17-10-2019

Declaración de Prácticas de Servicios de Confianza (DPC)

Servicios y Certificados

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.

Certificación ISO 9001. ISO 27001 e ISO 20000-1

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

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

Certificados

Norma	Certificado
ISO 20000-1:2011	SGI 6015629/114
ISO 27001:2013	SGI 6015629/19
ISO 9001:2015	SGI 6015629/11

Tabla de Contenidos

1 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	17/10/2019	Versión 2.7	Revisión para consolidar todas las mejoras identificadas en la auditoria eIDAS y las versiones internas de este documento.

TABLA2. HISTORIAL DE VERSIONES.

Propiedades del documento.	
Propietario	EADTrust European Agency of Digital Trust, S.L.
Fecha	09 de octubre de 2019
Distribución	Público
Nombre / Código	OPR-PG- V3.0- Declaración_Prácticas_Certificación_DPC_EADTrust

2 Introducción

Este documento es la **Declaración de Prácticas de Servicios Electrónicos de Confianza** (a partir de ahora, DPC, siglas de la denominación anterior "Declaración de Prácticas de Certificación") de EADTrust European Agency of Digital Trust, S.L. (en adelante, EADTrust). Describe las prácticas empleadas por la Autoridad de Certificación (CA, en inglés) de EADTrust. Estas prácticas se definen según los requisitos del REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y que deroga la Directiva 1999/93/CE (en adelante, **eIDAS**).

Estas prácticas también se definen considerando las recomendaciones técnicas siguientes: Política de certificados y marco de prácticas de certificación RFC3647, Política de Certificados (CP, en inglés) RFC6484 (IETF, 2012), RFC 6844(IETF, 2013) y los Requisitos Básicos de la Política de Certificado para la Emisión y la Gestión de los Certificados de Confianza Pública (CA/Browser Forum, 2019).

EADTrust es un Prestador de Servicios de Confianza Digital radicado en Madrid, España, que opera bajo la supervisión del Ministerio de Economía y Empresa (Secretaría de Estado para el Avance Digital), si bien la denominación del organismo puede cambiar por criterios políticos e incluso adscribirse a diferente Ministerio.

Presta servicios de confianza digital cualificados (definidos en el Reglamento UE 910/2014) y no cualificados (basados en otros enfoques de uso de la criptografía y de la gestión de evidencias digitales). La indicación de servicios "no cualificados" simplemente identifica los servicios de confianza no previstos en el citado Reglamento eIDAS y no indica una menor calidad en el diseño del servicio o su prestación.

EADTrust aplica principios de no discriminación entre sus clientes y sus trabajadores y esta comprometido con los objetivos de sostenibilidad de las NNUU[1].

Esta **Declaración de Prácticas de Servicios Electrónicos de Confianza** se centra en los servicios que EADTrust presta o tiene previsto prestar de entre los alineados con el Reglamento eIDAS, y en particular en su Infraestructura de Clave Pública (ICP, en inglés, PKI, Public Key Infraestructure).

La PKI está diseñada para garantizar mediante certificados digitales la identidad de personas físicas, personas jurídicas y el dominio de internet de sitios web, y dar cobertura a la realización de firmas electrónicas, sellos electrónicos y sellos de tiempo con las claves privadas asociadas a los certificados electrónicos expedidos.

Dentro de estas prácticas, se establece que los servicios de confianza incluyen los siguientes servicios electrónicos normalmente proporcionados a cambio de una remuneración:

- La creación, verificación y validación de certificados cualificados para autenticación y firma electrónica de personas físicas, basados en sus documentos de identidad, tales como el pasaporte, o el DNI.
- La creación, comprobación y validación de certificados cualificados de autenticación y firma electrónica de representant**es legales de personas jurídicas**, basándose en la identificación de documentos de identidad, tales como el pasaporte o el DNI de la persona y en la documentación legal que acredita la representación.

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

- La creación, comprobación y validación de certificados cualificados de autenticación y firma electrónica de **empleados públicos,** basados en sus documentos de identidad y en la documentación legal que acredita su vinculación con el sector público.
- La creación, comprobación y validación de certificados cualificados de autenticación y sello electrónico de **persona jurídica** basándose en la identificación de documentos de identidad, tales como el pasaporte o el DNI del solicitante y en la documentación legal que acredita la representación,
- La creación, comprobación y validación de certificados cualificados de autenticación y sello electrónico de **persona jurídica** sujeta a la normativa PSD2[2] basándose en la identificación de documentos de identidad, tales como el pasaporte o el DNI del solicitante y en la documentación legal que acredita la representación, así como la constancia registral en el registro de entidades del organimo de supervisión financiera del país en el que opera.
- La creaciónde **firmas electrónicas en nombre del firmante usando mecanismos que garanticen con un alto nivel de confianza que se realizan bajo su exclusivo control**, con posibilidad de hacerlo de forma remota, en la nube,
- La creación de **sellos electrónicos en nombre del creador del sello usando mecanismos que garanticen con un alto nivel de confianza que se realizan bajo su exclusivo control**, con posibilidad de hacerlo de forma remota, en la nube
- La creación de **sellos de tiempo electrónicos cualificados,**
- La comprobación y validación de firmas electrónicas, **sellos electrónicos, y** de **sellos de tiempo electrónicos.**
- La creación, verificación y validación de certificados electrónicos orientados a **firmas de aplicación y código,**
- La creación, comprobación y validación de certificados para la autenticación de **sitios web**,
- La **conservación** de firmas electrónicas, sellos o certificados para estos servicios
- **Servicios de entrega electronica certificada.**

Según el Reglamento eIDAS, y dentro del alcance de esta **Declaración de Prácticas de Servicios de Confianza** y las políticas de certificados y servicios, estos se definen como:

TABLA2.NIVEL DE ASEGURAMIENTO DEL CERTIFICADO (LOA, LEVEL OF ASSURANCE EN INGLÉS)

Tipo	Certificado	Policy Identifier	Policy OID	Formato	Nivel de seguridad
Persona física	Individuo	0.4.0.194112.1.0 (QCP-n)	1.3.6.1.4.1.501.2.1.1.0.41221 1.3.6.1.4.1.501.2.1.1.1.41221 0.4.0.194112.1.2	Dispositivo Software HSM/Secure token	Alto Sustancial Alto
	Representante	0.4.0.194112.1.0 (QCP-n) 2.16.724.1.3.5.8 (OID MPR)	1.3.6.1.4.1.501.2.1.1.0.41222 1.3.6.1.4.1.501.2.1.1.1.41222 0.4.0.194112.1.2	Dispositivo Software HSM/Secure token	Alto Sustancial Alto

[2]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

Tipo	Certificado	Policy Identifier	Policy OID	Formato	Nivel de seguridad
	Empleado Público[3]	0.4.0.194112.1.0 (ETSI QCP-n) 2.16.724.1.3.5.7.2	1.3.6.1.4.1.501.2.1.1.0.41223 1.3.6.1.4.1.501.2.1.1.1.41223 0.4.0.194112.1.2	Dispositivo Software HSM/Secure token	Alto Sustancial Alto
	Empleado público (Seudónimo/Firma)	0.4.0.194112.1.2 (ETSI QCP-n-qscd) 2.16.724.1.3.5.4.1	1.3.6.1.4.1.501.2.1.1.1.41224	Dispositivo Software HSM/Secure token	Alto Sustancial Alto
	Empleado público (Seudónimo/ Autenticación)[4]	0.4.0.194112.1.2 (ETSI QCP-n-qscd) 2.16.724.1.3.5.4.1	1.3.6.1.4.1.501.2.1.1.1.41225	Dispositivo Software HSM/Secure token	Alto Sustancial Alto
Entidad legal	Sello corporativo	4.0.194112.1.1 (OID ETSI QCP-l)	1.3.6.1.4.1.501.2.1.1.0.421 1.3.6.1.4.1.501.2.1.1.1.421 0.4.0.194112.1.3	HSM/Secure token Browser HSM	Alto Sustancial Alto
	Sello Corporativo		1.3.6.1.4.1.501.2.1.1.0.3161	HSM/Secure token Browser HSM	No cualificado
	Sello Corporativo	0.4.0.194112.1.1 (OID ETSI QCP-l)	1.3.6.1.4.1.501.2.1.1.0.41231 1.3.6.1.4.1.501.2.1.1.1.41231 0.4.0.194112.1.3	HSM/Secure token Browser HSM	Alto Sustancial Alto
Entidad legal PSD2	Sello Corporativo	0.4.0.194112.1.1 (OID ETSI QCP-l)	1.3.6.1.4.1.501.2.1.1.0.41232 1.3.6.1.4.1.501.2.1.1.1.41232 0.4.0.194112.1.3	HSM/Secure token Browser HSM	Alto Sustancial Alto
Autenticación de sitio web **Autenticación de sitio web**	SSL DV	0.4.0.194112.1.4 (ETSI QCP-w) 2.23.140.1.2.1 (CAB/FORUM DV)	1.3.6.1.4.1.501.2.1.1.0.41241	Software	Sustancial
	SSL OV	0.4.0.194112.1.4 (ETSI QCP-w) 2.23.140.1.2.2 (CAB/FORUM OV)	1.3.6.1.4.1.501.2.1.1.0.41242	Software	Sustancial

[3] 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 1671/2009 y está adaptado a las disposiciones de la Ley 39/2015 de 1 de Octubre, de Procedimiento Administrativo Común de las Administraciones Públicas, la Ley 40/2015 de 1 de Octubre, de Régimen Jurídico del Sector Publico (LRJ) y al Reglamento (UE) 910/2014.

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

Tipo	Certificado	Policy Identifier	Policy OID	Formato	Nivel de seguridad
	SSL EV	0.4.0.194112.1.4 (ETSI QCP-w) 2.23.140.1.1 (CAB/FORUM EV)	1.3.6.1.4.1.501.2.1.1.0.41244	Software	Sustancial
	SSL PSD2	0.4.0.194112.1.4 (ETSI QCP-w) 2.23.140.1.1 (CAB/FORUM EV)	1.3.6.1.4.1.501.2.1.1.0.41243	Software	Sustancial

Este documento especifica la DPC que EADTrust ha establecido para la emisión de certificados y servicios de confianza basados en las siguientes normas:

TABLA 5. CONTEXTO NORMATIVO

Servicio	Norma general	Norma específica	Perfiles
Firma electrónica	EN 319 401 v2.2.1	EN 319 411-1 v1.2.2 EN 319 411-2 v2.2.2	EN 319 412-1 v1.1.1 EN 319 412-2 v2.1.1 EN 319 412-5 v2.2.1
Sellos electrónicos	EN 319 401 v2.2.1	EN 319 411-1 v1.2.2 EN 319 411-2 v2.2.2	EN 319 412-1 v1.1.1 EN 319 412-3 v1.1.1 EN 319 412-5 v2.2.1
Sello de tiempo electrónico	EN 319 401 v2.2.1	EN 319 421 v1.1.1	EN 319 422 v1.1.1
Autenticación de sitio web	EN 319 401 v2.2.1	EN 319 411-1 v1.2.2 EN 319 411-2 v2.2.2	EN 319 412-1 v1.1.1 EN 319 412-4 v1.1.1 EN 319 412-5 v2.2.1

En relación con la expedición de certificados para sitios web, además de cumplir con la normativa técnica y jurídica desarrollada en el marco del Reglamento eIDAS, EADTrust cumple los requisitos denominados “Baseline Requirements” 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

Además, cumplirá los requisitos denominados “Guidelines For The Issuance And Management Of Extended Validation Certificates” para la emisión de dicho tipo de certificados. La versión disponible en la última revisión de esta DPC es la 1.6.9. Además de lo indicado en dicha versión, se han tenido en cuenta los resultados de la aprobación del Ballot SC 17 en relación con la codificación del campo **organizationIdentifier** para incluir datos identificativos específicos necesario para el cumplimiento de la normativa PSD2.Cuando los certificados se expidan a empleados públicos o a personas o entidades que por su relación con las administraciones públicas deban hacer constar determinados datos en los certificados, se tendrán en cuenta las normas que les afecten.

Las normas ya identificadas que afectan a a los perfiles de los certificados son:

- Perfil de certificados 2.0[5] en el marco de la Leyes españolas 39/2015 y 40/2015. Incluye el perfil de certificado de representante.

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

- Perfil de certificados del ámbito judicial aprobado por el CTEAJE en el marco de la Ley 18/2011 española.

Las CAs se organizan en una jerarquía de dos niveles, con diferentes roots, adaptadas a las normas actuales y las mejores prácticas del sector. Se diferencian por algoritmo de clave pública, tamaño de la clave y por diferentes usos de los certificados de entidad final, cualificados y no cualificados. Las jerarquías destinadas a emitir certificados de sitio web no emiten certificados de otro tipo para favorecer la interoperabilidad con los requisitos de CAB Forum.

EADTrust, como CA, emite algunos certificados directamente. Sin embargo, como empresa orientada a servicios, el mercado de certificados se alcanza generalmente a través de sus Autoridades de Registro (AR, en inglés. RA Registration Authority).

Como tal, hay dos formas principales que la RA puede adoptar en la estructura de EADTrust respecto a la verificación de identidad de los solicitantess: inscripción en persona con personación ante una agente de RA e inscripción mediante videoconferencia (también descrita como telepresencia) o videograbación verificada. La plataforma que se esta proyectando emplear, cumplirá con la normativa española publicada por el Servicio de Prevención de Blanqueo de Capitales (SEPBLAC) para videoidentificación [6] y videoconferencia[7] y con la Directiva (UE) 2015/2366 (PSD 2), que se utilizará incluso en los servicios de iniciación de pagos como medio para proporcionar autenticación fuerte de los clientes.

Además, EADTrust también proporciona servicios de confianza más allá del ámbito actual del Reglamento eIDAS, que, por no estar contemplados en dicha normativa se denominan “no cualificados”:

- Comprobación fehaciente de publicaciones en sitios web (Publicación Fehaciente),
- Foro electrónico de accionistas,
- Voto electrónico,
- Custodia de documentos electrónicos,
- Digitalización certificada,
- Custodia de claves privadas para entornos de firmas biométricas,
- Custodia de software de análisis biométrico forense,
- Sistemas de gestión de evidencias electrónicas mediante Blockchain

2.1 Resumen

Esta DPC describe:

- Participantes
- Publicación de los certificados y las Listas de Revocación de Certificados (CRLs, en ingles).
- Cómo se emiten, gestionan, reconfiguran, renuevan y revocan los certificados.
- Gestión de instalaciones (seguridad física, personal, de auditoria, etc.).
- Gestión de la clave.
- Procedimientos de auditoria.

