2h0dHA6Ly9jYS5lYWR0cnVz
dC5ldS9lYWR0cnVzdC1yb290LWVjYzM4NGVhZGV2cHNkMjIwMTkuY3J0MCMGCCsG
AQUFBzABhhdodHRwOi8vb2NzcC5lYWR0cnVzdC5ldTAdBgNVHSUEFjAUBggrBgEF
BQcDAQYIKwYBBQUHAwIwCgYIKoZIzj0EAwMDZwAwZAIwGtzHs7pI00elA9QaPgjG
bZZrH2AUuz8+0Jp0OpPpAqsavD6slEBAIDV+QIpD0Ga+AjABhvTQpMrL7vJgjaGi
mVIgisJqhgNZ82WDmERYQ9dR8ETvlzVWkCLboXvF0tszlI4=
-----END CERTIFICATE-----



17.8.1 EADTrust RSA 4096 Root CA For Qualified Web DV/OV Cert 2019

-----BEGIN CERTIFICATE-----
MIIFzjCCA7agAwIBAgIIaUgRCWiBiBUwDQYJKoZIhvcNAQELBQAwgYQxRDBCBgNV
BAMMO0VBRFRydXN0IFJTQSA0MDk2IFJvb3QgQ0EgRm9yIFF1YWxpZmllZCBXZWIg
RFYvT1YgQ2VydCAyMDE5MS8wLQYDVQQKDCZFdXJvcGVhbiBBZ2VuY3kgb2YgRGln
aXRhbCBUcnVzdCwgUy5MLjELMAkGA1UEBhMCRVMwHhcNMTkwNjA2MTEyMzM0WhcN
NDMwNTMxMTEyMzM0WjCBhDFEMEIGA1UEAww7RUFEVHJ1c3QgUlNBIDQwOTYgUm9v
dCBDQSBGb3IgUXVhbGlmaWVkIFdlYiBEVi9PViBDZXJ0IDIwMTkxLzAtBgNVBAoM
JkV1cm9wZWFuIEFnZW5jeSBvZiBEaWdpdGFsIFRydXN0LCBTLkwuMQswCQYDVQQG
EwJFUzCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBALwsCMbnfiu95vK8
pyDOIGJAJegcH7EURLP979Fxtyz47Tb5GSLO8ltGW6ncwTFYtQKh6UMSiL0+tW44
QM9DLYWu3kSvAQpxiImFKQIkkZPxNoQ7X35EGwDQ5R/Z10aX7x0kwwu9hGS+FwBQ
tTPHWR7t7GpNbmFu/qggL3tbTDZRQHPlEgpQWkND4CGLXS452CXpmymNg36/NMKU
3kLODCoWno02SUMtbehIwCwPZknWNFBGdXE3AZVUFDHRk8JXRQug+G5Ma7gMQ+Dy
TG6vWM0UVSlRpEmUXvD6EJ6te3g9+L5uSUkJ5HNlUAk4nCZi560/ek6b5ga+Tuit
MtlCN+exp+vnXTy4eXDjwrfNUS4dc0pzn3nwVR7uuJ/vrWPDHqjdDZIWb2pMQ9qy
rcGlhmz2lHQWPx+MeTwTfDniDYeFYSovv2bBEakeTGq5qRdx32vNseKabhC4qsjL
HP20700hiqwjKPao1S/8JdhwIvsOr0ao8Ey/vxA37S3IxPzIz+J6PfuOwx3Taqr1
K3zmHXamu7l2NFaPygxecU7LbVu6xwsx0HT8Ch2bvjLTLW2pc112XxdrQ1bM83jT
qA1McGNGKjH7Yma7sI+T5ToUyFlLb6xLnFkMW15Fmz1sDKdWUvAYt4oLkgQi4Erp
TgtYSpWFUtTqVDRYp2HS1PSvBEkVAgMBAAGjQjBAMA8GA1UdEwEB/wQFMAMBAf8w
DgYDVR0PAQH/BAQDAgEGMB0GA1UdDgQWBBS2xXmeFhyF2VIdyxzSiMUsya8NRzAN

BgkqhkiG9w0BAQsFAAOCAgEAdajcm8hyZIMZXHdZFbmSGm8KtjzT7wPNytf79ajU
QBAlvT3X9EnlEVROZfHAEcbn4qLHvp3oZ9MQzUP/QRqZsJKNzBzkHiNCDAB5gLdj
cx5GBD23YuEPhxgt0uWf0xCBH9SGQiSMS+KBD2XTbwOPOWQ2fdJ7VnI/loRVks17
Hkk+SD9rycRyPJu4nnl3pqsHqsBGtdLKCyLuw0x0bvVGHdgEf0nSdmzSHJMn/rpb
ka9EoMIV3IIirkC2coXSmkyasyhmI3EiMwYyTnI08262cF1sIWftH7VAW+p2H1tj
h8kZZT7bm9HyMfNGCUXWKR+QeAVZl/Wgi+luxuxsqigiLOiWTG2jPriuIlu0ujDG
TBtQnc1Reig0ImTmfy844e+7uGJVzQHl649YUl+OZS8SlmLgbN8fC4l6qj7OxmLs
t/kTU4zj6PrwqaNkSIi8446A4TsC789SXqK6pEqs9GvJvPZS/mESNytjyIwZbVup
nqGDqbmqNhrVos++aQEtenWkLw4mHGwqJBiW7xWVCNEv4R/vhywfFLjaruSThwRi
O2siulXBgAmP7yHu3Nh/Np8h9HvQyE6/tVEvecexO4xOLCY5H3Rs6l2nxfxxEbyM
TeBNpVXdT0R9dVzhLRCfKuYpCPWFENAFj+WUd/CydiJVC/7EtYHO/gc8fnAckNXg
5ZM=
-----END CERTIFICATE-----

17.8.1 EADTrust RSA 4096 SubCA For Qualified Web DV/OV Cert 2019

-----BEGIN CERTIFICATE-----
MIIHKzCCBROgAwIBAgIIZGZmQkR4M5cwDQYJKoZIhvcNAQELBQAwgYQxRDBCBgNV
BAMMO0VBRFRydXN0IFJTQSA0MDk2IFJvb3QgQ0EgRm9yIFF1YWxpZmllZCBXZWIg
RFYvT1YgQ2VydCAyMDE5MS8wLQYDVQQKDCZFdXJvcGVhbiBBZ2VuY3kgb2YgRGln
aXRhbCBUcnVzdCwgUy5MLjELMAkGA1UEBhMCRVMwHhcNMTkwNjA2MTEyNDE0WhcN
MzEwNjAzMTEyNDE0WjCBgjFCMEAGA1UEAww5RUFEVHJ1c3QgUlNBIDQwOTYgU3Vi
Q0EgRm9yIFF1YWxpZmllZCBXZWIgRFYvT1YgQ2VydCAyMDE5MS8wLQYDVQQKDCZF
dXJvcGVhbiBBZ2VuY3kgb2YgRGlnaXRhbCBUcnVzdCwgUy5MLjELMAkGA1UEBhMC
RVMwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCwSupgVOitys8szrKD
eMCvgqHgQyX3HA02ifanOGpBFbEpZc2Ts8y7ueKj5t6BVHPIEcvQolUR7202L9Ii
2TnjfyIWF6vwvrtuKF4vOy3PUJMohrFOAGGfwOBcltSmfY09jNQolWBlG25cxLYI
Ea2WCSVYzolaPiiO9Az/BMTZBm87RgIUqIs+6SDPAyA6ZUcERziKZaK1zAGS51Sa
DaDYhkttApjbtFvO55clX7QX/hQes8EuRL6S/FDTWRWkGiUUvITZKqAZnNU9ZnjC
moV5gD7Gv/zQeOgpzDSyDP3ZdMKWObA1cS65sP0s+Oy+tv9ORejYQljojg70EC/V
g1i1aNQR6sT3tdi2PN1UDPLNGoXtUDAsmrsNC97X0nj0LSLw+fsHxjZFB77eXy5K
vneohNg8z8u/1lDUIO+3XdRym6uk3HLXyJTaYpZwn/F6NrzgSnwhvR/s2FMjO+cd
EUfyyGOJczU9PmxYp0vDU94etdWYFTRel037MO79Td3W7fSOhfhwHSO4SAycVXJI
0foCdHRcVPH0GgBVQmrh2zH80dmZcmFeNO7qrc7v4GyLl54ZNw9kK0RiblrwjDJV
RsU3FmDV2PNvkSCti/ZyJdFXWmXhlTaA92eSa8h6Ktvb+thO9nmhobUaw/XJl1r9
TEuGegl4UHlqPZ52daBEQ51eQQIDAQABo4IBnzCCAZswSwYDVR0gBEQwQjAGBgRV
HSAAMDgGDSsGAQQBg3UCAQEBgxEwJzAlBggrBgEFBQcCARYZaHR0cDovL3BvbGlj
eS5lYWR0cnVzdC5ldTASBgNVHRMBAf8ECDAGAQH/AgEAMA4GA1UdDwEB/wQEAwIB
hjAdBgNVHQ4EFgQUUGru8dcfpa4oD6W5AMAn884urLcwHwYDVR0jBBgwFoAUtsV5
nhYchdlSHcsc0ojFLMmvDUcwTAYDVR0fBEUwQzBBoD+gPYY7aHR0cDovL2NybC5l
YWR0cnVzdC5ldS9lYWR0cnVzdC1yb290LXJzYTQwOTZlYWRkdm92MjAxOS5jcmww
ewYIKwYBBQUHAQEEbzBtMEYGCCsGAQUFBzAChjpodHRwOi8vY2EuZWFkdHJ1c3Qu
ZXUvZWFkdHJ1c3Qtcm9vdC1yc2E0MDk2ZWFkZHZvdjIwMTkuY3J0MCMGCCsGAQUF
BzABhhdodHRwOi8vb2NzcC5lYWR0cnVzdC5ldTAdBgNVHSUEFjAUBggrBgEFBQcD
AQYIKwYBBQUHAwIwDQYJKoZIhvcNAQELBQADggIBAG0egb6nmjfLyVdrWKq2Cszu
8pSEV5ixWAw4AvID5ruZ6DNp4VMYBEHKNiY2EQFCOII1Gg79B2oYUwRXzD6lkorN
3zisx0dnn8fvpwv+kWTI2LyIUlRtyv0/Vg/orE/ZNVtEqrnY7hcGiFh+Kufw8uN8
4TusMCDoLDxVVb+0lYmhEjN3S6y9Gjp41KK4Hw2Ou4RBmJSv5D7HZibgWVwwWEk2

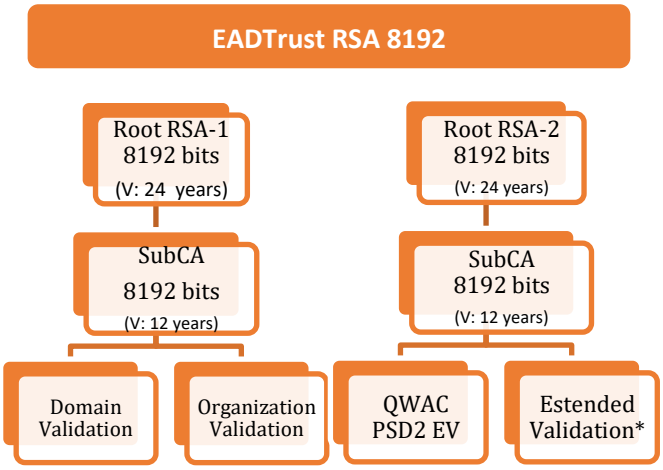
sdntO319YTbRC3A+3jAK2CKRPmZvkBPdJDXFbHi3Bd7qnf80yOsxN+Fig/Ej8+F+
CIb8+97/kAngAS8L0uRHU9CW/4/ogA8ypHTScQLWPehRFwVOlC1S0AmP6rGM+OEK
3vpFsRtP0kHHBROs5Mmtek3CFssdXal7ftZZJs2l2HQ1MM/OgplNSKHku/soVC8b
TdN5g5+yfUStdURRIjgkDxQCuyqXFcJf29smDzGCwQ2y7RSgLs0Qr0uasDojS92r
3BPrp/hFvvlkjsN4IvfgArnjfndzEfubf4tgUT8doxadAgHect64fMWlkWdtns3c
VFmvg9lySzKRWe5KIWVO2NymeuryRbRVaY2dVYBr1ARFcX4Nv1I0apLGrAmJxRD4
elDNuDczE1T2EvVaR0l68W90I5WVACn0+eQCAworop0lXK12YcsaaRKd3NhlVrDx
jv1Dg1sLTsbhUFv2RvQK
-----END CERTIFICATE-----

17.8.2 EADTrust RSA 4096 Root CA For Qualified Web EV/PSD2 Cert 2019

-----BEGIN CERTIFICATE-----
MIIF0zCCA7ugAwIBAgIJAJSCBgEgJCdBMA0GCSqGSIb3DQEBCwUAMIGGMUYwRAYD
VQQDDD1FQURUcnVzdCBSU0EgNDA5NiBSb290IENBIEZvciBRdWFsaWZpZWQgV2Vi
IEVWL1BTRDIgQ2VydCAyMDE5MS8wLQYDVQQKDCZFdXJvcGVhbiBBZ2VuY3kgb2Yg
RGlnaXRhbCBUcnVzdCwgUy5MLjELMAkGA1UEBhMCRVMwHhcNMTkwNjA2MTEzNjMx
WhcNNDMwNTMxMTEzNjMxWjCBhjFGMEQGA1UEAww9RUFEVHJ1c3QgUlNBIDQwOTYg
Um9vdCBDQSBGb3IgUXVhbGlmaWVkIFdlYiBFVi9QU0QyIENlcnQgMjAxOTEvMC0G
A1UECgwmRXVyb3BlYW4gQWdlbmN5IG9mIERpZ2l0YWwgVHJ1c3QsIFMuTC4xCzAJ
BgNVBAYTAkVTMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAqd1bZClu
b8Oc7Ehs6nPuqjmVkuNbFWXNPIBtPg74gNGtO1GpKcz2C2b46Numxn1zjL7HVTFv
ovdlMVVpq9eRzlPTV+KeeuNHXeXmWbleQNt2uCPLnlnf1hPIs2QL8/66WtueLTQ0
EjygIbLEgAAGEniFwch0GTNHPWoIOmTOfXnurpvXYI1w0f2vM3p5LeRD/wVD6v3D
I0on20/JcXldtsGbucKxRa65mzkGfc7ARrMKer0gJDEFaLigvd+CFbcqpXB/kk2u
6qxA/IhsIYZ3vly+EaVXhm0h05WMvC2XeW+lxguavsw2n+ru0HljcNBJh9Np0WKe
3Tr4RU+ZDvOOdrfUM9B84P/FPhvpTYqHwmdjm3lVdl3qMI5fyasTBeFJKWOjybch
mEFrwFP+VTy5fCh5j9mt682PonMbgxxQGX9Uqy0qzo0x62fSiXzPAoTRJdd6RfY7
fNm64gndW09Rn9j4LLuGoyf16yFsEfv5SutiJMK9j1tsaVc0Y4x9ec7QA+58cLMM
yZWfTEoJ8fZv6CUycBv4WldTzzA/HP9FTDjQmbHqdBw0bsSyzN37M6dgdr5+TQ1A
Lf6VOcYEMcT8YDZ8nHe2waBYix4fKlKi//nnpJTiPp07v1Ptp13zpOd/sOep2bus
IWg3FcODltY0jQw5533Yf/i/QcMz/Y6ApHcCAwEAAaNCMEAwDwYDVR0TAQH/BAUw
AwEB/zAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFLQeKNTqqmAPEAR0y3eUaUwR
h+JEMA0GCSqGSIb3DQEBCwUAA4ICAQBCWyYycusmGsjmtaZU9Y6w8FHPQ9yJUNWg
9gKykaYKcEPv/AJf6tINI1nh7si22kGYS5PpVx6wcNdnUjoMfZpwErAQIzdb6kkg
5LDe19xAD2fsgMb/zV0Xa6ZcEJyimp74uaXCdGFHqUwhFyusS9HSWhnSURiO1zzk
cZ1AgyKllm8e/RndiY8gvD+TXUDkVGfimtF26zCUtgaO1Fzu1+mi/ShfJfrSnpgX
qn2zoCCpImefkRpz/7YseQDcnJ7sYAPxveM+b0C6vk5VH9B5bkSWdLZ+dSJlgp1p
HAaGTLYn4GXt8JYSp0CNzjeqBMJVaGCxPqmGloDFIg+IecLZdTZRtdaIr3pnD0jB
hrZ/WyxuFFlCXsNgTfcqZK2LS2yY5dRfNu+zyTgg4XtAzkq0Wbn2JNCjxihzl6no
E1daeNdtCNqFoxTFK8gItFTwxHBhl8H7dkQmyiZe4qvWT8qvuO8VzJfAuQ7aEAlC
lmGJR4wGo7h/QL0iMV9MiiTIbkDK9M3cboH9UV8uEHFVVM5NkDhFhXwDBo5s85Ix
bIKkfZBvoesJ2yveTELWGztSED3JzCsIU7GH0lJdW9MMjjFGrY2/s35/+KLsosgN
WlKAJX8Lg61JQER4PNWh5bUEl1gN3HYd75bLdEXlwblMEbuoHfhi7CtsjrHf7G+v
lhVDgRGPCA==
-----END CERTIFICATE-----