[6] http://www.sepblac.es/espanol/sujetos_obligados/Autorizacion_video_identificacion_11052017.pdf

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

- Temas legales y de negocio.

Esta PKI (infraestructura de clave pública) abarca varios tipos de certificados (ver Sección 2.4 y RFC6480] para más detalles):

- Certificados de CA: para las CAs raíz y subordinadas.
- Certificados de entidad final (EE): que las organizaciones utilizan para validar firmas digitales en objetos firmados con PKI (ver definición en la Sección 2.6).
- En el futuro, la PKI también puede incluir certificados de entidad final en apoyo al control de acceso para el sistema de repositorio, como se describe en la Sección 2.4.

2.2 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

- Iso (1)
- identified-organization (3)
- dod (6)
- internet (1)
- private (4)
- enterprise (1)
- eadtrust (501)
- pki-doc (10)
- statement (1)
- certification-practices (1)

Este documento está disponible en el sitio web de EADTrust (www.eadtrust.eu), de acuerdo con su estado público.

EADTrust ha definido cada tipo de certificado emitido de acuerdo con esta **Declaración de Prácticas de Servicios de Confianza**, asignando diferentes identificadores de objeto a cada uno de ellos. Cada secuencia de OID comienza con el arco de EADTrust: 1.3.6.1.4.1. 501

Además, según la definición ETSI EN 319 412-5, pueden incluirse los siguientes identificadores:

- QcCompliance: certificado cualificado según eIDAS.
- QcSSCD: certificado emitido en un dispositivo cualificado de creación de firma.
- QcRetentiodPeriod: periodo de conservación de la documentación.
- QcPDS: ruta de acceso a los términos de uso, comprensible para terceros que confían en los certificados.
- Qctype: indica el tipo de certificado según eIDAS (para sello electrónico, firma electrónica o autenticación de sitios web).

2.3 Participantes de la PKI

Nótese que en una PKI el término "suscriptor" se refiere a un individuo u organización que es sujeto de un certificado emitido por una CA. El término se utiliza de esta manera a lo largo de todo este documento, sin cualificación, y no debe confundirse con el uso en red del término para referirse a un individuo u

organización que recibe el servicio de un ISP. Obsérvese también que, por razones de brevedad, este documento siempre se refiere a los participantes de PKI como organizaciones o entidades, aunque algunos de ellos sean individuos.

2.3.1 Autoridades de certificación

Como se indica en el resumen anterior, las CAs están organizadas en una jerarquía de dos niveles, con varias CAs raíz offline, adaptadas a las normas y prácticas actuales del sector, desde el punto de vista tecnológico:

Para certificados cualificados web:

- RSA Root CA Web 4096-bit key size with SHA256 digest algorithm (Domain y Organization Validated).
- RSA Root CA Web 8192-bit key size with SHA512 digest algorithm (Domain y Organization Validated).
- ECC Root CA Web P-256 with SHA256 digest algorithm (Domain y Organization Validated).
- ECCRoot CA Web P-384 with SHA384 digest algorithm (Domain y Organization Validated).
- RSA Root CA Web 4096-bit key size with SHA256 digest algorithm (Extended Validation y PSD2).
- RSA Root CA Web 8192-bit key size with SHA512 digest algorithm (Extended Validation y PSD2).
- ECC Root CA Web P-256 with SHA256 digest algorithm (Extended Validation y PSD2).
- ECCRoot CA Web P-384 with SHA384digest algorithm (Extended Validation y PSD2).

Para el resto de certificados cualificados

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

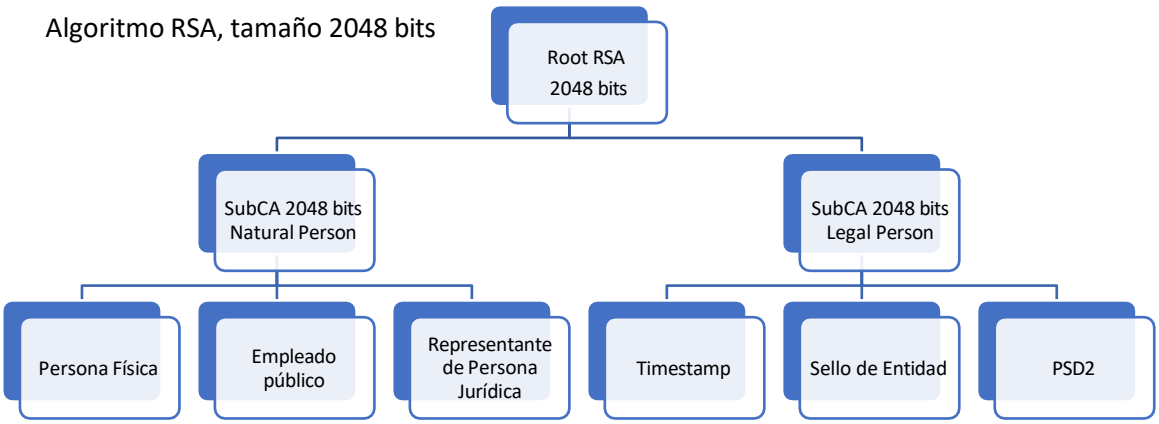
Para certificados no cualificados

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

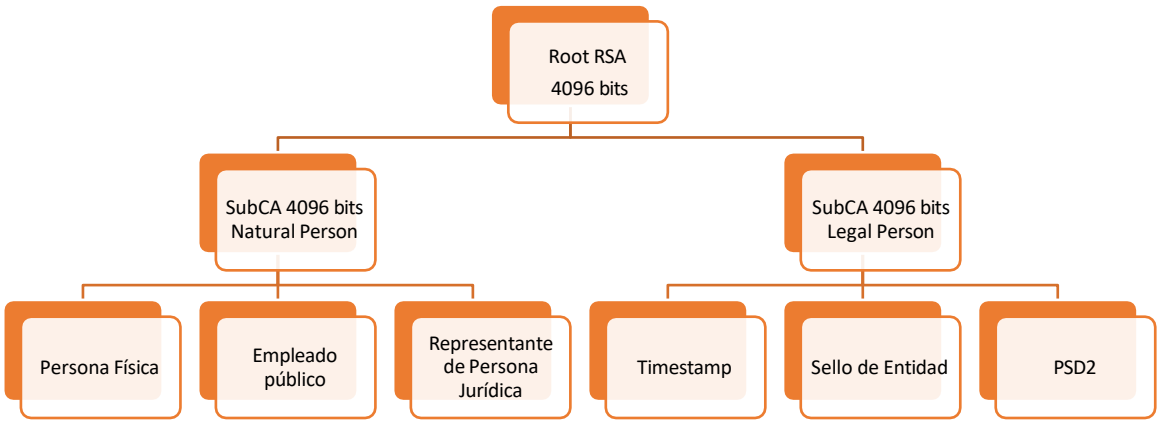
Gráficamente:

Root's Cualificadas para Certificados:

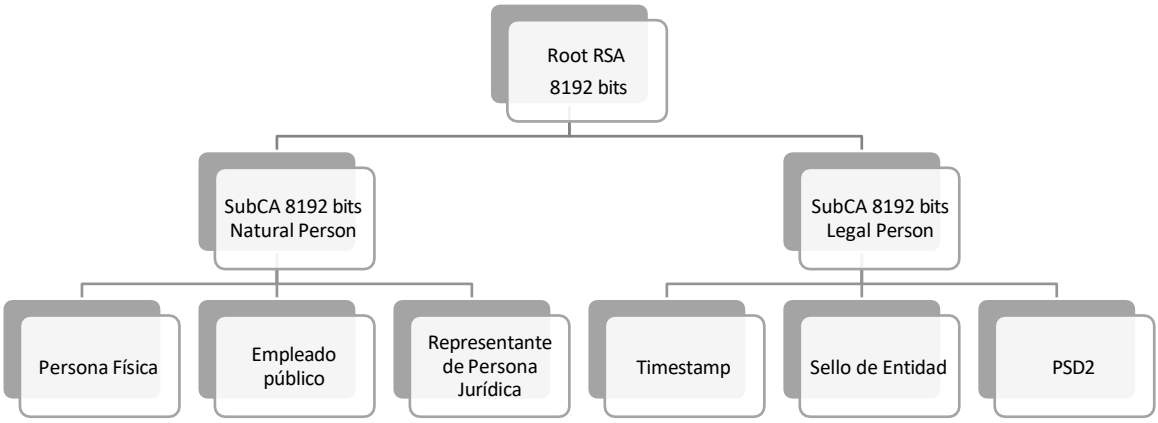
- Algoritmo RSA, tamaño 2048 bits



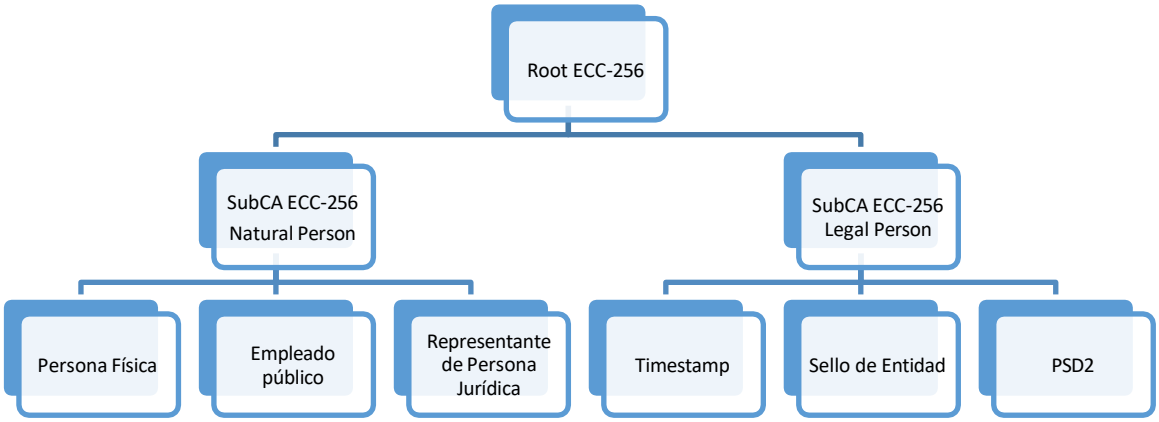
- Algoritmo RSA, tamaño 4096 bits



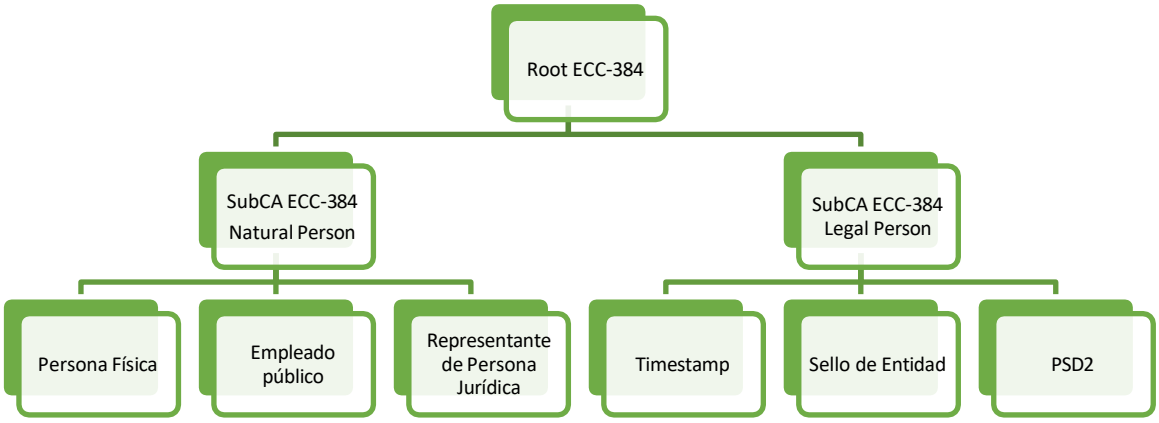
- Algoritmo RSA, tamaño 8192 bits



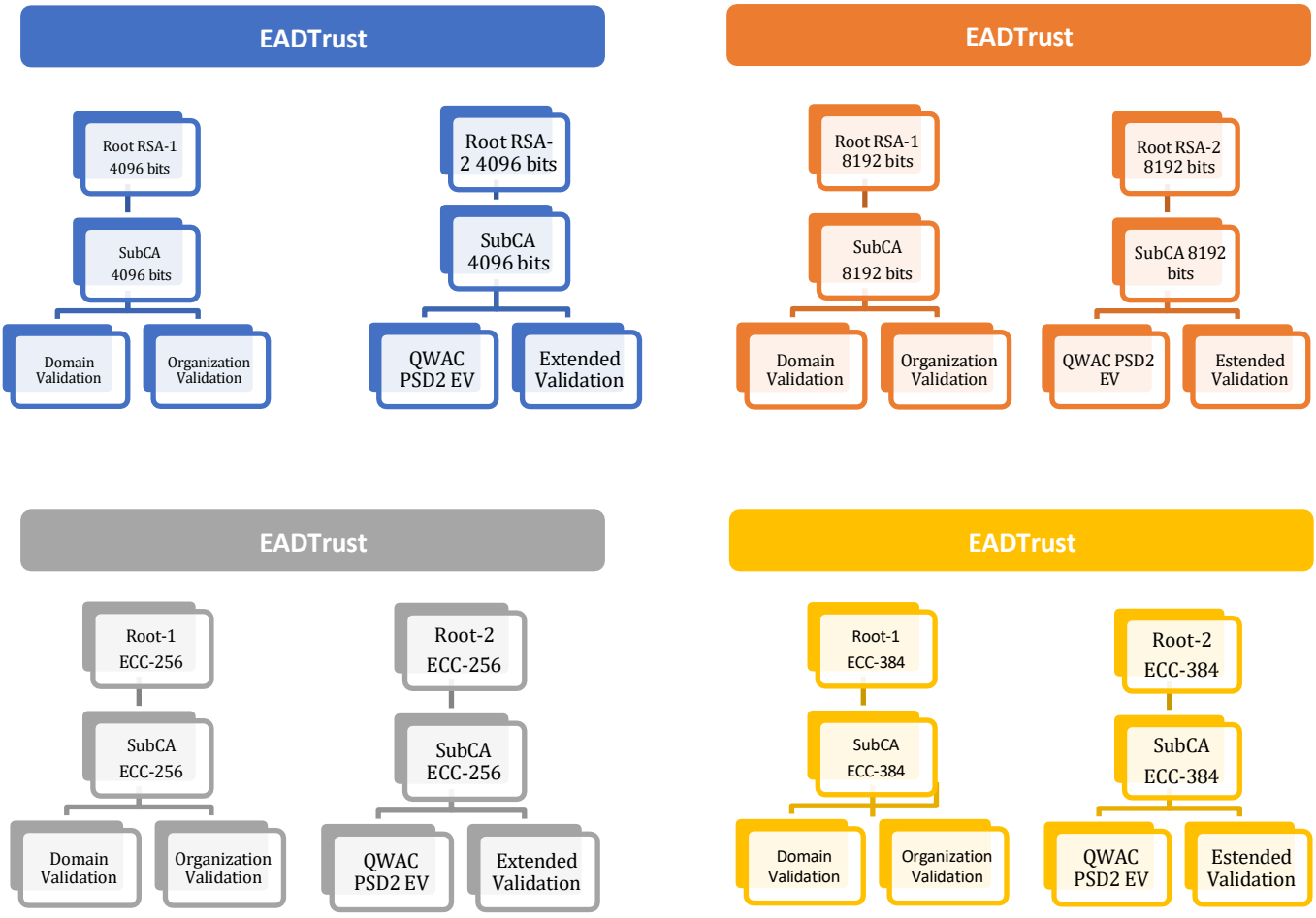
- Algoritmo ECC, tamaño 256 bits



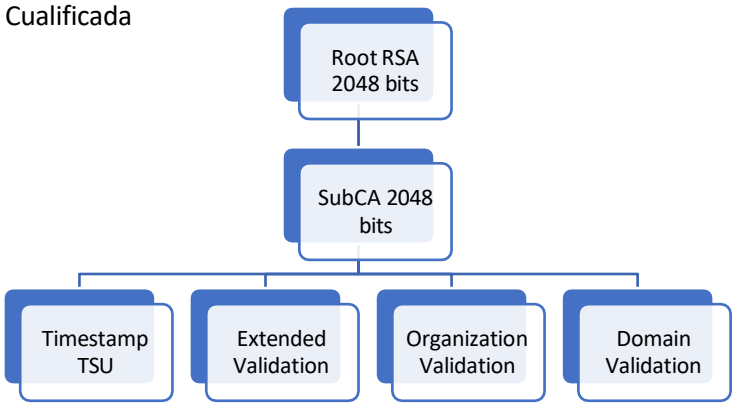
- Algoritmo ECC, tamaño 384 bits



- Root's Cualificadas para Web



- Root NO Cualificada



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

Pueden emitir Certificados bajo la jerarquía EADtrust las Autoridades de Certificación operadas por organizaciones externas cuyas Políticas o DPC (CPS) estén conformes con las Política de Certificación contempladas en en esta DPC (CPS) y hayan sido previamente autorizadas. Existirá una relación escrita formal y contractual con EADTrust para dar cobertura a los compromisos mutuos.

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 un tamaño adicional de clave RSA Root CA de 2048 bits con algoritmo de función compendio o reúmen (hash) SHA256 completamente offline, dedicado 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.

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 Web DV/OV Cert 2019	E016ADB43E92839E8ADD93C6FD2693CEE2F48D13	Root
CN=EADTrust ECC 256 Root CA For Qualified Web EV/PSD2 Cert 2019	48529AB176EA39B4F54C5DC94100A50CA652B3DD	Root
CN=EADTrust ECC 256 Root CA For Qualified Certificates 2019	1FBE6EC155A781C727BC529B533EDA2A0627C567	Root
CN=EADTrust ECC 384 Root CA For Qualified Web DV/OV Cert 2019	3B0E527B93526DDC0845DD6BC375D0BD99F2A4AC	Root
CN=EADTrust ECC 384 Root CA For Qualified Web EV/PSD2 Cert 2019	1B07BD9DD7487BB8D6A718A66077B9A18B87D18A	Root
CN=EADTrust ECC 384 Root CA For Qualified Certificates 2019	FB20B3C5541E4C97DDD31F0B5D71CCD190D14BA8	Root

Denominación	Fingerprint SHA1	Tipo
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 Web DV/OV Cert 2019	09EC23597594A2BC4C9FC323511434A7BC5F4ED8	Root
CN=EADTrust RSA 4096 Root CA For Qualified Web EV/PSD2 Cert 2019	A59FA630D8B62C93EE2C510AF552822A87571707	Root
CN=EADTrust RSA 4096 Root CA For Qualified Certificates 2019	B591E1174767810CC783E5CB07BA1F235FE31560	Root
CN=EADTrust RSA 8192 Root CA For Qualified Web DV/OV Cert 2019	13FF6D569A8BA6BE55A56C1BAE82AE3CF2C663FF	Root
CN=EADTrust RSA 8192 Root CA For Qualified Web EV/PSD2 Cert 2019	C5E3448AAACBE1CBEC4F39C83654D61FF8DFBE82	Root
CN=EADTrust RSA 8192 Root CA For Qualified Certificates 2019	BDABBA2FA168ADD556BDAB8379B7444C2C187859	Root
CN=EADTrust ECC 256 SubCA For Qualified Web DV/OV Cert 2019	CBFE041345914E251554E89257BEDE6234CC70E0	SubCA
CN=EADTrust ECC 256 SubCA For Qualified Web EV/PSD2 Cert 2019	BBB45B672821C66FB8243AEDC0A603C23040E08C	SubCA
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 Web DV/OV Cert 2019	5B26E8460282E847A02D2063543D93D4AD85A190	SubCA
CN=EADTrust ECC 384 SubCA For Qualified Web EV/PSD2 Cert 2019	413A2E207C3CD94D73CF3131F5FADA231D9F70B2	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

Denominación	Fingerprint SHA1	Tipo
CN=EADTrust RSA 4096 SubCA For Qualified Web DV/OV Cert 2019	1C990967E4FF74D852B776FC7C6408A6CC55FCF0	SubCA
CN=EADTrust RSA 4096 SubCA For Qualified Web EV/PSD2 Cert 2019	94E13DE0D28EAACC08E18AD0621157549474686B	SubCA
CN=EADTrust RSA 4096 SubCA For Qualified Certificates 2019/OU=Legal Person	6CFD78D91F9B1839A1A54F72609EDFC893E0DE89	SubCA
CN=EADTrust RSA 4096 SubCA For Qualified Certificates 2019/OU=Natural Person	FADAF7FA8B9FBF505CCD82A75DDBFCB04C8A480B	SubCA
CN=EADTrust RSA 8192 SubCA For Qualified Web DV/OV Cert 2019	B5A00C68743677361D9D3693E9D98DFA61A32CCF	SubCA
CN=EADTrust RSA 8192 SubCA For Qualified Web EV/PSD2 Cert 2019	B2D05C291921EEB0069CB9B8ED9ED12C025E024D	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

2.3.2 Autoridades de registro

Como se indica en el resumen anterior, EADTrust, como CA, emite algunos certificados directamente. Sin embargo, como empresa de servicios, el Mercado de certificados normalmente se alcanza a través de sus Autoridades de Registro (AR, en inglés, RA, Registration Authorities).

Estas RAs son entidades que actúan de acuerdo con las Políticas de Certificación descritas en esta DPC (CPS), junto con una relación escrita formal y contractual con EADTrust. Su objetivo principal es la gestión de relaciones de suscriptores, que incluye la identificación y registro de los suscriptores, las solicitudes de certificados y cualquier otra obligación indicada en esta DPC (CPS), y las políticas específicas de certificados en relación con la gestión del ciclo de vida de los certificados.

Hay dos formas principales que la RA puede adoptar en la estructura de EADTrust respecto a la verificación de identidad de los solicitantess: inscripción en persona con personación ante una agente de RA en persona y se esta implementando la posibilidad de inscripción mediante videoconferencia (también descrita como mediante telepresencia) o videograbación (“digital onboarding”. La plataforma a utilizar cumplirá con la normativa española publicada por el Servicio de Prevención de Blanqueo de Capitales (SEPBLAC) para videoidentificación[8] y videoconferencia[9] y la Directiva (UE) 2015/2366 (PSD 2), que se

[8] http://www.sepblac.es/espanol/sujetos_obligados/Autorizacion_video_identificacion_11052017.pdf

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

utilizará incluso en los servicios de iniciación de pagos como medio para proporcionar autenticación fuerte de los clientes.

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

- Identificación y autenticación de los potenciales suscriptores de certificados.
- Desarrollo de una relación contractual para la emisión de certificados con la entidad final o el suscriptor.
- Generación de certificado (por medio de comunicación autenticada con la CA online) y la entrega del certificado en un dispositivo cualificado de creación de firma o sello (en caso de que se establezca como requisitoen la política de certificado específica).
- Conservación de cualquier documentación relevante y relacionada con la emisión del certificado o con la relación del suscriptor con la RA.
- Proporcionar cualquier información requerida por EADTrust relacionada con sus servicios de certificación y operaciones, en cualquier momento, y, especialmente, durante la evaluación de cumplimiento anual con las Políticas de Certificación de EADTrust.

El período de conservación para cualquier documentación es de 15 años, excepto en aquellos casos en los que se especifique un período de conservación más corto en la política del certificado.

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

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

2.3.3 Suscriptores

2.3.3.1 Entidades finales

Las entidades finales son cualquier persona u organización que reciba servicios de emisión de certificado, gestión y uso de certificados digitales. Entre otros se incluyen (pero no están limitados a estos):

- Solicitantes de certificados, por sí mismos o cualquier otro interesado.
- Suscriptores de certificados que tienen la propiedad del certificado.
- Propietarios de la clave, quienes las utilizan para los propósitos específicos del certificado.
- Terceros representados.
- Terceros que confíen en los certificados.

2.3.3.2 Solicitantes de certificados

Todo certificado debe solicitarse por una persona, en su propio nombre o en el de una entidad con la cual se establece una relación contractual especificando el alcance de la representación.

Por ello, los solicitantes de certificados pueden ser:

- Suscriptor potencial del certificado y, como tal, el propietario de la clave.
- El propietario potencial de la clave, en representación de un suscriptor potencial del certificado.

- Representante, con funciones de representación del suscriptor potencial del certificado, que no debe tener acceso a las claves del certificado.

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.

2.3.3.3 Suscriptores del certificado

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

En los certificados individuales, el suscriptor y el propietario de la clave coinciden. En los certificados en los que ambas figuras no coinciden (como las entidades y los certificados de las organizaciones), el suscriptor suele ser una persona jurídica y el propietario de la clave es una persona física, representante o empleado autorizado por la organización para recibir y utilizar el certificado. En este caso, no sólo el suscriptor firmará el acuerdo correspondiente, sino que cada uno de los propietarios del certificado, recibirá y firmará el documento en el que se le informa de sus obligaciones, en el momento de identificarse ante la RA.

2.3.3.4 Propietarios de la clave

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

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

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

La capacidad del propietario de la clave y el alcance para actuar y operar en lugar del suscriptor real se especificarán, en cada caso, en el certificado, cumpliendo con los requisitos establecidos en esta DPC (CPS) y la política de certificados específicos.

2.3.3.5 Representante del solicitante

Cualquier persona física o jurídica se considerará como representada en caso de que cualquier solicitante de certificado solicite el certificado debidamente identificado y con documentación legal que acredite que actúa en nombre y representación de su constituyente para obtener y gestionar dicho certificado. Esto no será perjudicial para el propietario real del certificado, ni para el representante, que puede ser también un suscriptor individual actuando en su nombre.

2.3.4 Partes que confian

Las entidades o individuos que actúan confiando en certificados u objetos firmados emitidos bajo esta PKI son partes que confian.

Las partes que confían pueden o no ser suscriptores dentro de esta PKI, pero, en cualquier caso, se proporcionarán diferentes canales de comunicación, para que puedan (como deberían) verificar la validez del certificado y su propósito.

Deben comprobar por el campo AIA (Authority Information Access) de los certificados que pueden reconstruir la cadena de confianza desde el certificado de entidad final hasta la autoridad Raiz, y que pueden indentificar el punto de consulta de validez de certificados por el servicio OCSP, o, cuando corresponda, por la lista CRL.

En el caso de los certificados cualificados, deben poder identificar las autoridades incluidas en las listas de confianza TSL administradas por el Organismo de Supervisión correspondiente al país, en España la Secretaría de Estado para el Avance Digital adscrita al Ministerio de Economía y Empresa[10] y por el organismo europeo que consolida las TSL nacionales[11].

Las partes que confían deben conocer y sujetarse a las garantías, límites y responsabilidades aplicables en la aceptación y uso de los certificados en los que confían, y aceptar sujetarse a las mismas. Un resumen de lo que deben conocer se encuentra disponible en el documento PDS (PKI Disclosure Statement), redactado de forma que se facilite la divulgación de los servicios con lenguaje sencillo de forma similar al prospecto de un medicamento.

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

2.4 Uso del certificado

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

2.4.1 Usos adecuados del certificado

Estos Requisitos sirven para informar a los usuarios y ayudarles a tomar decisiones informadas cuando confían en los Certificados.

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

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

[10] https://sede.minetur.gob.es/es-ES/datosabiertos/catalogo/lista-prestadores-tsl

[11] https://ec.europa.eu/digital-single-market/en/eu-trusted-lists-trust-service-providers

Si los certificados se emiten a personas jurídicas 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.

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 pueden usar en equipos de control destinados su utilización en situaciones peligrosas o en los que un mal funcionamiento suponga un peligro para la vida humana o para objetos valiosos. Cualquier uso en estos contextos exime de responsabilidad al Prestador de servicios de confianza digital.

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

2.5 Administración de políticas

2.5.1 Organización que administra el documento

EADTrust, con domicilio social en Calle Alba, 15 de Madrid (España) y NIF B-85626240, es la Autoridad de Certificación que emite los certificados bajo esta Declaración de Prácticas de Certificación (DPC, en inglés CPS, Certification Practice Statement).

2.5.2 Contacto

Nombre del PSC	European Agency of digital Trust, S. L.
Dirección	C/ Alba,15, 28043 Madrid - Spain
Dirección de email	policy@eadtrust.eu
Dirección de email para PSD2	CA-request@eadtrust.eu
Teléfono	(+34) 902365612 / (+34) 917160555

2.5.3 Procedimiento de aprobación de las políticas de certificados

El Órgano de Aprobación y Gestión de Políticas de Certificación de EADTrust aprueba los cambios finales realizados en este documento una vez que determine que cumplen con los requisitos establecidos.