17.8.1 EADTrust RSA 4096 SubCA For Qualified Web EV/PSD2 Cert 2019


```
-----BEGIN CERTIFICATE-----
MIIHMzCCBRugAwIBAgIIRhJxmAQWRCYwDQYJKoZIhvcNAQELBQAwgYYxRjBEBgNV
BAMMPUVBRFRydXN0IFJTQSA0MDk2IFJvb3QgQ0EgRm9yIFF1YWxpZmllZCBXZWIg
RVYvUFNEMiBDZXJ0IDIwMTkxLzAtBgNVBAoMJkV1cm9wZWFuIEFnZW5jeSBvZiBE
aWdpdGFsIFRydXN0LCBTLkwuMQswCQYDVQQGEwJFUzAeFw0xOTA2MDYxMTM3MDJa
Fw0zMTA2MDMxMTM3MDJaMIGEMUQwQgYDVQQDDDtFQURUcnVzdCBSU0EgNDA5NiBT
dWJDQSBGb3IgUXVhbGlmaWVkIFdlYiBFVi9QU0QyIENlcnQgMjAxOTEvMC0GA1UE
CgwmRXVyb3BlYW4gQWdlbmN5IG9mIERpZ2l0YWwgVHJ1c3QsIFMuTC4xCzAJBgNV
BAYTAkVTMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAyl7ySeyjAr2M
TvJXpWgzTqonx/k3SJVYrz70KG8Ogm57ojCUAHoMX7bJtdyAujWUY+afyGZDbVfb
oU/KjZ8ruimtX2cT/AI93KFjRU4Ld1Adr+7KiE6iih3jCnwnsw7WnGJA+zarqExD
qTsXJODdWsVzgrE7vaWqGmx3QVa15Aen31QadKBSlPiZ/BjRlEnUC92vrMNjTzVE
2sGQIPd6xVB4bQVvgZIGbH4xkRXSUQWz9m/wuI+rmiUmxMUAY/LCoeBKnNiOwwra
JxzbqJuP23GM5i9xVVjRATmumKPPdgGpZQFMp7/OAhUqzSxLoCLUh5WMYULokJHT
FZQippX01DB/iU/lR80vHipaWdAQycgs5ez/540FmK9iFFDIHEr0k5+lSxCLvldk
EGuDzmmDyVRc9tE1Gissp53esfEj7tXXmH74032rOJz0ycGVs51KaMNClyNHeUOw
SsYvaehAmG3fWl7Z+/9SBac6dlEh8Imip2sagmLiQLKs+CflU6N+rkmX7deOM6hs
dJDnHsXB/WhBm8gBjlWuX4dnkjs67HK6MKh/FGoMCyihISNN9PMFJQOMGIy1Lvw7
U1LdlxcJfwqmT4rzUiXNL3DcHa9Aj+Qd7SEGw0Rjz0oWustEdLPqfZXVsvzJDLcp
fhTnzc29OtvPaMuppdLXkVAGuHoTmvkCAwEAAaOCAaMwggGfMEsGA1UdIAREMEIw
BgYEVR0gADA4Bg0rBgEEAYN1AgEBAYMRMCcwJQYIKwYBBQUHAgEWGWh0dHA6Ly9w
b2xpY3kuZWFkdHJ1c3QuZXUwEgYDVR0TAQH/BAgwBgEB/wIBADAOBgNVHQ8BAf8E
BAMCAYYwHQYDVR0OBBYEFITO82uqplcwJ/fDEpkg5eCbWh5EMB8GA1UdIwQYMBaA
FLQeKNTqqmAPEAR0y3eUaUwRh+JEME4GA1UdHwRHMEUwQ6BBoD+GPWh0dHA6Ly9j
cmwuZWFkdHJ1c3QuZXUvZWFkdHJ1c3Qtcm9vdC1yc2E0MDk2ZWFkZXZwc2QyMjAx
OS5jcmwwfQYIKwYBBQUHAQEEcTBvMEgGCCsGAQUFBzAChjxodHRwOi8vY2EuZWFk
dHJ1c3QuZXUvZWFkdHJ1c3Qtcm9vdC1yc2E0MDk2ZWFkZXZwc2QyMjAxOS5jcnQw
IwYIKwYBBQUHMAGGF2h0dHA6Ly9vY3NwLmVhZHRydXN0LmV1MB0GA1UdJQQWMBQG
CCsGAQUFBwMBBggrBgEFBQcDAjANBgkqhkiG9w0BAQsFAAOCAgEAnVdxWWcf0MEm
71hVxgNgaiGr5lsxPnZvme9gc1XL8WLq8Nbcoq57ZHwHtqWwIHfVpUDz1gxPC963
jfgZgr/6ows7S5lQ9fOZqPsoL9axi9LOk9F74s7/JRyRgqpvkmW2u1h4WLB92KJH
XgbCazHS87a+uTjqruBerU2lMNM0HD3FD1QbXWvb2pK5ukdaaaQKnujAJRLLiUso
rhUdGMM/0uUjokzywAizc051DGzIUdrbqfVOp1yik2zdS3XmcG0mY+/P+0ILiKFf
fV10jyTnyxIt5zL/b9uliyjq3Uy2ZJ6WPdYuFhIyVCjEW8Nns3Gne4KgHUwitM5D
KS39q4U/MzuY2E5p9E5gRT5ZWxekrc2MCGSoQcjbpKozDlAFx7V6FZdN3D8tJA0C
22MLblaSNg0Wxh1HnN3/tP93JogwKNuHQcYAz1vXK5PI4JCok8QuQNhGZT3nJlLM
lFtEhNdxjBI/LahjE2/yhfUt+1ZUgHYjVEk03CQv35zTPDcWZSUj/GxxOURoAvQc
loTPCF/y0bfqD4vVaoESERX0vvijbZw2TW4HHvsx6uGY+INVSsUTHjoWbuwsx/x/
jmdHoVi1QrQbWfzlpyOvhcoyxuFNDeBd8RB0PXv0O3dWTMzSeQWPga7HZmo24ZHQ
ivDguM8/3NuSF/lKI2p/Eh7g2JPEGSI=
-----END CERTIFICATE-----
```



17.8.1 EADTrust RSA 8192 Root CA For Qualified Web DV/OV Cert 2019


```
-----BEGIN CERTIFICATE-----
MIIJzjCCBbagAwIBAgIINpRQh3QHYJYwDQYJKoZIhvcNAQENBQAwgYQxRDBCBgNV
BAMMO0VBRFRydXN0IFJTQSA4MTkyIFJvb3QgQ0EgRm9yIFF1YWxpZmllZCBXZWIg
RFYvT1YgQ2VydCAyMDE5MS8wLQYDVQQKDCZFdXJvcGVhbiBBZ2VuY3kgb2YgRGln
aXRhbCBUcnVzdCwgUy5MLjELMAkGA1UEBhMCRVMwHhcNMTkwNjA2MTEyODI4WhcN
NDMwNTMxMTEyODI4WjCBhDFEMEIGA1UEAww7RUFEVHJ1c3QgUlNBIDgxOTIgUm9v
dCBDQSBGb3IgUXVhbGlmaWVkIFdlYiBEVi9PViBDZXJ0IDIwMTkxLzAtBgNVBAoM
JkV1cm9wZWFuIEFnZW5jeSBvZiBEaWdpdGFsIFRydXN0LCBTLkwuMQswCQYDVQQG
EwJFUzCCBCIwDQYJKoZIhvcNAQEBBQADggQPADCCBAoCggQBAN0LprZCZ8+5dEQl
RYCdFq91cpjmUkuf3sECKJKk53nnXxbDQhup/gS9I8K0FQrs0iWouxsKSDLr9gdh
bWp0O0fOGDKbMb3Wfktq2qlhce/HNqYHP9HrrqHEXg4V/wXuHGVC1edWk2pR08js
PrcZZf/IjdavwRp57AnmFjIyhm1ypiEqHBieHHgeDdEn2i43CSd7l0t7dXCnhmlr
wUhtgI18umIeMdAPy4cEhVTL8IWjzAkhbcUoC6ZGYs7WaXYeCflxD4tcZUv0/o6k
RLT24bZRKxrUwygL8JmravQaDSDZ9biGnZ9PkfQOK/0N6V3lmSxdAJ0zykeXWCPt
IvxoNn9ewfCKehfUhRfSY/DK7nL3oDkuT3zHTywymasa6oE7HYqOqAoXzKPAcDal
xiW7At8A5+Tsh1jPaOzZfIGEAgM7VqnDnvPjXttn+WII7rf8RM932UEsqkpCrmw1
H/u/V5cj4uFuGk4UHVVJJKEQ49vI2nO0i2LsJsm16tY+OPCEXZFkcJZxWE7rc10G
UXkD9OyYCIc8ZKOQ6/lt5mMMm5Xxx6qudMApLsB/ZFhqNB4kFvgvwWWDk9MyvosJ
mp5KpSjkqhjCHucng33KYGFAZQJtz7IRv4pHDTyAJxEyCNQGRiaMq9YX8d1DTxgc
Qqx0IG5Gq4zNHe7PzR/ihARNR+1CAtbC+VbKNTRbkvxpkwIPOGU5EU2lda/Sb/2q
RHZwJkcID0t3rP1gxuB/AlWO+YnxE/lfTGw91Ba3fbt+wweHvYhvS9jpcR7OSvs3
9TiwHE+0aDHVpJwHnpXq2TrfYY8pFp9fJ8REACPF0s18xRFmS4BbEQd95v6B+3Ik
t54GghcnDBr9Q0fYSWJPBqCuaAFWDN0pWD9UObVAUXzaTMEr7zjInYyLXHb9mXGf
ADOwEbisvmhEINKx9GxalrhZ68Icy6rC1b8h9ON8DnoGja7AeLP+zMAJSjvomBpI
1VvxFoS7b4zNok02Lcsa2250TcAXIBeK2oECPUtiJFfn8MUp/XmbT0fwOeqFZ38q
QX3BDRAbXCOGs3vhMXHqiP1+Z3h59jHfjwtUj0gPEuybG8JLg0qdNtqVTGc5rjL3
Gbvf6GK4eJoVKPh14/TquV8up8TwVPr8MErrcD7SmuHvhZL0rYzsxJcBHimvGkRY
xIixukKuIXqJgRmquAfj4Ss5psU1mrIOlgf/iekI62g0aGyvCe2XPpLtu4n/JK2V
zAVjyciwY0Ysc9uR8tFChkyQjpP3KSqDGV7JfO8Tpnkibwx0zA3dLPSeotlW8vrK
NVdrkis3eSnqCJLICbCrbFkL7AmBSOmv5gcQ8SHZClzm7d7XsuSXJTv3CScDEcKc
PwEeo/8CAwEAAaNCMEAwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYw
```

HQYDVR0OBBYEFJ7tDEGBam/6Zgn6fH+MSGMINn0AMA0GCSqGSIb3DQEBDQUAA4IE
AQCSbCQ7Y0FPXeWl5+HKKSE4wl9Gx1fznLKBzXaqgj8sNfS+FM7snBlMXbrUUNWQ
kt8r82B4N1Zu7g5jZhjTN6jey9BxA41yHtBhOA6M6tG5ITEWIq+Oa3L1PhCuvfty
kz0CsAg/g3j3RTB4k9az6JnuivihwlYgoi4GcV7JZiUOHk9+DyFSliuvBuOmXstl
PVg6I5H4R3vBcIL44THdAkfLTXORXs7Db3aqQmG/tyMxwalKrBLs3mJnPRUzrlp4
6MZ9bHtJp7Q0gFGYA/KtR3H5GFbxgqQnaBUpEwWbRBHTD+HtiY9zcJ/h9CeC/Tt+
q9J9s6x2MeBWLpZ+nn4UEj5E+WWfNOt1TXzty1EdjoqY9CgddoneE3UpHV8Lp40w
ewE+pNx6SH7QsunxKokasdEkENyd6BmNdlm2g8PbSb/eSJcAKVvs8mhrKM6UbE40
rO361KNrShEwQhG82eSbInHwG1mF/LWr6PdIm33AsKac28wluoA6b8jV7Zu637R1
1giwSJRugcceYrH7CTQAiVGKEfovBSGGOOMtY/UHY8GWbgKlufGqpSBZOyofQwVI
CQh6HEakHHXWtSOrJdQqPpAF8eMgDJkO7ggF9ZHdeZBgLWf3fx3+A+JLODxE5q30
DvcMJ5tp5MG37vRnozwEyP2xRj9jJKqpAvD3hu7zwjv4T2hlJO4l5L88ck9963Ni
mRWpu+uh+0HB3o2+xaWAsQeqYevSiWC69NHA47TPeph2aSEzSgggSH6st088QqcY
3zscUQj+kYI05y/TF49fxQPp+6EiCHmMPZa6qZflOCWADMRjRVXxLXIIXhByEOGK
qg831boLmiH8LU/FpC48hqslPAn0T1tL/TDTGkUhgw7816D/y9sCu08Ee9I3ijJG
MuRQiS89DCRyKBsbJ+pG7KD+nu2acYh/bt73XS0pet9eGCnwLNCaAwCFOpDBKzzI
e8/aVbtEyFoNxi/X1KKmLpys9Sx/o9B5m8xEVKSm6jQVABe1e/uIiR1bkt4PFvZv
VBzDN6Sq29Exln3mdUpFvqh9e7tC+kgE5z9T9QEyTdsdUStfFnXbkQQ0Y1LALzKv
C6did9gA2pOKHr7cNGSDbpY2xKg8WsBR+CsMzNT4aadA5jOqC1SmfMae6Ei6PhFT
TPsUQfW7Ug+0OmRJRN35I4hk46nr+6N6cAD9sodVbOjLYUmh1NwyARoHJd99RaWJ
NM7l046ltdQM5KNjp85b9Yq3iB1ZnqmR5nWwxHdfGDnxdM3iyszITu9Ey0vx9BSD
jI5h3cZCZc2WUZrbyG6d16n1mXdV4ANo0zTzE6NNQef6JRfAzXzpFep5PT80a4je
2VSvVuVhT5VEYQbgkNhkIFh/
-----END CERTIFICATE-----

17.8.1 EADTrust RSA 8192 SubCA For Qualified Web DV/OV Cert 2019

-----BEGIN CERTIFICATE-----
MIILKzCCBxOgAwIBAgIIIilxABI5kTcwDQYJKoZIhvcNAQENBQAwgYQxRDBCBgNV
BAMMO0VBRFRydXN0IFJTQSA4MTkyIFJvb3QgQ0EgRm9yIFF1YWxpZmllZCBXZWIg
RFYvT1YgQ2VydCAyMDE5MS8wLQYDVQQKDCZFdXJvcGVhbiBBZ2VuY3kgb2YgRGln
aXRhbCBUcnVzdCwgUy5MLjELMAkGA1UEBhMCRVMwHhcNMTkwNjA2MTEzMzM0WhcN
MzEwNjAzMTEzMzM0WjCBgjFCMEAGA1UEAww5RUFEVHJ1c3QgUlNBIDgxOTIgU3Vi
Q0EgRm9yIFF1YWxpZmllZCBXZWIgRFYvT1YgQ2VydCAyMDE5MS8wLQYDVQQKDCZF
dXJvcGVhbiBBZ2VuY3kgb2YgRGlnaXRhbCBUcnVzdCwgUy5MLjELMAkGA1UEBhMC
RVMwggQiMA0GCSqGSIb3DQEBAQUAA4IEDwAwggQKAoIEAQCx1dSRf8fT/UNMTLAu
ISQ9i9zLrUDRrqVRVJmJydIrfL8TSIAkS0OHE1ai1QLZ/YWJqwI8MzLGisp+aMQG
ZlkNpqJ0WHrg/XX0tMye54K0g8GLPRt1DwKv9KPlti63EKrBTh7a0OlkzEhFIhhv
zgbvLBdjafI9y7z9IOA/mnmu7Ks/MzduOTn9A4I3ATdV6osE2vIkmS+fAiooHe4k
oCBbS+iKUHnD7x0dxtq7ytwP0FF/WqyT64bX8uognTkrRBzf48Bvh/ebl1forERh
9g44Vztok7TGfcGEH/wtNKKwvMRBTmIM4n/Lqcl88Ov9kIn3ueQiMFLiB0pqiuev
mjlkhn4Zhl121Xd1rZSg8qDh1dCABFwaqNpzhaeBKdViE3mDDhO5KywB2zITf/rN
USyj2Qz+19SAtZ7WpS3FkYp71EmrTAYnQ7vdqeY/4EiCELEGrJP+yb36UPbbCJ2E
upH20zH1PmCxwNXb5O6Zb0ZoI7nB4xBZFrKyKWv8o2lvs3KhckyqAFDSWH81vLDg
uXxohKt7OPMDzJKKTzu2dvcVSgla2EYr6Sq5F+aY80MTFFFuxOaP+DsjNdIJBics
dp8WfrVah3yrLaHan7XdqFHRW0SdBhK+yRRgUSdjN/4iDDDvg+bpGfaFbmfGt6U3
2hKCToj7nNOjRGT58J/bfSmy7wxCnYnjnKQLs8nGcLxHdIvizzHDJYf1wneI6s2y
iwhD5L1SrH85Yr5lGVZJU0VyYQs6WQ0ZFoxA1TuCwAQhsmx4P+XfJ5TxkFhFAcF0
Bveb0qT6Rw8N/HvDtge3UpN848/U1tbi1434K584pqJHTqEhEfRP9ZqBQgy1j+TR