Es posible contactar con el Órgano de Gestión y Aprobación de Políticas de certificados en: E-mail: policy@eadtrust.eu. Las direcciones postales, teléfonos y fax se encuentran publicadas en https://www.eadtrust.eu.

2.6 Definiciones y acrónimos

Afiliado: Empresa, asociación, joint venture u otra entidad que controle, esté controlada por o bajo control común por otra entidad, o agencia, departamento, subdivision política o cualquier entidad que actúe bajo el control directo de una entidad gubernamental.

Solicitante: La persona física o jurídica que solicita (o busca la renovación de) un Certificado. Una vez que el Certificado es emitido, nos referimos al Solicitante como el Suscriptor. Para Certificados emitidos a dispositivos, el Solicitante es la entidad que controla u opera el dispositivo nombrado en el Certificado, incluso si el dispositivo está enviando la solicitud de certificado real.

Representante del Solicitante: Persona física o un representante que sea el Solicitante empleado por el Solicitante o un agente autorizado que tenga autoridad expresa para representar al Solicitante: (i) que firme y envíe, o apruebe una solicitud de certificado en nombre del Solicitante, y o (ii) que firma y envía un Acuerdo de Suscriptor en nombre del Solicitante, y / o (iii) que reconoce las Condiciones de Uso en nombre del Solicitante cuando el Solicitante es un Afiliado de la CA o es la CA.

Proveedor de software de aplicación: Proveedor de software de navegador de Internet u otro software de aplicación de confianza que muestra o utiliza certificados e incorpora Certificados Raíz.

Carta de Certificación: Carta que atestigua que la Información del Sujeto está escrita de forma correcta por un contable, abogado, funcionario del gobierno u otro tercero confiable en el que se suele confiar para tal información.

Informe de Auditoría: Informe de un Auditor Cualificado que declara la opinión del Auditor cualificado sobre si los procesos y controles de una entidad cumplen con las disposiciones obligatorias de estos Requisitos.

Nombre de Dominio de Autorización: Nombre de Dominio utilizado para obtener autorización para la emisión de certificados para un FQDN (fully qualified domain name) determinado. La Autoridad de Certificación puede utilizar el FQDN devuelto de una búsqueda DNS CNAME como un FQDN con el propósito de validación de dominio. Si el FQDN contiene un carácter comodín, entonces la CA DEBE eliminar todas las etiquetas de character comodín de la parte izquierda del FQDN solicitado. La CA puede suprimir cero o más etiquetas de izquierda a derecha hasta encontrar un Nombre de Dominio Base y puede utilizar cualquiera de los valores intermedios con el propósito de la validación del dominio.

Puerto autorizado: Uno de los puertos siguientes: 80 (http), 443 (https), 115 (sftp), 25 (smtp), 22 (ssh).

Nombre de dominio base: La parte de un sufijo controlado o público aplicado –para un FQDN[12] que es el primer nodo de nombre de dominio que queda de un registro – más el registro (por ejemplo, "example.co.uk" o "example.com "). Para los FQDN en los que el nodo de nombre de dominio más a la derecha es un gTLD que tiene la Especificación 13 de ICANN en su acuerdo de registro, el gTLD en sí puede utilizarse como el Nombre de Dominio de Base.

CAA: De RFC 6844 (http: tools.ietf.org/html/rfc6844): "El Registro de recursos DNS de Autorización de Autoridad de Certificación (CAA) permite a un titular de nombre de dominio DNS especificar las Autoridades de Certificación (CA) autorizadas para emitir certificados para ese dominio. La publicación de los registros de recursos de CAA permite a una Autoridad de Certificación pública implementar controles adicionales para reducir el riesgo de errores no intencionados en el certificado ".

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

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.

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.

Informe de Problemas del Certificado: Consiste en una queja sobre una sospecha de Compromiso de la Clave, uso incorrecto del Certificado, u otros tipos de fraude, compromise, mal uso o conducta inapropiada relacionada con los 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.

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.

Declaración de Prácticas de Certificación: Uno de varios documentos que forman el marco de gobierno en el cual los Certificados son creados, emitidos, administrados y usados.

Control: "Control" (y sus significados correlativos, "controlado por" y "bajo control común de") significa la posesión, directa o indirectamente, del poder de: (1) dirigir la dirección, gestión, finanzas o planes de dicha entidad; (2) controlar la elección de la mayoría de los directores; o (3) votar la parte de las acciones con derecho a voto necesaria para el "control" bajo la ley de la Jurisdicción de Incorporación o Registro de la entidad, pero en ningún caso inferior al 10%.

CSPRNG: «Cryptographically Secure PseudoRandom Number Generator» Generador de números aleatorios seguro destinado a ser utilizado en el sistema criptográfico.

[12]Fully qualified domain name

Tercera persona delegada: Persona física o entidad jurídica que no es la CA, pero está autorizada por la CA para ayudar en el Proceso de Administración de Certificados mediante la realización o el cumplimiento de uno o más de los requisitos de la CA que se encuentran aquí.

Documento de autorización de dominio: Documentación proporcionada por, o documentación de CA de una comunicación con, un Registro de Nombres de Dominio, el Registrador de Nombres de Dominio o la persona o entidad enumerada en WHOIS como Registrador de Nombres de Dominio (incluyendo cualquier servicio de registro privado, anónimo o proxy) que acredite la autoridad de un Solicitante para solicitar un Certificado para un Espacio de Nombre de Dominio específico.

Contacto de Dominio: El Registrador de Nombre de Dominio, contacto técnico o contrato administrativo (o el equivalente bajo un ccTLD) como se indica en el registro WHOIS del Nombre de Dominio de Base o en un registro de SOA de DNS.

Nombre de Dominio: La etiqueta asignada a un nodo en el Sistema de Nombres de Dominio.

Espacio de Nombres de Dominio: Conjunto de todos los Nombres de Dominio posibles que están subordinados a un solo nodo en el Sistema de Nombres de Dominio.

Registrador de Nombres de Dominio: A veces se le denomina "propietario" de un Nombre de Dominio, pero, más apropiadamente, es tanto la persona o entidades registradas con Registrador de Nombres de Dominio con el derecho a controlar cómo se utiliza un Nombre de Dominio, como como la persona física o Entidad Legal que aparece como "Registrante" por WHOIS o el Registrador de Nombres de Dominio.

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

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

Nombre de Dominio Completamente Cualificado: Nombre de Dominio que incluye las etiquetas de todos los nodos superiores en el Sistema de Nombre de Dominio de Internet.

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.).

Solicitud de Certificado de Alto Riesgo: Solicitud que la CA marca para un escrutinio adicional por referencia a criterios internos y bases de datos mantenidas por la CA, que pueden incluir nombres con mayor riesgo de phishing u otros usos fraudulentos, nombres contenidos en solicitudes de certificados previamente rechazadas o Certificados revocados, nombres listados en la Lista de phishing de Miller Smiles o en la Lista de Navegación Segura de Google o los nombres que la entidad de certificación identifica utilizando sus propios criterios de mitigación de riesgos.

Nombre Interno: Cadena de caracteres (no una dirección IP) en un campo Nombre Común o Nombre Alternativo de Sujeto de un Certificado que no se puede verificar como globalmente único dentro del DNS público en el momento de la emisión del certificado porque no termina con un Dominio de Nivel Superior registrado en la base de datos de la Zona Raíz de IANA.

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

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.

Script de Generación de Clave: Plan documentado de procedimientos para la generación del par de claves de la CA.

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

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

Identificador de Objeto: Identificador único numérico o alfanumérico registrado bajo las normas aplicables de la Organización Internacional de Normalización para un objeto o clase de objeto específico.

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.

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.

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.

Auditor Cualificado: Persona física o Entidad Legal que evalúa la conformidad con los requisitos de acuerdo a los requerimientos cualificados.

Valor Aleatorio: Valor especificado por una CA al Solicitante que muestra al menos 112 bits de entropía.

Nombre de Dominio Registrado: Nombre de dominio que se ha registrado con un Registrador de Nombres de Dominio.

Autoridad de Registro (RA): Cualquier Entidad Jurídica que sea responsable de la identificación y autenticación de los sujetos de Certificados, pero no es una CA, y por lo tanto no firma ni emite 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, pero puede ser parte de la CA.

Fuente de Datos Confiable: Documento de identificación o fuente de datos utilizada para comprobar la Información de la Identidad del Sujeto que es normalmente reconocida por las empresas comerciales y los gobiernos como confiable y que fue creada por un tercero con un propósito distinto al de que el Solicitante obtenga un Certificado.

Método Confiable de Comunicación: Método de comunicación, como una dirección de entrega postal / mensajería, número de teléfono o dirección de correo electrónico, comprobada utilizando una fuente distinta al Representante del Solicitante.

Parte 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.

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.

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.

Sujeto: Persona física, dispositivo, sistema, unidad o entidad jurídica identificada en un Certificado como el Sujeto. El Sujeto es tanto el Suscriptor como un dispositivo bajo control y operación del Suscriptor.

Información de Identidad del Sujeto: Información que identifica al Sujeto del Certificado. La información de la Identidad del Sujeto no incluye un nombre de dominio que aparezca en la extensión subjectAltName ni en el campo Subject commonName.

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

Suscriptor: Persona física o jurídica a la que se expide un Certificado y que está legalmente obligada por un Acuerdo de Suscriptor o Términos de Uso.

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

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.

Términos de Uso: 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.

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.

Sistema Confiable: Hardware, software y procedimientos informáticos que son razonablemente seguros contra intrusiones y mal uso; proporcionan un nivel razonable de disponibilidad, fiabilidad y funcionamiento correcto; son razonablemente adecuados para realizar sus funciones previstas; y garantizan el cumplimiento de la política de seguridad aplicable.

Nombre de Dominio no Registrado: Un Nombre de Dominio que no es un Nombre de Dominio Registrado.

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

Especialistas de Validación: Persona que realiza los deberes de comprobación de la información especificada por estos Requisitos.

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

Certificado Wildcard: Certificado que contiene un asterisco (*) en la posición más a la izquierda de cualquiera de los Nombres de Dominio de Sujeto Completamente cualificados contenidos en el Certificado.

2.6.1 Acrónimos

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.

2.6.2 Referencias

ETSI TS 119 612, Electronic Signatures and Infrastructures (ESI); Trusted Lists

ETSI EN 319 403, Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers.

ETSI EN 319 401 V2.2.1 (2018-04) - Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

ETSI EN 319 411-1 V1.2.2 (2018-04) - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

ETSI EN 319 411-2 V2.2.2 (2018-04) - 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.

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.

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[13].

CAB Forum - Baseline Requirements[14]. Ultima version consultada: BR1.6.5[15]

CAB Forum - Guidelines for The Issuance and Management of Extended Validation Certificates.

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

2.6.3 Convenciones

Los términos no definidos en este documento pueden estar definidos en los acuerdos aplicables, manuales de usuario, Políticas de Certificado y Declaraciones de Prácticas de Certificación de la CA.

3 Responsabilidades de publicación y repositorio

3.1 Repositorios

La CA proporciona información de revocación para los Certificados Subordinados y los Certificados de Suscriptor disponibles de acuerdo con esta DPC (CPS).

La URL en la que está disponible la información de revocación (y que se indica en el campo AIA del certificado) es:

- ocsp.eadtrust.eu

Además, la posible revocación de las CA raíz y las CAs subordinadas quedará registrada en la URL:

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

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

[15] https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.6.5.pdf

- crl.eadtrust.eu

Las políticas de certificación, la declaración de prácticas de certificación y la declaración abreviada para terceros que confían (PDS, Policiy Disclosure Statement) estarán disponles en la URL:

- policy.eadtrust.eu

3.2 Publicación de la información de certificación

La CA divulga públicamente sus Políticas de Certificados (habitualmente, formando parte de a DPC) y la Declaración de Prácticas de Certificación a través de su web (un medio on line apropiado y fácilmente accesible que esta disponible 24 horas al día, 7 días a la semana). EADTrust divulga públicamente sus prácticas empresariales de Certificación en la medida requerida por el esquema de auditoría seleccionado de la CA (ver Sección “Auditoría de cumplimiento y otras evaluaciones”).

La URL en la que está disponible la información de políticas y la Declaración de Prácticas de Certificación es:

- policy.eadtrust.eu

La divulgación incluye todo el material requerido por la norma RFC 3647 y se estructura de acuerdo con dicha norma.

La CA destinada a la emisión de certificados para SSL/TLS se ajusta a la versión actual de los Requisitos Básicos para la Emisión y Gestión de Certificados de Confianza Pública publicados en http://www.cabforum.org. En caso de cualquier incoherencia entre este documento y los Requisitos, dichos Requisitos prevalecerán sobre este documento.

EADTrust aloja páginas web de prueba que permiten a los Proveedores de Software de Aplicación probar su software con Certificados de Suscriptor que encadenan cada Certificado Raíz de confianza pública. EADTrust aloja páginas web separadas utilizando Certificados de Suscriptor de diversos tipos: (i) válidos, (ii) revocados y (iii) expirados.

Los dominios de los sitios web de pruebas responden a esta estructura:

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

- https://rsa-4096-ov-tst.eadtrust.eu/
- https://rsa-4096-psd2-tst.eadtrust.eu/
- https://rsa-8192-dv-tst.eadtrust.eu/
- https://rsa-8192-ev-tst.eadtrust.eu/
- https://rsa-8192-ov-tst.eadtrust.eu/
- https://rsa-8192-psd2-tst.eadtrust.eu/

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.

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

3.3 Tiempo o frecuencia de publicación

EADTrust se compromete a desarrollar, implementar, hacer cumplir y actualizar con periodicidad 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 destinada a la emisión de certificados para SSL/TLS serán anuales.

4 Identificación y autenticación

4.1 Nombre

4.1.1 Tipos de nombres

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

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

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

- Common Name: El nombre en texto libre del suscriptor, autorizado por la Entidad de Registro.

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

- policy.eadtrust.eu

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

- **Persona física:** En certificados correspondientes a personas físicas la identificación del signatario estará formada por su nombre y apellidos, más su número de identificación de los admitidos en la norma EN 319 412-1.
- **Persona física - representante persona juridica:** Determina la relación de representación legal o de apoderado general entre la persona física (titular del certificado/Sujeto/Firmante) y una entidad con personalidad jurídica. .
- **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.

4.1.2 Necesidad de que los nombres sean significativos

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

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

4.1.3 Anonimidad o pseudonimidad de los suscriptores

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

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

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

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

4.1.4 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.

4.1.5 Normas para interpretar diferentes formas de nombres

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

- **X.509 -** ISO/IEC 9594-8[16]
- X.520 -ISO/IEC 9594-6[17]

4.1.6 Singularidad de los nombres

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

4.2 Validación inicial de la identidad

4.2.1 Método para probar la posesión de la clave privada

Se demuestra que la clave privada está con un alto nivel de confianza bajo control exclusivo del solicitante, de varias formas según el procedimiento de solicitud de certificado seguido.

Cuando se genera el par de claves por la CA o la RA:

- 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 que contienen el certificado y el par de claves almacenados de forma segura.
- 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

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

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

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.

- Si las claves se generan y se almacenan en un HSM asociado a un servicio de firma electrónica o de sello electrónico en la nube, en el que el prestador del servicio actúa en nombre del firmante o del creador del sello electrónico, la prueba de posesión de la clave privada se demuestra en virtud del procedimiento confiable de entrega y aceptación del certificado asociado a la solicitud vinculada al HSM y la posesión o entrega de las claves de control del servicio de firma o sello por el solicitante, para lo que se podrá hacer uso de técnicas de comunicación de doble factor de autenticación (por ejemplo, un mensaje de correo electrónico o un SMS). Solo se admite esta modalidad de expedición de certificados si el servicio de firma electrónica o de sello electrónico en la nube, lo proporciona un prestador de servicios de confianza cualificado.

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.

4.2.2 Autenticación de la organización e identidad del dominio

Como parte del proceso de autenticación de EADTrust, en el caso de expedición de certificados de persona física representante, de persona jurídica y de certificados para servidor web, se valida el nombre de la organización introducido durante la inscripción, que se hace constar en el campo apropiado del certificado.

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

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

Si la entidad hace uso en su DNS de las extensiones [18] que restringen la emisión de certificados a determinados Prestadores de Servicios de Certificación, EADTrust solo emitirá certificados de servidor web en caso de que se indique expresamente esta preferencia. EADTrust revisa los registros CAA (Certification Authority Authorization) al comprobarlos datos de Dominios Completamente Cualificados dejando constancia de las acciones de comprobación en sus registros y logs.

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

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

4.2.3 Autenticación de la identidad individual

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

Si en un futuro EADTrust implementara el servicio mediante identificación a distancia, se dará cumplimiento a los controles definidos en las siguientes normas de SEPBLAC:

- Autorización de procedimientos de vídeo-identificación[19]
- Autorización de procedimientos de identificación no presencial mediante videoconferencia[20]
- Autorización de procedimiento de identificación no presencial[21]

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

- BAFIN (Alemania) - Circular 3/2017 (GW) - video identification procedures[22]
- Gabinete Nacional de Segurança (Portugal) - Despacho 154/2017 da Entidade Supervisora nacional, de 5 de dezembro Relativo à Identificação de pessoas físicas através de procedimentos de identificação à distânciacom recurso a videoconferência[23].

4.3 Identificación y autenticación para la solicitud de revocación

El inicio de una solicitud de revocación se produce:

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

[19] http://www.sepblac.es/espanol/sujetos_obligados/Autorizacion_video_identificacion_11052017.pdf

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

[21] http://www.sepblac.es/espanol/sujetos_obligados/autorizacion_procedimiento_identificacion_no_presencial.pdf

[22] https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Rundschreiben/2017/rs_1703_gw_videoident_en.html

[23] https://www.gns.gov.pt/media/10442/Despacho-154-2017-ID-Videoconferencia.pdf

5 Requisitos operacionales del ciclo de vida del certificado

Esta Declaración de Prácticas de Certificación regula los requisitos operativos comunes para los certificados emitidos.

La normativa específica para cada tipo de certificado debe consultarse en la documentación específica de cada certificado. El usuario genera su clave privada y luego emite su solicitud.

5.1 Solicitud del certificado

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

5.1.1 Quién puede enviar una solicitud del certificado

Pueden solicitar un certificado las personas que necesiten:

- Autenticar la identidad de un usuario, de forma electrónica, ante terceros
- Firmar o sellar documentos o transacciones digitalmente de forma que se garantice la integridad de los datos trasmitidos y su procedencia.
- Cifrar datos para que solo el destinatario del documento pueda acceder a su contenido. En este caso, es recomendable contar con un procedimiento de respaldo de claves privadas, dado que, si se produjera alguna incidencia con ellas, EADTrust no tiene posibilidad de proporcionarlas.
- Los representantes de personas jurídicas que requieran realizar sellos digitales o que requieran el uso de comunicaciones cifradas en servidores web.

5.1.2 Proceso de inscripción y responsabilidades

Las tareas de identificación y validación de la información en el certificado y validación y aprobación de las solicitudes de emisión, revocación y renovación serán realizadas por las Oficinas de Registro.

Las Oficinas de Registro Propias de EADTrust o de las entidades usuarias con las que EADTrust firme el correspondiente instrumento legal deberán asumir las siguientes obligaciones:

- Validar la identidad y otros detalles personales del solicitante, del suscriptor y del propietario de la clave en los certificados o la información relevante para el fin de los certificados según estos procedimientos.
- Mantener toda la información y documentación relativa a los certificados, y gestionar su emisión, renovación, revocación o reactivación.
- Notificar a EADTrust sobre las solicitudes de revocación de certificados con la debida diligencia y de una manera rápida y confiable.
- Permitir a EADTrust el acceso a sus archivos de procedimiento y registros de auditoría para desempeñar sus funciones y mantener la información necesaria.
- Informar a EADTrust sobre las solicitudes de emisión, renovación, reactivación y cualquier otro aspecto relacionado con los certificados emitidos por EADTrust.

- Validar, con la debida diligencia, las circunstancias de revocación que puedan afectar a la validez del certificado.
- Cumplir con los procedimientos establecidos por EADTrust y con la legislación vigente en esta materia, en sus operaciones de gestión relacionadas con la emisión, renovación y revocación de certificados.
- Cuando proceda, puede realizar la función de poner a disposición del titular de la clave los procedimientos técnicos para la creación de firmas (clave privada) y la comprobación de la firma electrónica (clave pública).

5.2 Procedimiento de solicitud de certificado

Una vez haya tenido lugar una petición de certificado, el operador de la RA mediante el acceso a la plataforma de gestión verifica que la información proporcionada es correcta.

5.2.1 Realización de funciones de identificación y autenticación

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

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

En relación con las medidas de seguridad adoptadas por los diferentes países miembros de la unión europea en relación con los documentos de identidad, se toman en consideración los datos recogidos en la plataforma PRADO (Registro Público de Documentos Auténticos de Identidad y de Viaje en Red)[24]. Para una referencia respecto a los términos utilizados, se recomienda acceder al Glosario[25].

Características difractivas:

- Hologramas
- Identigramas
- Estructuras cinemáticas (Kinegramas)

Técnicas de personalización:

- Imagen láser cambiante
- Tipografía

Material:

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

[24] http://www.consilium.europa.eu/prado/es/prado-start-page.html

[25] https://www.consilium.europa.eu/prado/ES/prado-glossary/prado-glossary.pdf

Impresión de seguridad:

- Microimpresión
- Estructuras de guilloché

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

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

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

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

En el caso de los certificados PSD2 se comprueba que la entidad figura inscrita en alguno de los registros mantenidos por las Autoridades Competentes del país en el que se realiza la supervisión. Una vez realizada la verificación EADTrust informará por email a las Autoridades Competentes que hubieran proporcionado ese dato de contacto sobre la emisión de un certificado a entidades de su ámbito de competencia

5.2.2 Aprobación o rechazo de solicitudes de certificado

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

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

En el proceso de expedición de certificados “Extended Validation” se aplicarán controles duales, de modo que la decisión de expedición del certificado no la pueda tomar la misma persona que comprueba la información asociada a la solicitud.

5.2.3 Tiempo para procesar las solicitudes de certificado

Una vez verificada la información requerida en el proceso de solicitud de certificados, se podrá proceder a la emisión del certificado que se requiera. El tiempo estimado de emisión de certificados tras la verificación es de 24 horas en días laborables.

5.3 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.

5.3.1 Acciones de la CA durante la emisión del certificado

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

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

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

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

- La Autoridad de Registro autentica la validez de la documentación presentada por el solicitante, y audita la generación de la solicitud de certificado en HSM y la solicitud de certificado con formato PKCS#10.
- 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.

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.

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

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

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

5.4 Aceptación del certificado

La aceptación de un certificado supone la aceptación por el suscriptor de los términos y condiciones del contrato que determinan los derechos y obligaciones de EADTrust y la comprensión por el suscriptor de las disposiciones de esta Declaración de Prácticas de Certificación que rigen los aspectos técnicos y operativos de los servicios de certificación digital proporcionado por EADTrust.

El suscriptor/propietario de la clave tiene un plazo determinadode 10 dias desde la entrega del certificado para asegurarse de que funciona correctamente y, si es necesario, devolverlo a la Autoridad de Registro.

Si se devuelve un certificado debido a defectos técnicos (por ejemplo, funcionamiento defectuoso del almacenamiento en soportes de los certificados, problemas con la compatibilidad del programa, error técnico en el certificado, etc.) o a errores en los datos contenidos en el certificado, EADTrust revocará el certificado emitido y emitirá uno nuevo.

5.4.1 Conducta que constituye la aceptación del certificado

Dependiendo del documento de solicitud del certificado, se especifica tanto la aceptación de las condiciones de uso y como el contrato del suscriptor, a los que se debe dar cumplimiento. Como evidencia, el suscriptor debe firmar una hoja de recepción y aceptación, si bien serán válidas las diferentes

formas de prestar consentimiento admitidas en derecho, siempre que generen evidencias digitales de forma semejante para todos los intervinientes. El uso del certificado determina su aceptación.

5.4.2 Publicación del certificado por la CA

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

Los certificados destinados a sitios web se registrarán cuando corresponda en el sistema de "Certificate Transparency" desde el que estarán disponibles para terceros. Esta es una medida de seguridad definida en el marco de CAB Forum.

5.4.3 Notificación de la emisión del certificado por la CA a otras entidades

EADTrust podrá publicar los certificados de sitio web (utilizados en contextos de securización de comunicaciones mediante protocolos de tipo TLS) según la normativa "CertificateTransparency"[26]

5.5 Par de claves y uso del certificado

5.5.1 Clave privada del suscriptor y uso del certificado

El suscriptor que tiene la custodia de las claves:

- Garantizará el uso correcto y el mantenimiento de los soportes de almacenamiento del certificado.
- Facilitará a EADTrust y a sus entidades de registro información completa y adecuada, conforme a los requerimientos de esta 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 suscriptor piense que pueda confiar en el certificado, sin demora razonable, si se produce alguna de las siguientes situaciones:
  - La clave privada del suscriptor se ha perdido, ha sido robada o se ha visto potencialmente comprometida.
  - El control sobre la clave privada del suscriptor se ha perdido debido a que los datos de activación se han visto comprometidos (por ejemplo, código PIN del dispositivo criptográfico) o debido a otras razones.
  - Inexactitud o cambios en el contenido del certificado, según lo notificado o sospechado por el suscriptor, solicitando la revocación del certificado cuando tales cambios constituyan una causa de revocación.
- Dejará de usar la clave privada al final del período de validez del certificado.
- Transferirá obligaciones específicas a los propietarios de la clave.

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

- Se abstendrá de supervisar, interferir o realizar un proceso de ingeniería inversa de la implementación técnica de los servicios de certificación sin la previa aprobación por escrito de la Autoridad de Certificación.
- Se abstendrá de comprometer intencionadamente la seguridad de los servicios de certificación.
- Se abstendrá de utilizar las claves privadas correspondientes a las claves públicas incluidas en los certificados con el fin de firmar un certificado como si desempeñara la función de una Autoridad de Certificación.
- Los suscriptores de certificados cualificados que generen firmas digitales utilizando la clave privada correspondiente a la clave pública incluida en el certificado deben asumir que tales firmas electrónicas son equivalentes a firmas manuscritas, siempre que se utilice un dispositivo criptográfico (dispositivo cualificado de creación de firma electrónica), según las disposiciones del Reglamento eIDAS.
- Los suscriptores de certificados cualificados que generen sellos digitales utilizando la clave privada correspondiente a la clave pública incluida en el certificado deben asumir que tales sellos digitales gozan de presunción de integridad de los datos y de la corrección del origen de los datos a los que el sello electrónico cualificado esté vinculado, siempre que se utilice un dispositivo criptográfico (dispositivo cualificado de creación de sello electrónico), según las disposiciones del Reglamento eIDAS.
- Abonar las tarifas por los servicios de certificación y sellado de tiempo solicitados en los términos y condiciones previstos por la CA
- Autorizar a la CA a que, a través de la RA, utilice los datos personales aportados por el SOLICITANTE para validar, comprobar y autenticar la identidad declarada por este.
- Solicitar la modificación/renovación/suspensión/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.

El suscriptor que hace uso de un sistema de firma o sello electrónicos en la nube:

- 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 las claves que le permiten acceder al sistema de firma remota o a los mecanismos complementarios de autenticación de forma que se garantice que el uso de la clave privada esta con un alto grado de confianza bajo su exclusivo control.
- Notificará a EADTrust, y a cualquier otra persona que el suscriptor piense que pueda confiar en el certificado, sin demora razonable, si se produce alguna de las siguientes situaciones:
  - El control sobre la clave privada del suscriptor se ha perdido debido a que los datos de activación se han visto comprometidos (por ejemplo, código PIN del dispositivo criptográfico) o debido a otras razones.
  - Inexactitud o cambios en el contenido del certificado, según lo notificado o sospechado por el suscriptor, solicitando la revocación del certificado cuando tales cambios constituyan una causa de revocación.

- 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.
- Los suscriptores de certificados cualificados que generen firmas digitales utilizando la clave privada correspondiente a la clave pública incluida en el certificado deben asumir que tales firmas electrónicas son equivalentes a firmas manuscritas, siempre que se utilice un dispositivo criptográfico (dispositivo cualificado de creación de firma electrónica), según las disposiciones del Reglamento eIDAS.
- Los suscriptores de certificados cualificados que generen sellos digitales utilizando la clave privada correspondiente a la clave pública incluida en el certificado deben asumir que tales sellos digitales gozan de presunción de integridad de los datos y de la corrección del origen de los datos a los que el sello electrónico cualificado esté vinculado, siempre que se utilice un dispositivo criptográfico (dispositivo cualificado de creación de sello electrónico), según las disposiciones del Reglamento eIDAS.
- Abonar las tarifas por los servicios de certificación y sellado de tiempo solicitados en los términos y condiciones previstos por la CA
- Autorizar a la CA a que, a través de la RA, utilice los datos personales aportados por el SOLICITANTE para validar, comprobar y autenticar la identidad declarada por este.
- Solicitar la modificación/renovación/suspensión/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.