PXX234aA147rAYMO+FteetVPAxeZbf+cWzj2ilEPUYSa2Dl4DJ7LXBIzdRJ83bGo
KvZeSPuPxt1GvW8OtSk9DeS0S7uAWLeYFVJu8hIAHTRau1sfLGolivKLsc1p8iy9
3DushjiID4+RsE5FN/6coq/pprxA6qwnhWWLKdkgyRNJxa8rP9/fW4vQiI+7kfqF
GM8j17b/iHpXzoiHbrXPM+gGWyZZ/MJlTodFLNq5jZup+6+1S2S/sYBhAl8fAM67
KNDstO08VkGpXjSHIJm6QA4pwcLLhCd2aClzwdEWO30+wwuS+7tpneP4P78r1ECN
nrAgpUBVYKF5F+2h7xOiZu6IZifA0Ri1TKfxVPGUVG/5wKrFzUvEys2SMaD/9C9p
oKioY/maBjNMHnTiLHwspS5TQaUAd0glUXwIKJaLj1ncsn5jntAv+OCzveSSZOxD
2PaaStQNr0Bm6PecUvUlu1hm8se7YTXlQnJtGP8us3ifFq1lXRIV8RqHPSB6KLlI
AIfjAgMBAAGjggGfMIIBmzBLBgNVHSAERDBCMAYGBFUdIAAwOAYNKwYBBAGDdQIB
AQGDETAnMCUGCCsGAQUFBwIBFhlodHRwOi8vcG9saWN5LmVhZHRydXN0LmV1MBIG
A1UdEwEB/wQIMAYBAf8CAQAwDgYDVR0PAQH/BAQDAgGGMB0GA1UdDgQWBBRRzoY4
OeBXojWZsYxjV2WKyn57FTAfBgNVHSMEGDAWgBSe7QxBgWpv+mYJ+nx/jEhjCDZ9
ADBMBgNVHR8ERTBDMEGgP6A9hjtodHRwOi8vY3JsLmVhZHRydXN0LmV1L2VhZHRy
dXN0LXJvb3QtcnNhODE5MmVhZGR2b3YyMDE5LmNybDB7BggrBgEFBQcBAQRvMG0w
RgYIKwYBBQUHMAKGOmh0dHA6Ly9jYS5lYWR0cnVzdC5ldS9lYWR0cnVzdC1yb290
LXJzYTgxOTJlYWRkdm92MjAxOS5jcnQwIwYIKwYBBQUHMAGGF2h0dHA6Ly9vY3Nw
LmVhZHRydXN0LmV1MB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjANBgkq
hkiG9w0BAQ0FAAOCBAEAulcF47Uj9RV84rdUSpbjPve5mB4843uhTTCE1NwGC+uQ
pkMk+JNG968iRbv2l1aJFz6Rdb0FeXyqN5ppo9ry+aHG4fMNzjGNbVUq77Ua1NAQ
9uWUHMFDBH5Qm05StXuGwbHdquwZoP6PEpYzBpETjUmwUNzjR8HG9SYEs+kPG63x
xN0R6gynM+aYQPAut+IA/oMrrBeEavYggj9XyJTbHpRj5/b1LYe7CA6J5ru8P9BQ
PYGnO9M5YWrKd2ua9Znvu91uy7pehUiztOluKbV9GBHzsvEUtSis/5eWq7jJ6CMz
hP9AIOrq35KZI3weyDyw3I7knMZbJIXJj0e7OQds27TDCJWg5b6rY/YBeg1uZI2x
kBtZEc6NDcV2312luvI93uqyg5ZKOjTm1EQEyhr7UlCxcqQYO9j+CtnolH4ng/iX
AKjon2ve4fM3jVmaulTk4JmQaXRYtuyUJxBP2vNmthVCQ8mSNUbHucZGQAisNdq7
DvdSdlXsLKEv4V8Cp9vEhWZ+0iHKUAhITeychOhE1Hnxg/mrD0n4SIOMSxuIPM4j
lmByaeVUpF2UGQnOnCTsuBgvAuX8zfLXElhg+VZLZ6ZqN1ZeuRQ4F1KKX+jm6zmj
6pV8dXvs/sUahglxQAmhj4+MQY3lq0kLUkw2h1PKG7Dy/iAvcPXyadH92lZQgztP
QTKn7J5VvJF7P8w6HbbXa5EmlP3nnfSiuuPhxS/q+2VVhuVm48iCl8913CA82biY
Kkv7IXGV9Bn4m07YODnw4tJW8SX/WlO72PLQEM85kljeANbVQG0T4/sgDqlQKaVd
gaYytaabtTpjVXgkaQBIXtCI6TL1mruPGiy7NHmaP6+/RFxsSEYkJ7QI2ZPEBOK9
jEVCc2ZpIGTNmg8+eXVU/QrEe41MjwkYrmAbHrqd7mQFovXUrg4QThhcBXE08TIv
DHiD2PZAyJWE+dZBgKChbV1l/hsTMUaphKFz1Rrvk6CPhs46AaFvbcVeeYJyOIdy
e3/EJXta/bsRVONbGiVkspkweD2JwBjSRy/FwKs0oHGpBETRbOC9h2VXKC7wpfyt
6JeDKK1TRKR0cH94oOtJD6Q1em5phpSH+CEXogdJCwpYM1nTha0NFujYSfBC/zpU
1PtAWS1tt8e9YKoBfiaTcpvUtv6pnrBeOyC4Z24nLJtolxGNz/IapsRwKAIi6DTA
Eyyk3PA3OgyZ/ra6fCN0gDsJcp0HbZsr5yinfIrsTvQz+dNkLfXkni865CfeZLa4
o1LrNbCU6kWFJeGjlmvyblRnbAGo6+J6PAJ674ctL5ONS4DE9bMkv7MwA9rhasvn
rrUirfyVUJB4szSbVhnWF2LI0inGqOif3hMZETXbaQ==
-----END CERTIFICATE-----

17.8.2 EADTrust RSA 8192 Root CA For Qualified Web EV/PSD2 Cert 2019

-----BEGIN CERTIFICATE-----
MIIJ0jCCBbqgAwIBAgIIBpeYBykiiEMwDQYJKoZIhvcNAQENBQAwgYYxRjBEBgNV
BAMMPUVBRFRydXN0IFJTQSA4MTkyIFJvb3QgQ0EgRm9yIFF1YWxpZmllZCBXZWIg
RVYvUFNEMiBDZXJ0IDIwMTkxLzAtBgNVBAoMJkV1cm9wZWFuIEFnZW5jeSBvZiBE
aWdpdGFsIFRydXN0LCBTLkwuMQswCQYDVQQGEwJFUzAeFw0xOTA2MDYxMTQ1Mzda
Fw00MzA1MzExMTQ1MzdaMIGGMUYwRAYDVQQDDD1FQURUcnVzdCBSU0EgODE5MiBS

b290IENBIEZvciBRdWFsaWZpZWQgV2ViIEVWL1BTRDIgQ2VydCAyMDE5MS8wLQYD
VQQKDCZFdXJvcGVhbiBBZ2VuY3kgb2YgRGlnaXRhbCBUcnVzdCwgUy5MLjELMAkG
A1UEBhMCRVMwggQiMA0GCSqGSIb3DQEBAQUAA4IEDwAwggQKAoIEAQDnFBGJSZQF
iCvbIU5x8/ssEZE0hb0WoksMQcGdJsGpEY3FHIbgkg9J/CMAqKpbHemtrQoalRU+
5a7iTMH+dYyoiKyUYgoZ1wxWYjXD88U1XW06Jhk3wkqEe0Ps8rHoTcSW1XqHvEte
QYW/jaO+3vAFFBYAFGzmC4bYnGksxRO+4uKdPzpteXNVDV06GA/WnX34lVXnQNAd
dK4XxhmmF6Ztkoj0ev+U0lRlv6WekBL5MJpesV8xehYkTtoitiPdAVpScOJ6gDzy
2ELhKrewz6u/Htf9G1cRUsbYXvL09UOlOQ/z6WnaSOr6e9VDZuNz1SZx1nPatCj7
g4Wo7/8TsbRRlRMyh6M/ZMFODvb54V6e0lEGPNBZF0HMKnRk15459/2P0qWh7VK+
LeXAbQIf0QVib1B7LxkcF4c/yFro61ge/vdTHHn5/oV9NpWfdwdzcgfQg7MoZGi7
llfZ9gvm4lGeAlV0Z+3lt6nrSDidWxsknWoEioxE0fmfGiFBdTUWmwtGEla4nd/V
DLf4Rh7LZBeMvqiu/PSVlet7TtSLJt4ZFPc75k9FX3I6zjoZQRJsNkXXtpRaoyv1
hfEzCboAKZYyvSz5PmWicB2xuX4yOkUqqEHqg5qmA8GQVtzABVDkmCBGOghdrZJy
DjsPsdlhZXvSbSFVTFCZbLHnUeU+mtf1Ed3HDGq/HL5xSFRNfex3aYgerOpjCrS2
2Bcqb3c06LVnappJ8BTY8sBV0dLEHFaNLsHGP/NtWW1nZ9Mw6m5Dc/LNmSWvHWa9
PGxyJAWxYOL331QIzh/+GnSWDA5vHgfolLuHRtr06euBQGDLakZo7vTpQKrnIdOf
111nc4K2sJVMlch7MRup+dppwb2mvASClHmXQtGwS2cujxAeCCCN2paJ1wEUO0ed
BxKkPmI6zu38zJUO53A2GvB/pVPZlnyfOAS+/ywtayoD/zRK8oT1O1ytzDeb6K7V
LZsQtAqtKhOTZobSLSIYNYdsIAajnMsleQwWEcyb9lHDlJgn+wsLV8MHfTCnSvAb
YgT3MbZLHQhz4Q1CvjJu7fl68cdnXGDhvkqwzx1C3zqoWKlyTvtFEV+OTVBZVZ/J
Asg+SqbMaBhUVTEuVfHc3ATLKwNouh9cjGtVf6n96H59TXmUpgEvWtcZd9SNH+N1
TapoXnJcBWYObl0GYCk2H93WCJ14rGfuZczwzBdiHGjE9Gi1vVzBPb9+wX+xIX4o
pQ/mwTWCExE1Raqz6xocmMeaic7JDbGA2xcvHOeZZkhTuFoQPmfDrkl88q2A4cLq
d1vLc0Bsyjj9Nw5MGHShMJIfzK6gfWCaRsz9+XKyF9+/eNu7sZ1ivL/wXhiiYN0C
zwfPP4aJ1CRjAgMBAAGjQjBAMA8GA1UdEwEB/wQFMAMBAf8wDgYDVR0PAQH/BAQD
AgEGMB0GA1UdDgQWBBS6ag6YJzYcqjRN21X33bBzSfNd9zANBgkqhkiG9w0BAQ0F
AAOCBAEAV2eZUHqml3Diu81TiUkUfPf+xMZ4XtuL7HmFx0YDoLOpOdjt31finw+Q
f9VvVOX5xx7CHmW9L51gyqVWhDpeGE4obJsYlreJ9J0tvt+siY0nCJsrYyS54p5g
66UjMUZnRLN61+/vsIekC3RyoovoPm36EGUccKvQKpBtZHybBriolT90IenSFGaR
Wl1f6VjP1C+64wcnNCLSL95fkqLTLSwcQGNizRtv1lEhmz6eY7EREak5Bn1YdrAX
PDtvPR9kxCSn2yU3ZyTZrni8c6od/XmEMp5GC/tWorKnGmLQ5Lq0IrH3NkHX/iqN
nK0nqk/40uo8ZtJu4xlQFkL365np4j6y9LzN3++es0eQ4rtVbC++1sUOPQYUm9jC
rgobKlW/pOLXMTM+u6ecFh7Yhn+LCzKtNaeEpc5RcDWZmXt8OhcYjtH2D0k0TsD8
DbjDjx35H6RNLVXEx5xM4YZaKNZGx3QZBYQwF/p2qLKn6WzoOzfCKRC6WaAEiugj
vfcR/CfiU15Ia5DoQbl6yJ7vFYRCprLqm2ZU3K/mZQPwgEM1qb1+dF+5TzuoiBQq
VqH6f+eLv3qY6IuzWPIyoCmz7U/Xin0Ei4nOCzbwAeVGD5vqLk86/zxiK8jfm2ud
SpfFPFK7w6B0SzUbjOp7ZXOeX4N460McCr2s+aEApUc0m6N+1Yltub2aH+ILbiFM
HuK9eQdnIvVsX2BEJ69+tqbQiMX6JF3ImnUVLciRWKW9DeNrJfdS+c8GSZOVmwpc
sw0ZQeTeCcSePBYxAABRtFv+8NuNcRd68HomWDfoEYjzJPB7zEQ3V2TYgVMBabBG
RiutN7eQWcBEbfo1ockx/Ii+XJ45Ci8Q1Q85P2nmB2s1hbYptlQnL0ofHrk7hGDG
u44Hxd1PB6DarGVnI7btjgNSTfXwyVdTiORel4oz2fB9JlMeNcgQFF4QmjyLwhAX
asoD7lO266R42E2F3ge2qFvfWAD/z3vFLQROrAFhvs95s01ZiZPAXxNR6sZml+wq
TBtGCNZRZDlRXtBdtSN1EJw00dultZcuK9nPwhf1XREj3ZsZdnpIFXRJmXJwM0OK
pT+6ByQiy6Y+hJD2DYmNoYQ888KuFPJksHDcx1ZfsWjPNkjcgBj1k53ZmGVyD++I
J+BumObgqFekH467k43He0EI+5lUc6OfnwcatN+ODBhm/j+lXRQi6EGqYnB3mtbx
dVc5e3evuX2CfJIZM3iu4Z80jF7tp+3bDN3zUEHIlS4sI9UDao31GFv7ungpS1R+
Zt6W7wTxwd0BGZ4QQULYhd+cAfg1BnjDuwU/Rh6WghWKlXoD8ccwFZeq2n86RcfX
UlL1gL1xAbTFdLYLwLesBxOqU6D+Ew==
-----END CERTIFICATE-----