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

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

- Evaluar independientemente la idoneidad del uso de un certificado y determinar que, de hecho, se utilizará para un propósito apropiado.
- Ser consciente de las condiciones para usar los certificados de conformidad con lo establecido en la Declaración de Práctica de Certificación, y especialmente, en la PDS (Policy Disclosure Statement), es decir, la declaración abreviada para terceros que confían.
- Comprobar la validez, suspensión o revocación de los certificados emitidos, utilizando la información sobre el estado del certificado, disponible en el servicio OCSP.
- Comprobar todos los certificados en la jerarquía de certificados antes de confiar en una firma digital o en cualquiera de los certificados de la jerarquía. En relación con los certificados cualificados, comprobar que la autoridad de certificación raíz de EADTrust en cuya jerarquía se encuentra el certificado, está inluída en la lista TSL correspondiente.[27]

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

- Tener en cuenta las 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.

5.6 Renovación del certificado

5.6.1 Circunstancias para la renovación del certificado

El certificado se puede renovar si el certificado no ha expirado o si han transcurrido menos de 5 años desde su última personación e identificación ante la RA. EADTrust realiza las renovaciones de certificados emitiendo nuevas claves, por lo tanto, el proceso técnico de emisión es igual al que se sigue cuando se realiza una solicitud por primera vez.

5.6.2 Quién puede solicitar la renovación

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

5.6.3 Procesamiento de solicitudes de renovación de certificados

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

5.6.4 Notificación de una nueva emisión de certificado al suscriptor

Se tomarán las siguientes medidas:

- EADTrust podrá comprobar que un certificado está a punto de expirar.
- El suscriptor será informado de que puede renovar su certificado.

- El suscriptor solicitará una cita con la RA por teléfono o por medio del sitio web e incluso podrá firmar la solicitud utilizando su certificado, firmando la renovación de su certificado.
- El certificado se generará siguiendo el procedimiento habitual de emisión.
- El certificado generado se entregará al suscriptor.

5.6.5 Conducta que constituye la aceptación de un certificado de renovación

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

5.6.6 Publicación del certificado de renovación por la CA

Los nuevos certificados de autenticación, firma y sello no se publican en repositorios de certificados, si bien los certificados de sitio web pueden ser registrados en repositorios de control de seguridad.

En particular será de aplicación lo previsto en la normativa de “Certificate transparency” publicada por CAB Forum para los certificados de servidor web

5.6.7 Notificación de la emisión del certificado por la CA a otras entidades

EADTrust podrá publicar los certificados de sitio web (utilizados en contextos de securización de comunicaciones mediante protocolos de tipo SSl o TLS) según la normativa “CertificateTransparency”[28]

5.7 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.

5.7.1 Circunstancias para la modificación del certificado

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

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

5.7.2 Quién puede solicitar la modificación del certificado

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

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

5.7.3 Procesamiento de las solicitudes de modificación del certificado

Las solicitudes de modificación por error se gestionan a instancia del solicitante que cursó la petición que dio como resultado el certificado erróneo. En el resto de los casos, se gestionan como solicitudes de renovación.

5.7.4 Notificación de la emisión de un nuevo certificado al suscriptor

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

5.7.5 Conducta que constituye la aceptación de un certificado modificado

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

5.7.6 Publicación del certificado modificado por la CA

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

5.7.7 Notificación de la emisión del certificado por la CA a otras entidades

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

5.8 Revocación y suspensión del certificado

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

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

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

5.8.1 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 juridica.
- Los datos de creación de firma del firmante o del prestador de servicios de certificación han sido comprometidos o si el firmante o un tercero han utilizado los datos de forma incorrecta.
- Cuando se haya emitido una orden legal o administrativa a tal efecto.
- Que una Autoridad Competente indique la necesidad de revocar un certificado PSD2.

- La muerte del firmante o la extinción de la persona jurídica titular del certificado de sello, la incapacidad total o parcial imprevisible del firmante o de la persona jurídica representada por el firmante, la terminación de la representación, la disolución de la persona jurídica representada, el cambio en las circunstancias de la custodia o uso de los datos de creación de firma o de sello incluidos en los certificados expedidos a una persona jurídica.
- El caso de que EADTrust termine su actividad, excepto en los casos en que el firmante haya dado su consentimiento para que los servicios de gestión de certificados electrónicos sean transferidos a otro prestador de servicios de certificación.
- Cambio en los datos suministrados para obtener el certificado o modificación de las circunstancias verificadas para la emisión del certificado.
- Que haya perdido la clave privada asociada al certificado, que haya sido robada o no sea útil debido a daños en el soporte del certificado o cuando se haya cambiado a otro soporte no previsto en la política de certificación.
- Una de las partes incumple sus obligaciones, como, por ejemplo, el pago.
- Se detecta un error en el procedimiento de emisión del certificado, ya sea porque uno de los requisitos previos no se ha cumplido o debido a problemas técnicos durante el proceso de emisión del certificado.
- Existe una amenaza potencial para la seguridad de los sistemas y para la fiabilidad de los certificados emitidos por EADTrust por razones distintas del compromiso de los datos de creación de firmas.
- Fallo técnico en la emisión o distribución de certificados o de la documentación asociada.
- Que hayan transcurrido 3 meses desde el momento en que se solicita la certificación sin que se recoja el certificado.
- Si EADTrust recibe una solicitud para la emisión del certificado y ya existe un certificado válido de la misma clase y unicidad, el certificado válido será revocado a petición del solicitante.

5.8.2 Quién puede solicitar la revocación

La revocación de un certificado podrá solicitarse por

- El sujeto/Firmante.
- El Solicitante responsable.
- La Entidad (a través de un representante de la misma).
- La RA o la AC.
- 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.

5.8.3 Procedimiento para la solicitud de revocación

El suscriptor puede ponerse en contacto con EADTrust y solicitar la revocación de un certificado. EADTrust le informará sobre cómo formalizar su solicitud.

El certificado puede ser revocado en cualquier momento y en todos los casos de pérdida o robo.

Se registra y archiva la solicitud de revocación autenticada y la información que justifica la revocación.

Si la revocación es solicitada por otra persona que no sea el solicitante, suscriptor o titular de la clave, antes o simultáneamente a la revocación, EADTrust informará al propietario de la clave del certificado y al suscriptor sobre la revocación de su certificado y especificando el motivo de la revocación. El solicitante puede revocar el certificado a través de los siguientes canales:

- En línea, en la dirección www.eadtrust.eu o por correo electrónico con solicitud firmada electrónicamente utilizando un certificado cualificado.
- Por correo, enviando la solicitud de revocación de certificado firmada y validada ante notario.
- Por un sistema de entrega certificada cualificada que acredite la identidad del remitente, que debe coincidir con uno de los sujetos legitimados para solicitar la revocación.

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, s perjuicio de las comprobaciones adiionales 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.

5.8.4 Periodo de gracia para comprobar certificados revocados

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

El período de precaución o período de gracia que corresponda aplicar para la validación de los certificados es el máximo tiempo transcurrido entre renovaciones de CRL (cuando se aplica este procedimiento para comprobar si un certificado está revocado).

En la relación de firmas elctrónicas, este periodo podrá ser, desde el momento en que se realiza la firma o el sellado de tiempo, como mínimo, el tiempo máximo permitido para el refresco completo de las CRLs (CertificateRevocationLists) o el tiempo máximo de actualización del estado del certificado en el servicio OCSP (Online Certificate Status Protocol). Esta definición tendrá en cuenta también la posibilidad de que estos tiempos varíen según el Prestador de Servicios de Certificación.

El período de gracia recomendado es de 24 horas, si bien la disponibilidad de la información de revocación a través del servicio OCSP es de como máximo 10 minutos tras la finalización de la comunicación que da noticias de las razones de la revocación.

En caso de que sea de aplicación una política de firma concreta, es responsabilidad del tercero que confía en los certificados expedidos por EADTrust la comprobación de que la Política de Firma aplicable es compatible con la Política de Certificación de EADTrust.Tres de las posibles políticas a aplicar, en España, son la de factura electrónica[29], la de la Administración General del Estado[30] y la de la Administración de Justicia[31].

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

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

[31] 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

EADTrust mantiene información sobre certificados revocados más allá de la fecha de caducidad tanto en la CRL como en el servicio de OCSP. El período de tiempo es configurable y en la actualidad esta establecido a 31.536.000 segundo (1 año).

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

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

5.8.6 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 y 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”.

5.8.7 Frecuencia de emisión de la CRL

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

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

La CRL para los certificados de entidad final se emite cada 24 horas o cuando se produce una revocación.

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

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

No se generan “Last CRL’s”. Si una CRL caduca y no se ha emitido otra en el período estipulado (fecha eb 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.

5.8.8 Latencia máxima para CRLs

El tiempo máximo de latencia, es decir, el tiempo que transcurre tras la finalización de la comunicación que da noticias de las razones de la revocación, hasta que la información está disponible en el servicio OCSP y en la lista CRL se establece en 10 minutos.

5.8.9 Servicios de estado de certificado

EADTrust proporciona a las Entidades Usuarias un servicio de comprobación de certificados en tiempo real basado en OCSP (Online CertificateStatusProtocol)[32].

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.

5.9 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.

6 Controles de instalaciones, de gestión y operacionales

6.1 Controles físicos

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.

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

6.1.1 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[33] y OVH[34]

6.1.2 Acceso físico

Las instalaciones de EADTrust cuentan con un sistema completo de control de acceso físico que consiste en:

- Seguridad perimetral que se extiende desde el suelo hasta el techo para evitar el acceso no autorizado.
- 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 posble 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.

6.1.3 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.

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

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

6.1.4 Exposición al agua

EADTrust ha tomado las precauciones necesarias para minimizar el impacto de la exposición al agua.

6.1.5 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 ignífuga cuenta con una protección adicional de espuma ignífuga.

6.1.6 Almacenamiento de soportes

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

6.1.7 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.

6.1.8 Copia de seguridad externa

EADTrust mantiene copias de seguridad de los soportes de almacenamiento en un entorno seguro y protegido contra accidentes y una distancia suficiente para evitar daños en caso de un desastre en el sitio originario.

6.2 Controles de procedimiento

6.2.1 Puestos de confianza

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

Para asegurar que las personas de confianza cumplan adecuadamente sus deberes, se abordan las siguientes consideraciones:

- La primera es que la tecnología está diseñada y configurada para prevenir errores y conducta inadecuada.
- La segunda es que las tareas se distribuyen entre varios individuos de manera que cualquier conducta impropia requeriría la complicidad de varios de ellos.

EADTrust tiene definiciones completas de todas las funciones desempeñadas en la organización. Se definen los deberes y responsabilidades asociados a cada función, y cada uno tiene un conjunto de procedimientos documentados que regulan la práctica anexa a cada uno.

6.2.2 Número de personas requeridas por tarea

Para reforzar la seguridad del sistema, se asigna más de una persona a cada función, con la excepción de la función de operador, que puede realizar el administrador.

Se puede asignar varias personas a la misma función.

6.2.3 Identificación y autenticación para cada puesto

Los roles de confianza requieren la comprobación de la identidad por medios seguros. Todos los roles de confianza son realizados por individuos.

EADTrust tiene documentación específica que da más detalles de cada función.

6.2.4 Puestos que requieren separación de deberes

EADTrust sigue la política de seguridad CIMC (Certificate Issuing and Management Component)[35] que se define en su modelo de seguridad.

6.3 Controles de personal

6.3.1 Antecedentes, cualificaciones, experiencia y requisitos de aplicación

EADTrust emplea personal con la experiencia y con las cualificaciones necesarias para desempeñar sus responsabilidades laborales.

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

6.3.2 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.

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

6.3.3 Requisitos de formación

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

- Una copia de la Declaración de Prácticas de Servicios Electrónicos de Confianza.
- 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.

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.

6.3.4 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.

6.3.5 Rotación y secuencia laboral

No aplica

6.3.6 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. Existe un régimen disciplinario interno que define las sanciones aplicables al personal en función de la gravedad de las actuaciones.

6.3.7 Requisitos de contratación del personal

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.

6.3.8 Documentación proporcionada al personal

Todo el personal con funciones de confianza recibe:

- Una copia de la Declaración de Prácticas de Certificación
- Una copia del Manual de Acogida que incluye consideraciones específicas de confidencialidad y seguridad.
- Documentación que define las obligaciones y procedimientos asociados a cada rol.
- El personal también tiene acceso a los manuales de operaciones de los distintos componentes del sistema.

6.4 Procedimientos de registro de auditoría

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 dio origen al registro. Los registros también se utilizarán en el arbitraje para resolver cualquier posible conflicto comprobando la validez de una firma en un momento dado.

6.4.1 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 AC 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 AC.
- Encendido y apagado de la aplicación de la AC.
- Cambios en los detalles de la AC 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.

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 compromisos y discrepancias.
- 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.

6.4.2 Frecuencia de procesamiento del registro

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

6.4.3 Periodo de retención del registro de auditoría

EADTrust almacena la información de los registros de auditoria 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, para ello se utiliza un sistema de hashes encadenados y firma digital.

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.

6.4.4 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. Siempre habrá respaldo de la última modificación, y, en su caso, en ubicaciones separadas a las de prestación del servicio.

6.4.5 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”

6.4.6 Cambio de clave

Para renovar un certificado de usuario, ya sea porque se ha revocado o porque ha expirado el período de validez, se debe solicitar un nuevo certificado siguiendo el proceso de emisión del certificado descrito en la documentación específica de cada certificado. El cambio clave implica la renovación del certificado.

En las CA subordinadas no se realizan cambios de claves. Las ceremonias de generación de claves obtienen siempre claves nuevas.

6.4.7 Terminación o cese de la CA o RA

6.4.7.1 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.

EADTrust deberá notificar 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 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, y los revocados que hayan caducado hasta un año antes del momento de generación de la CRL. Siempre que sea posible, se gestionarán las CRL´s en el proceso de terminación de manera que no queden certificados vigentes al generar la última CRL.

Tal como indica el artículo 21.3 de la LFE (59/2003), el Organismo supervisor registrará y mantendrá accesible durante un período de tiempo apropiado, incluso cuando hayan cesado las actividades del

prestador cualificado de servicios de confianza, toda la información pertinente referente a los datos expedidos y recibidos por el prestador cualificado de servicios de confianza, en particular al objeto de que sirvan de prueba en los procedimientos legales y para garantizar la continuidad del servicio.