17.8.1 EADTrust RSA 8192 SubCA For Qualified Web EV/PSD2 Cert 2019


```
-----BEGIN CERTIFICATE-----
MIILMzCCBxugAwIBAgIIdpISCXExMwAwDQYJKoZIhvcNAQENBQAwgYYxRjBEBgNV
BAMMPUVBRFRydXN0IFJTQSA4MTkyIFJvb3QgQ0EgRm9yIFF1YWxpZmllZCBXZWIg
RVYvUFNEMiBDZXJ0IDIwMTkxLzAtBgNVBAoMJkV1cm9wZWFuIEFnZW5jeSBvZiBE
aWdpdGFsIFRydXN0LCBTLkwuMQswCQYDVQQGEwJFUzAeFw0xOTA2MDYxMTQ5MTBa
Fw0zMTA2MDMxMTQ5MTBaMIGEMUQwQgYDVQQDDDtFQURUcnVzdCBSU0EgODE5MiBT
dWJDQSBGb3IgUXVhbGlmaWVkIFdlYiBFVi9QU0QyIENlcnQgMjAxOTEvMC0GA1UE
CgwmRXVyb3BlYW4gQWdlbmN5IG9mIERpZ2l0YWwgVHJ1c3QsIFMuTC4xCzAJBgNV
BAYTAkVTMIIEIjANBgkqhkiG9w0BAQEFAAOCBA8AMIIECgKCBAEAsSLKuBGGPqZp
FmyeIJdi45KUoXxS8ikbxnLJsd5ShVdkSFLAhQWuhqrgXCuGCgoWd1mSN+6ERdZC
XJ5TtIlCpVcHH0fvtuFQSklPU+//NjS0IBw+iZk/5iUzX6+gpE1fhm2UDhND9JZK
2S31MI0B27s/ZXBO3LpjbjUE/F0tcPiYec4iG23odTrqSczZEpJAnw42SB4To4Gf
oFtFQhIRCAieM5OKKsbWN9pfsI4mhIEepTnVd8umSOkEPNecOuf6izlKncOBPkkz
kJorgLwP/C8YTAEyXSPdI4KCz8pQQSmflGfJ7b4DSs/DpR1dKTOXko5Sx5ouz3H5
TY4x6/LXxJBzKTDcy4Dpaoon3OaDulAUHO0xH872s5FEZu/QDoRLhQ6fQCdOQKKH
IE9V6/RXyNrdBDDB+zL74aw7aydQRzv8R5v9RobMBjDAQujnZH2P8/dz3bTh8bOr
TWzMBKQ0uOWoVr7GhcwgZthxVqEGxYv+rD+3ROpvvNar2nm//sZKm5On0kqw3a7Y
Tqj4+rqj+N2QHNphSnCTCb5yqBP5fZOa4t1L+zsO8lyCl8UblI7w1yy/BwiPR90g
2ddIVmmLXeS6FAI/nzVgbDzGQsyrjfHOjYXBLf3PKNRx7GiBYpGLAhN/EQLsvksU
NTMZWqeor46S6u/maKH95yNPENQc/2ycBGvlIAQ9yq5D2gNOM/AVBQ/u85yYNa9R
XsG1OcgdusnNm7lvut2GjhLwaAChFmG+W+AmteQtQdAsEoZsNLHTzZjW0F9fgtlN
QqXXm3lIZkpULmQqe5XYpr/cip2+NhL91JYkIT+1NxDSKovEidjRfdbVZgu2uGMv
dssPllGXLwnaLP304ZcKCpDGE59WWuGPD2XabhCx5JcbG+LsXNUiaf8KStqAVqp7
cporbQxoqPzxvXDlNrvWojuAJhp+Ad0WVGqPuQ9+FkwANs9NrjavMLd6z/+7ycXP
UK6ASLLCRh9En5WGi9IpgvZNonTYDX/s/S1Z1hrcjo2etzocMhedUaStQhnoXLNx
NwMRaVqKz0avn1BlVpRhHLYz5hU0geudkmzPtodtq9vbbHzyEJACSpbr+jS4wQfL
zhwSMRVfEGa016kmV2qbA26IdzAZBoQei7fUm11EpMLQwV/JFA/X9MKRLNrksOvn
EsX2N9V0LOXzQsmIywv/rqEDKv+nypoEn/xV2pVXx8yOjjqmzIrlzOVYvYd/ex0g
Jj8O3vbxcmQWF+/4ENNBOaU3PsbXC7KiWVxq/qulX3jv6KqCrjCL/+bDf9xcmZzx
7byreMyfJTBMOAAoPo/k7UhmvQKDbezkPbgnUk0uPNYi2te5ggMTVdZc7rrzJVDn
zEAgyTH42QIDAQABo4IBozCCAZ8wSwYDVR0gBEQwQjAGBgRVHSAAMDgGDSsGAQQB
g3UCAQEBgxEwJzAlBggrBgEFBQcCARYZaHR0cDovL3BvbGljeS5lYWR0cnVzdC5l
dTASBgNVHRMBAf8ECDAGAQH/AgEAMA4GA1UdDwEB/wQEAwIBhjAdBgNVHQ4EFgQU
DmLLaHy9Yxsoi1Qhrg+NpHEnIl4wHwYDVR0jBBgwFoAUumoOmCc2HKo0TdtV992w
c0nzXfcwTgYDVR0fBEcwRTBDoEGgP4Y9aHR0cDovL2NybC5lYWR0cnVzdC5ldS91
YWR0cnVzdC1yb290LXJzYTgxOTJlYWRldnBzZDIyMDE5LmNybDB9BggrBgEFBQcB
AQRxMG8wSAYIKwYBBQUHMAKGPGh0dHA6Ly9jYS5lYWR0cnVzdC5ldS9lYWR0cnVz
dC1yb290LXJzYTgxOTJlYWRldnBzZDIyMDE5LmNydDAjBggrBgEFBQcwAYYXaHR0
cDovL29jc3AuZWFkdHJ1c3QuZXUwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUF
BwMCMA0GCSqGSIb3DQEBDQUAA4IEAQDGezJzPVt6JVluaxQLSGg9WHHd8era05Ft
O3h9WO6jZJ0FQUn79hze619uap5Cj6NhLiRXL2HbN2F7HqgU591Cedl1vMsZnCgP
6+itrMfxVSBC5R578SJfjwErezD1P6lylD7r68of3mSn0YdihkVWXE0Ja+uvsNl0
Hl4VjGho9RuSTdbl4sctFifd7C9Y9F+koF2Ge6SUn1CamcnqvM1KC88dBszfCMPt
KiDoLI49B/Plb31f06a6aKk/WZg77hGzi16FOVKHdKkoDOwzv74HTp9JJM/kJVhW
kZj1nEA3yX8KK96+bx0YpGuywuEMTKazfujwWXViam5DDzWB921QeBO0Kwa3ev8L
uHGLbSNyriRhzSvx/Bj3i9r4CoqTTyRPfJA8EkafHjWATXrtqeSI2KrpP6V7m/2X
e66HFfNDdRfVfrOIqjS9+L0rpjFuFrNyG9Wmij1kk2MlMXXf1U5NjYq3m5LXZm4M
COd+3yZfvsqGtDYw5JV8ZfW7i0CbdD+Vfuupvl7yXkP+0rmrPVc3RKtABzkFl1zY
```

Yz4AkJuWfAZ1TSC+e3/zTy01rN9LkKFq2ioOky3GLReTjUmVjMRf/quUsHacbqQZ
mHTwlwjK073vk7kEMlrB+awFGhBVG8vUKfooAAoSr9c27ZkONJcjSjRFTMa1/2l/
oAXxSebF7dILguLA31aiMn0VqMWUnBCYcDgA89EXQ0vGyoWFSzoU5JNOy4gWvvaw
pAvJMo7rAah37sh6OwkrEn8GBLD3m+eeFCaNRd1EnSdIF/PZKn/XLXvbMKIlLFU1
a689HWwVCYQhXkO3WwJBvpNcsCUQKuZQtYGuTVhoj+BiXPzKI9H2ZKyWqbTISvxS
atjEWl+FQ9DCi3jGLAzcQDVCNxs+I7Tx0Ex3nVGg2nsKU61dIbKdPh9hJBkgWsid
5mytHiYuwRbO1Dd8ZHRGOjL/cQwC0WfpB/VQtN4RJiaa0GJjuKAUdJcV4y2y1XIs
E6GZUiRw9kaAcMbmZtTcLwdDCTjzNKSUX6WfYTsfPbxph6y2Ch3t59VG8UmwJO90
kwQiQlVnG4ooFsevgqmmgqTOv59X6KV3sqwAcKWU4MUBvsJiRzQQ5fHL5FSkqx8s
cxruyjXTosvH6iGPONzGKZQGYlA4EVCzMoYncnXykM13GS25eVoQs715ckOPmkfl
e5JWVDn7udyaZCTSRGZaJKonLSFnVC7oEheBCqGe9eL6y4GalcTNHlhTIdXsFGVh
mjc6EAmZ96fB4L6fbFihBglfu1MUnwuARK32EDcSAcvS7Ilc/mZrSm+GXYw0S8nV
bet1gNql98wWM/PJnEVmQrO2JVQ2BsR/j9eiHFc6qKmC1/SZK9lP
-----END CERTIFICATE----