6.4.7.2 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.

6.4.8 Compromiso de claves y Plan de contingencias y de continuidad de negocio

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.

El Plan de Contingencia son se compone de varias fases:

1. Detección. Algún elemento indicador activa una alerta que requiere atención.
2. Evaluación. Se analiza la alerta y se dimensiona el problema. De ser necesario se activa el Plan de contingencia.
3. Notificación. Se informa a los organismos supervisores o a los usuarios, según corresponda.
4. Recuperación. Se actúa para restablecer temporal y parcialmente los servicios hasta la recuperación de los daños provocados en el sistema original.
5. Normalización. Se realizan las actuaciones para devolver el sistema y los procesos a su operativa habitual.
6. Reporting. Se analiza en profundidad lo ocurrido y se notifica a los organismos y partes interesadas.

6.4.8.1 En caso de compromiso de la clave privada

- 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:
    - La CA emisora
    - Las RA´s asociadas a dicha CA
    - 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:

- Generar un nuevo certificado para la CA subordinada.
- Asegurar que todos los nuevos certificados y CRL emitidos por la CA son firmados utilizando la nueva clave.
- La CA emisora podrá emitir certificados a todas las entidades finales afectadas.

En caso de que la clave comprometida sea la 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.

7 Controles técnicos de seguridad

7.1 Generación e instalación del par de claves

7.1.1 Generación del par de claves

Los sistemas de gestión de claves propios de EADTrust como Prestador de Servicos 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 CA´s root´s y subordinadas estarán disponibles en los repositorios de EADTrust accesibles a través de la web, incluso cuando hayan caducado.

7.1.2 Entrega de la clave privada al suscriptor

Método de entrega de clave privada a las diferentes entidades que componen o colaboran con EADTrust:

- 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. No necesita ser entregado.
- 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.

7.1.3 Entrega de la clave pública al emisor del certificado

El método utilizado por las distintas entidades que componen o colaboran con EADTrust para entregar la clave pública al prestador emisor de certificados 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.

7.1.4 Entrega de la clave pública de la CA a las partes de confianza

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

7.1.5 Tamaños de clave

El algoritmo de hash (compendio) 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).

7.1.6 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)[36]

7.1.7 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 y CRL.

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

7.2 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+.

7.2.1 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 equivalente.

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 ITSEC E3 o FIPS 140-2 Nivel 3

La Norma Europea de referencia para los dispositivos de suscriptor utilizada es la CEN CWA 14169, si bien se contemplan otras más actualizadas como la norma EN 419 211, y, en el caso de firma en servidor (TW4S, Trustworthy System Supporting Server Signing) la norma EN 419 241 partes 1 y 2.

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”.[37]

7.2.2 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 los procesos informáticos que permiten la generación de claves y certificados.

[37] https://ec.europa.eu/futurium/en/system/files/ged/eidas-art.31-list-2019-08-01.pdf

7.2.3 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.

7.2.4 Copia de seguridad de la clave privada

Existe un procedimiento para la recuperación de claves de módulo criptográfico de la CA (raíz o subordinada) que puede aplicarse en caso de contingencia. Se aplicarán los mismos controles multipersona indicados.

7.2.5 Archivo de la clave privada

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

Las claves privadas para los certificados internos que utilizan los diferentes componentes del sistema de la CA para comunicarse entre sí, firmar y cifrar la información, se desactivarán y archivarán después de emitir el último certificado.

Las claves privadas de los suscriptores se gestionan por ellos. EADTrust no conserva claves privadas de los suscriptores, 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 suscriptor 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.

No se contempla el escrow de claves privadas con el propósito de descifrar en el futuro la información histórica cifrada con las claves públicas asociadas.

7.2.6 Transmisión de la clave privada a o desde un 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.

7.2.7 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.[38]

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

Para la generación de las claves para el usuario final certificado almacenadas "en la nube", EADTrust sigue las recomendaciones de la Comisión Europea (Reglamento eIDAS) y la Especificación Técnica Europea CEN EN 419 241. Se tienen también en cuenta las normas ETSI TS 119 431-1 y ETSI TS 119 431-2.

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+.

7.2.8 Método de activación de una clave privada

La CA raíz y las claves de las CAs subordinadas se activan mediante un proceso que requiere el uso simultáneo de n de m dispositivos criptográficos (tokens criptográficos o tarjetas).

Se accede a la clave privada del suscriptor 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 tiene un código de desbloqueo de dispositivo. Si se introduce erróneamente cierto número de veces, el dispositivo se bloquea definitivamente y no se puede utilizar.

El acceso de la clave privada del suscriptor en el caso de certificados almacenados "en la nube" tendrá un segundo factor de autenticación, que puede variar dependiendo del tipo de certificado.

7.2.9 Método de desactivación de una clave privada

La retirada de la tarjeta criptográfica del lector o extracción del token del ordenador desactivará cualquier acción en funcionamiento.

7.2.10 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.

Las claves privadas de certificados almacenados "en la nube" se eliminarán una vez que la relación con EADTrust haya finalizado o que los certificados hayan caducado.

Este procedimiento no se aplica a las claves de firma de usuario o autenticación emitidas en un token criptográfico o en una tarjeta criptográfica, excepto en el caso de cambio de clave utilizando el mismo dispositivo criptográfico. En estos casos, la clave anterior se destruirá y se generarán nuevas claves en el mismo soporte.

7.2.11 Calificación del módulo criptográfico

Como se indica en la sección 7.2.1. de este documento.

7.3 Otros aspectos de la gestión del par de claves

7.3.1 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.

7.3.2 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**.

7.4 . Datos de activación

7.4.1 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 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.
- 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.
- Certificados emitidos "en la nube": el uso de la clave privada asociada a cada certificado requiere un segundo factor de autenticación.

7.4.2 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 junto al dispositivo criptográfico o compartirlo con otras personas.
- Cambiar el PIN y PUK antes de usarlos.

7.4.3 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.

7.5 Controles de seguridad informática

7.5.1 Requisitos técnicos específicos de seguridad informática

Existen una serie de controles en los diferentes componentes que conforman el sistema de servicio de certificación de EADTrust (CAs, bases de datos de EADTrust, servicios de Internet de EADTrust, funcionamiento de la CA y gestión de redes):

- Controles operativos
  - Todos los procedimientos operativos están debidamente documentados en los correspondientes manuales de operaciones. EADTrust mantiene un plan de contingencia.
  - Se han implementado herramientas para proteger contra virus y códigos maliciosos.
  - El equipo se mantiene de manera continua para garantizar la disponibilidad e integridad ininterrumpidas.
  - Existe un procedimiento para guardar, borrar y eliminar con seguridad medios de almacenamiento, medios extraíbles y equipos obsoletos.
- Intercambio de datos. Los siguientes intercambios de datos están encriptados para garantizar la confidencialidad.
  - Transmisión de los datos de registro entre las RAs y la base de datos de registro.
  - Transmisión de los datos de preinscripción.
  - Comunicación entre ARs y CAs.

- El servicio de publicación de revocaciones está disponible 24 horas al día, 7 días a la semana.
- Control de acceso
  - Las identificaciones de usuario únicas se utilizan de tal manera que los usuarios están asociados y pueden ser responsables de sus acciones.
  - Los derechos se asignan de acuerdo con la norma de proporcionar a los usuarios la menor cantidad de privilegios del sistema que necesitan para hacer su trabajo.
  - Los derechos de acceso se cancelan inmediatamente cuando los usuarios cambian de trabajo o salen de la organización.
  - El nivel de acceso asignado a los usuarios se revisa cada tres meses.
  - Los privilegios del sistema se asignan caso por caso y terminan una vez que el motivo de su asignación ya no es válido.
  - EADTrust mantiene directrices de calidad de contraseñas.

7.5.2 Calificación de la seguridad informática

Los productos utilizados para la prestación de servicios de certificación tienen la calificación internacional de "Common Criteria" o Norma ISO, ISO / IEC 15408. En su defecto, pueden estar certificados en base a la norma FIPS-140-2.

7.6 Controles técnicos del ciclo de vida

7.6.1 Controles de desarrollo del sistema

Se controla la implementación del software para los sistemas de producción.

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

- Existe un procedimiento de autorización formal 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 la producción.
- Se conserva un archivo de registro en todas las actualizaciones de las bibliotecas.
- Se conservan las versiones anteriores del software.
- El software adquirido se mantiene al nivel soportado por el proveedor.
- Se cuenta con procedimientos que permten incluir extensiones sobre el código fuente.

7.6.2 Controles de gestión de seguridad

Los productos utilizados para la prestación de servicios de certificación tienen la calificación de seguridad internacional de "Common Criteria" o Norma ISO ISO/IEC 15408. En su defecto, pueden estar certificados en base a la norma FIPS-140-2.

7.6.3 Controles de seguridad del ciclo de vida

Con el fin de realizar pruebas, se requiere un gran volumen de datos lo más similar posible a los datos de producción. EADTrust evita el uso de bases de datos de producción con información personal.

7.7 Controles de seguridad de red

Todas las medidas de seguridad y los controles especificados para el resto de los sistemas se aplican a los dispositivos de red.

En la política de seguridad para el uso de redes y servicios de redes se describe en la política de seguridad de red.

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

7.8 Timestamping

Se dedica una sección separada a la descripción de la prestación de servicios de Timestamping. La referencia en este apartado es por fidelidad a la norma RFC 3647.

8 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.
- 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.[39]

Los certificados incluyen como mínimo, los siguientes campos:

- Número de serie, que es un código único con respecto al nombre distinguido del emisor.
- Algoritmo de firma.
- El nombre distinguido del emisor.
- Inicio de validez del certificado, en Tiempo Coordinado Universal, codificado conforme a la RFC 3280.
- Fin de validez del certificado, en Tiempo Coordinado Universal, codificado conforme a la RFC 3280 - Nombre distinguido del sujeto.
- Clave pública del sujeto, codificada de acuerdo con RFC 3280
- Firma, generada y codificada, de acuerdo con RFC 3280 los certificados son conformes con las siguientes normas:
    - RFC 3280: Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile, April 2002
    - ITU-T Recommendation X.509 (1997): Information Technology – Open Systems Interconnection - The Directory: Authentication Framework, June 1997, con sus actualizaciones y correcciones posteriores.

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.

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

- 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).

8.1 Número de versión

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

8.2 Extensiones de certificado

Las extensiones utilizadas dependiendo del perfil en cada caso son:

- Authority key Identifier.
- subjectKeyIdentifier.
- basicConstraints.
- keyUsage.
- certificatePolicies.
- subjectAltName.
- issuerAltName.
- extKeyUsage.
- cRLDistributionPoint.
- Authority Information Access.

8.3 Perfiles de Root y SubCA

8.3.1 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 254 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

8.3.2 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 254 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

8.3.3 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

8.3.4 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 254 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

Campo	Crítico	Contenido
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

8.3.5 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 254 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

8.3.6 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

8.4 Perfiles de certificados de Entidad Final

8.4.1 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 254 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		
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

8.4.2 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 254 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 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

8.4.3 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
subjectPublicKeyInfo		RSA mínimo 2048 bits ECDSA 254 bits (prime256v1) ó 384 bits (secpr384r1)
Extensiones		
authorityKeyIdentifier		Derivada del resultado de aplicar el hash a la Clave pública de la AC emisora
subjectKeyIdentifier		Derivada del resultado de aplicar el hash a la clave pública del sujeto
issuerAltName		Igual al campo Subject Alternative Names de la CA Emisora
subjectAltName		rfc822 Name Correo electrónico del titular opcional DirectoryName 1.3.6.1.4.1.501.1.1 Nombre 1.3.6.1.4.1.501.1.2 Primer Apellido 1.3.6.1.4.1.501.1.3 Segundo Apellido 1.3.6.1.4.1.501.1.4 DNI/NIE/NIF/ PASS
certificatePolicies*		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.0.41221
cpsURI		http://policy.eadtrust.eu/cps
userNotice		European Agency of Digital Trust, S.L. Natural Person Qualified Certificate
policyIdentifier		0.4.0.194112.1.0 (QCP-n)
qcStatements**		
QcCompliance		Presente
QcType		id-etsi-qct-esign
QcRetentionPeriod		15 años
qcStatement-2		0.4.0.194121.1.1 (id-etsi-qcs-SemanticsId-Natural)
cRLDistributionPoints		
distributionPoint		http://crl.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadnp<Año>.crl
authorityInfoAccess		
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
** En caso de que la clave privada del certificado se encuentre en un **dispositivo cualificado de creación de firma** se añade el campo QSCD

8.4.4 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 254 bits (prime256v1) ó 384 bits (secpr384r1)
Extensiones		
authorityKeyIdentifier		Derivada del resultado de aplicar el hash a la Clave pública de la AC emisora
subjectKeyIdentifier		Derivada del resultado de aplicar el hash a la clave pública del sujeto
issuerAltName		Igual al campo Subject Alternative Names de la CA Emisora
subjectAltName		rfc822 Name Correo electrónico del titular DirectoryName 1.3.6.1.4.1.501.1.1 Nombre del representante 1.3.6.1.4.1.501.1.2 Primer Apellido del representante 1.3.6.1.4.1.501.1.3 Segundo Apellido del representante 1.3.6.1.4.1.501.1.4 NIF del Representante 1.3.6.1.4.1.501.1.6 Razón Social de la Entidad 1.3.6.1.4.1.501.1.7 NIF de la Entidad Representada
certificatePolicies*		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.0.41222
cpsURI		http://policy.eadtrust.eu/cps
userNotice		European Agency of Digital Trust, S.L. Power of Attorney Qualified Certificate
policyIdentifier		0.4.0.194112.1.0 (QCP-n)
PolicyIdentifier		2.16.724.1.3.5.8 (OID MPR)
qcStatements**		
QcCompliance		Presente
QcType		id-etsi-qct-esign
QcRetentionPeriod		15 años
qcStatement-2		0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)
cRLDistributionPoints		
distributionPoint		http://crl.eadtrust.eu/eadtrust-subca<algoritmo><tamañoclave>eadnp<Año>.crl
authorityInfoAccess		
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