17.8.2 EADTrust RSA 2048 Root CA For Non-Qualified Certificates 2019

-----BEGIN CERTIFICATE-----
MIIEbzCCA1egAwIBAgIIUWWJVGFyGTAwDQYJKoZIhvcNAQELBQAwgaAxRjBEBgNV
BAMMPUVBRFRydXN0IFJTQSAyMDQ4IFJvb3QgQ0EgRm9yIE5vbi1RdWFsaWZpZWQg
Q2VydGlmaWNhdGVzIDIwMTkxLzAtBgNVBAoMJkV1cm9wZWFuIEFnZW5jeSBvZiBE
aWdpdGFsIFRydXN0LCBTLkwuMQswCQYDVQQGEwJFUzEYMBYGA1UEYQwPVkFURVMt
Qjg1NjI2MjQwMCAXDTE5MDYwNjExNDkzMFoYDzIwNTEwNTI5MTE0OTMwWjCBoDFG
MEQGA1UEAww9RUFEVHJ1c3QgUlNBIDIwNDggUm9vdCBDQSBGb3IgTm9uLVF1YWxp
ZmllZCBDZXJ0aWZpY2F0ZXMgMjAxOTEvMC0GA1UECgwmRXVyb3BlYW4gQWdlbmN5
IG9mIERpZ2l0YWwgVHJ1c3QsIFMuTC4xCzAJBgNVBAYTAkVTMRgwFgYDVQRhDA9W
QVRFUy1CODU2MjYyNDAwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC2
6Guzxu4fwaJwcrUUvfbHKJewhuRrviqFNohy5x2cTgu8/X5R9Etb+KlOJl5JGkW8
i/05VFebp4Fq1c99Ia3GAzSbJXSw6yo0Yj5qBR6L81WHCMflpYlZqB7IL6iPfYfj
nR8ukVxsmeAAVsP2+7y/KnjoIdhQC7SL7XQ522kYZlbNZSXFpStH+yB6IzxCV/Bb
BCaaGDd3qD76qBMGqL2MJmWtNOXJ/v+ACFEPnSjbT+rLNqa75RWJFTVD4MOgKmkw
+1dNBjue3AEJdTRWc9tpKV48xpRDZdgZsQZKiL+sydpzv+qZw7Ek+Cq19yEWyTnf
swqzI0NC2Q+LEDIjzfKHAgMBAAGjgagwgaUwDwYDVR0TAQH/BAUwAwEB/zAOBgNV
HQ8BAf8EBAMCAQYwYwYDVR0RBFwwWoEOY2FAZWFkdHJ1c3QuZXWGFmh0dHA6Ly93
d3cuZWFkdHJ1c3QuZXWGFWh0dHA6Ly9jYS5lYWR0cnVzdC5ldYYZaHR0cDovL3Bv
bGljeS5lYWR0cnVzdC5ldTAdBgNVHQ4EFgQUHj9OU0LYXX1X0p370mwGG1FA288w
DQYJKoZIhvcNAQELBQADggEBACb5V/l+mUXJ3yzP/xnShKvg8RRSzTzQTctso+Xx
gSpqzEiTyPXZn+rn9AZki6MjT+QEe8u+Rw7eDJHRTF7q8VvvJ2Ha/mYV9ecyKRQD
AiqNzAGhDnHEayPTFH1fdyMKwLH5JzXlR0D/lfEk0UWYS1cgF0xPLzRP/OZHDiMY
3S9Jiuzy9bJNUfEbOy9vzfN/kKwgAiz+Yq7nI+LY6XALriqwI83PuvO5yEBXPmGD
BaVwUIbSLz/WqfWkFIz97zK+KmAZwkoyAHVKgFy44OWCPRVjJm/8QY/9bDFspUX1
h/1i6Lb9ARdsTIHLuHMt3TdTqTdJy/iAeTyy+6DfgTV5g1k=
-----END CERTIFICATE-----

17.8.1 EADTrust RSA 2048 SubCA For Non-Qualified Certificates 2019


```
-----BEGIN CERTIFICATE-----
MIIGaDCCBVCgAwIBAgIIR0EHGHZZVkkwDQYJKoZIhvcNAQELBQAwgaAxRjBEBgNV
BAMMPUVBRFRydXN0IFJTQSAyMDQ4IFJvb3QgQ0EgRm9yIE5vbi1RdWFsaWZpZWQg
Q2VydGlmaWNhdGVzIDIwMTkxLzAtBgNVBAoMJkV1cm9wZWFuIEFnZW5jeSBvZiBE
aWdpdGFsIFRydXN0LCBTLkwuMQswCQYDVQQGEwJFUzEYMBYGA1UEYQwPVkFURVMt
Qjg1NjI2MjQwMB4XDTE5MDYwNjExNDkzMloXDTM1MDYwMjExNDkzMlowgZ4xRDBC
BgNVBAMMO0VBRFRydXN0IFJTQSAyMDQ4IFN1YkNBIEZvciBOb24tUXVhbGlmaWVk
IENlcnRpZmljYXRlcyAyMDE5MS8wLQYDVQQKDCZFdXJvcGVhbiBBZ2VuY3kgb2Yg
RGlnaXRhbCBUcnVzdCwgUy5MLjELMAkGA1UEBhMCRVMxGDAWBgNVBGEMD1ZBVEVT
LUI4NTYyNjI0MDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAN6kUKdb
TiD/z68si8qvnGoJyr80GkHl5yaorZto0c1BeSNCu8Xna8DBvWHtBm6nFqoMIpXB
aKUGXCCNY0FeXSDYOg3XnUsJJm88aaosRs+DpXPiCrJuoGWeH9q7ASnE2ty14X2T
lK/+tuozxx3qG+oSlZk0wC+DroHbTDeTrfqFjRgycmL8NSa0l6+OwidXNx/63q4l
X7pu/7TyxcyTC/ujrpsSHGrEXFyG9QdzfmokcDjBIx/iEZZuGghs+1b1XHr2UFAj
Qne1ueZHUoLM+uXXYeFoAqbbUDs7lGW7iJ+Z5MURs/idrWUAuNl6ferJE9W3kkGr
5Lc0DBuSIMknNEsCAwEAAaOCAqQwggKgMIGoBgNVHSAEgaAwgZ0wBgYEVR0gADCB
kgYNKwYBBAGDdQIBAQGpIDCBgDAlBggrBgEFBQcCARYZaHR0cDovL3BvbGljeS5l
YWR0cnVzdC5ldTBXBggrBgEFBQcCAjBLDElTdWJvcmRpbmF0ZSBDZXJ0aWZpY2F0
ZSBBdXRob3JpdHkuIEV1cm9wZWFuIEFnZW5jeSBvZiBEaWdpdGFsIFRydXN0LCBT
LkwuMBIGA1UdEwEB/wQIMAYBAf8CAQAwDgYDVR0PAQH/BAQDAgGGMB0GA1UdDgQW
BBTn6+kvcuv5Wb19UOlOGNDPKFkXIjBjBgNVHRIEXDBagQ5jYUBlYWR0cnVzdC5l
dYYWaHR0cDovL3d3dy5lYWR0cnVzdC5ldYYVaHR0cDovL2NhLmVhZHRydXN0LmV1
hhlodHRwOi8vcG9saWN5LmVhZHRydXN0LmV1MGMGA1UdEQRcMFqBDmNhQGVhZHRy
dXN0LmV1hhZodHRwOi8vd3d3LmVhZHRydXN0LmV1hhVodHRwOi8vY2EuZWFkdHJ1
c3QuZXWGGWh0dHA6Ly9wb2xpY3kuZWFkdHJ1c3QuZXUwHwYDVR0jBBgwFoAUHj9O
U0LYXX1X0p370mwGG1FA288wSgYDVR0fBEMwQTA/oD2gO4Y5aHR0cDovL2NybC5l
YWR0cnVzdC5ldS9lYWR0cnVzdC1yb290LXJzYTIwNDhlYWRucTIwMTkuY3JsMHkG
CCsGAQUFBwEBBG0wazBEBggrBgEFBQcwAoY4aHR0cDovL2NhLmVhZHRydXN0LmV1
L2VhZHRydXN0LXJvb3QtcnNhMjA0OGVhZG5xMjAxOS5jcnQwIwYIKwYBBQUHMAGG
F2h0dHA6Ly9vY3NwLmVhZHRydXN0LmV1MA0GCSqGSIb3DQEBCwUAA4IBAQB16M+K
gaegSWpNfR4AIdPBWn2Tr9nRSaNCQ18j4H4MyavrKdyjiLuOvSfQzhYVsxDv8oy1
zmHaG2ZXlIZKic24KiGnzJQ8TerrYBozjmdl9jifyEKLicRIUEojVENKDNQPBcoT
qxHFNPpL5VjOS/ga+s8iKBkBcMNKiCXwVaThq5QYr0fu8Kuf1u5xVlEN02ju82pm
RfHppoDAZycCqFq31VmoMIc3g3hHpdkxmWDc5vAAtKfWAvAlm2VCG6BJLEt/sk7o
219gnZ63MDT6lE0lIkCrWO6sCt5kPgXxRUde6IenbAhfGzcfZ8mPvoTveJpRUEgd
1GARsw6cTjNMK8mg
-----END CERTIFICATE-----
```