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

8.4.5 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 ó ecdsa-with-SHA256 ó ecdsa-with-SHA384
Issuer		Same as the Subject field of the issuing CA certificate
Validity		2 años
Subject		
OrganizationalUnit		Type of web certificate
subjectPublicKeyInfo		RSA 2048 bits minimum or ECDSA 254 bits (prime256v1) or 384 bits (secpr384r1)
Extensions		
subjectAltName		
dnsName		DNS name(s)
extendedKeyUsage		serverAuth, clientAuth
subjectKeyIdentifier		Derived from the result of applying the hash to the public key of the subject
authorityKeyIdentifier		Derived from the result of applying the hash to the Public key of the issuing CA
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.0.41241
cpsURI		http://policy.eadtrust.eu
userNotice		European Agency of Digital Trust, S.L. EU qualified website authentication certificates.
policyIdentifier		0.4.0.194112.1.4 (ETSI QCP-w)
policyIdentifier		2.23.140.1.2.1 (CAB/FORUM DV)
cRLDistributionPoints		http://crl.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eaddvov<Año>.crl
authorityInfoAccess		
caIssuers		http://ca.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eaddvov<Año>.crt
Ocsp		http://ocsp.eadtrust.eu
basicConstraint	Crítica	CA false
qcStatements		
QcRetentionPeriod		15 years
QcCompliance		Present
QcType		id-etsi-qct-web
keyUsage	Crítica	digitalSignature, keyEncipherment
CT RFC6962		Certificate Transparency

8.4.6 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 ecdsa-with-SHA256 or ecdsa-with-SHA384
issuer		Same as the Subject field of the issuing CA certificate
validity		2 años
subject		
OrganizationalUnit		Type of web certificate
OrganizationName		Organization Name
LocalityName		Locality Name
StateOrProvinceName		State or province name
CountryName		CountryName
subjectPublicKeyInfo		RSA 2048 bits minimum or ECDSA 254 bits (prime256v1) or 384 bits (secpr384r1)
Extensions		
subjectAltName		
dnsName		DNS name(s)
extendedKeyUsage		serverAuth, clientAuth
subjectKeyIdentifier		Derived from the result of applying the hash to the public key of the subject
authorityKeyIdentifier		Derived from the result of applying the hash to the Public key of the issuing CA
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.0.41242
cpsURI		http://policy.eadtrust.eu
userNotice		European Agency of Digital Trust, S.L. EU qualified website authentication certificates.
policyIdentifier		0.4.0.194112.1.4 (ETSI QCP-w)
policyIdentifier		2.23.140.1.2.2 (CAB/FORUM OV)
cRLDistributionPoints		http://crl.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eaddvov<Año>.crl
authorityInfoAccess		
caIssuers		http://ca.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eaddvov<Año>.crt
ocsp		http://ocsp.eadtrust.eu
basicConstraint	Crítica	CA false
qcStatements		
QcCompliance		Present
QcType		id-etsi-qct-web
QcRetentiodPeriod		15
keyUsage	Crítica	digitalSignature, keyEncipherment
CT RFC6962		Certificate Transparency

8.4.7 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 ecdsa-with-SHA256 or ecdsa-with-SHA384
issuer		Same as the Subject field of the issuing CA certificate
validity		2 años
subject		
OrganizationalUnit		Type of web certificate
businessCategory		Private Organization, Government Entity, Business Entity or Non-Commercial Entity
jurisdictionCountryName		Country of Jurisdiction of Incorporation or Registration Field
jurisdictionStOrProvName		State or Province of Jurisdiction of Incorporation or Registration Field
jurisdictionLocalityName		Locality of Jurisdiction of Incorporation or Registration Field
OrganizationName		Organization Name
LocalityName		Locality Name
StateOrProvinceName		State or province name
CountryName		CountryName
serialNumber		Registration Number
subjectPublicKeyInfo		RSA 2048 bits minimum or ECDSA 254 bits (prime256v1) or 384 bits (secpr384r1)
Extensions		
subjectAltName		
dnsName		DNS name(s)
extendedKeyUsage		serverAuth, clientAuth
subjectKeyIdentifier		Derived from the result of applying the hash to the public key of the subject
authorityKeyIdentifier		Derived from the result of applying the hash to the Public key of the issuing CA
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.0.41244
cpsURI		http://policy.eadtrust.eu
userNotice		European Agency of Digital Trust, S.L. EU qualified website authentication certificates.
policyIdentifier		0.4.0.194112.1.4 (ETSI QCP-w)
policyIdentifier		2.23.140.1.1 (CAB/FORUM EV)
cRLDistributionPoints		http://crl.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadevpsd2<Año>.crl
authorityInfoAccess		
caIssuers		http://ca.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadevpsd2<Año>.crt
ocsp		http://ocsp.eadtrust.eu
basicConstraint	Crítica	CA false
qcStatements		
QcCompliance		Present
QcType		id-etsi-qct-web
QcRetentiodPeriod		15
keyUsage	Crítica	digitalSignature, keyEncipherment
CT RFC6962		Certificate Transparency

8.4.8 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 – DNI/NIE (Número de DNI/NIE)
Given Name		Nombre
CountryName		CountryName
subjectPublicKeyInfo		RSA 2048 bits
extensions		
subjectAltName		
rfc822Name	Opcional	Email del responsable
directoryName		
2.16.724.1.3.5.7.2.1		CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO
2.16.724.1.3.5.7.2.2		Entidad suscriptora
2.16.724.1.3.5.7.2.3		Número único de identificación de la entidad
2.16.724.1.3.5.7.2.4		DNI o NIE del firmante
2.16.724.1.3.5.7.2.5	Opcional	Número de identificación del firmante
2.16.724.1.3.5.7.2.6		Nombre (40 caracteres)
2.16.724.1.3.5.7.2.7		Apellido1 (40 caracteres)
2.16.724.1.3.5.7.2.8		Apellido2 (40 caracteres)
2.16.724.1.3.5.7.2.9	Opcional	Correo electrónico del firmante
2.16.724.1.3.5.7.2.10	Opcional	Unidad, dentro de la Administración, en la que está incluida el firmante
2.16.724.1.3.5.7.2.11	Opcional	Puesto desempeñado por el firmante dentro de la administración.
Othername: UPN	Opcional	UPN para smart card logon
extendedKeyUsage		clientAuth, emailProtection
subjectKeyIdentifier		Derivado de aplicar el hash a la clave del suscriptor
authorityKeyIdentifier		Derivado de aplicar el hash a la clave del emisor
certificatePolicies*		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.0.41223
cpsURI		http://policy.eadtrust.eu
userNotice		European Agency of Digital Trust, S.L. Certificado cualificado de empleado público
policyIdentifier		0.4.0.194112.1.0 (ETSI QCP-n)
policyIdentifier		2.16.724.1.3.5.7.2
cRLDistributionPoints		http://crl.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadnp<Año>.crl
authorityInfoAccess		
caIssuers		http://ca.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadnp<Año>.crt
ocsp		http://ocsp.eadtrust.eu
qcStatements**		
QcCompliance		Present

Campos/Extensiones	Crítico	Contenido
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

Se podrán emitir certificados con otros niveles de aseguramiento para empleado publico 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 1671/2009 y está adaptado a las disposiciones de la Ley 39/2015 de 1 de Octubre, de Procedimiento Administrativo Común de las Administraciones Públicas, la Ley 40/2015 de 1 de Octubre, de Régimen Jurídico del Sector Publico (LRJ) y al Reglamento (UE) 910/2014.

8.4.9 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
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

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

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

Campos/Extensiones	Crítico	Contenido
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
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)
extendedKeyUsage		clientAuth, emailprotection
keyUsage	Crítica	digitalSignature

Contempla el uso de dispositivo cualificado de creación de firma

Se podrán emitir certificados con otros niveles de aseguramiento para empleado 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 1671/2009 y está adaptado a las disposiciones de la Ley 39/2015 de 1 de Octubre, de Procedimiento Administrativo Común de las Administraciones Públicas, la Ley40/2015 de 1 de Octubre, de Régimen Jurídico del Sector Publico (LRJ) y al Reglamento (UE) 910/2014.

8.4.11 Perfil de certificado cualificado de web PSD2 (QWAC)

Campos/Extensiones	Crítico	Contenido
version		3
serialNumber		Unique non-sequential positive number of minimum length 64 bits
signature		Sha256WithRSAEncryption or ecdsa-with-SHA256 or ecdsa-with-SHA384
issuer		Same as the Subject field of the issuing CA certificate
validity		2 años
subject		
OrganizationIdentifier		ETSI EN 319 412-1 and CA/B Forum format
OrganizationalUnit		Type of web certificate
OrganizationName		Organization Name
LocalityName		Locality Name
StateOrProvinceName		State or province name
CountryName		CountryName
businessCategory		Private Organization, Government Entity, Business Entity or Non-Commercial Entity
jurisdictionCountryName		Country of Jurisdiction of Incorporation or Registration Field

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 254 bits (prime256v1) or 384 bits (secpr384r1)
extensions		
subjectAltName		
dnsName		DNS name(s)
extendedKeyUsage		serverAuth, clientAuth
subjectKeyIdentifier		Derived from the result of applying the hash to the public key of the subject
authorityKeyIdentifier		Derived from the result of applying the hash to the Public key of the issuing CA
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.0.41243
cpsURI		http://policy.eadtrust.eu
userNotice		European Agency of Digital Trust, S.L. EU qualified website authentication certificate for payment service provider.
policyIdentifier		0.4.0.194112.1.4 (ETSI QCP-w)
policyIdentifier		2.23.140.1.1 (CAB/FORUM EV)
cRLDistributionPoints		http://crl.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadevpsd2<Año>.crl
authorityInfoAccess		
caIssuers		http://ca.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadevpsd2<Año>.crt
ocsp		http://ocsp.eadtrust.eu
basicConstraint	Crítica	CA false
qcStatements		
QcCompliance		Present
QcType		id-etsi-qct-web
QcRetentiodPeriod		15
qcStatement-2		0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)
PSD2QcType		ETSI TS 119 495 Format
keyUsage	Crítica	digitalSignature, keyEncipherment
CT RFC6962		Certificate Transparency
cabfOrganizationIdentifier		Effective January 31, 2020, if the subject:organizationIdentifier field is present, this field MUST be present

8.4.12 Perfil de certificado cualificado de sello electrónico para entidad 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

Campos/Extensiones	Crítico	Contenido
Organization Name		Nombre registrado completo
Country		País
OrganizationalUnit		Certificado de Sello de Entidad
subjectPublicKeyInfo		RSA 2048 mínimo ECDSA 254 bits (prime256v1) ó 384 bits (secpr384r1)
extensions		
issuerAltName		Igual al campo SubjectAlternativeNames de la CA Emisora
extendedKeyUsage		clientAuth, emailProtection
subjectKeyIdentifier		Derivada del resultado de aplicar el hash a la clave pública del sujeto
authorityKeyIdentifier		Derivada del resultado de aplicar el hash a la Clave pública de la AC emisora
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.0.41231
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
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)
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

8.4.13 Perfil de certificado cualificado PSD2 de persona jurídica para sello electrónico

Campos/Extensiones	Crítico	Contenido
version		3
serialNumber		Número positivo único
signature		Sha256WithRSAEncryption ó ecdsa-with-SHA256 ó ecdsa-with-SHA384
issuer		Igual al campo Subject del certificado de la CA emisora
validity		4 años
subject		
serialNumber	Opcional	DNI/NIE en formato ETSI EN 412-1
Surname	Opcional	Apellidos
Givenname	Opcional	Nombre
CommonName		Nombre común
organizationIdentifier		<3 caracteres de tipo de identidad><país>- <identificador>. Ejemplo: VATES-B12312312

Campos/Extensiones	Crítico	Contenido
Organization Name		Nombre registrado completo
Country		País
OrganizationalUnit		Certificado de Sello de Entidad
subjectPublicKeyInfo		RSA mínimo 2048 bits ECDSA 254 bits (prime256v1) ó 384 bits (secpr384r1)
extensions		
issuerAltName		Igual al campo SubjectAlternativeNames de la CA Emisora
extendedKeyUsage		clientAuth, emailProtection
subjectKeyIdentifier		Derivada del resultado de aplicar el hash a la clave pública del sujeto
authorityKeyIdentifier		Derivada del resultado de aplicar el hash a la Clave pública de la AC emisora
certificatePolicies*		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.0.41232
cpsURI		http://policy.eadtrust.eu
userNotice		"European Agency of Digital Trust, S.L. Legal Person Qualified Certificate for Qualified Payment Service Provider."
policyIdentifier		0.4.0.194112.1.1 (OID ETSI QCP-l)
userNotice		European Telecommunications Standards Institute. eIDAS European Regulation Compliant
cRLDistributionPoints		http://crl.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadlp<Año>.crl
authorityInfoAccess		
caIssuers		http://ca.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadlp<Año>.crt
ocsp		http://ocsp.eadtrust.eu
basicConstraint	Crítica	CA false
qcStatements**		
QcCompliance		Presente
QcType		id-etsi-qct-eseal
QcRetentiodPeriod		15
qcStatement-2		0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)
PSD2QcType		ETSI TS 119 495 Format
keyUsage	Crítica	digitalSignature, nonRepudiation, keyEncipherment

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

8.5 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.

8.6 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 ó 2048 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

9 Auditoría de cumplimiento y otras evaluaciones

EADTrust ha superado anualmente desde 2009 diversas auditorías de su **Sistema Integrado de Gestión** con respecto a varias normas.

En estos momentos, **EADTrust** está certificado respecto a las normativas "**UNE EN ISO 9001:2015**", "**UNE ISO/IEC, 27001:2014**" y "**UNE ISO/IEC 20000-1:2011**" a través de la entidad **LRQA Business Assurance**, 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.* Estos son los certificados:

Norma	Certificado
ISO 20000-1:2011	SGI 6015629/114
ISO 27001:2013	SGI 6015629/19
ISO 9001:2015	SGI 6015629/11

EADTrust ha superado varias auditorías de tipo "Penetration testing" para verificar la resistencia de su infraestructura a diversos ataques de seguridad potenciales y se estima una cadencia aproximadamente anual para repetir las auditorías de este tipo.

EADTrust se somete con la periodicidad indicada en el Reglamento UE 910/2014 a auditorías de cumplimiento de los requisitos relativos a los prestadores de servicios electrónicos de confianza cualificados, en base a las normas:

- ETSI EN 319 401 V2.2.1 (2018-04) - Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- ETSI EN 319 411-1 V1.2.2 (2018-04) - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- ETSI EN 319 411-2 V2.2.2 (2018-04) - 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.

En el marco de los requisitos de CAB Forum, las auditorías son anuales.

10 Otros servicios electrónicos de confianza

10.1 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.

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.

10.1.1 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. 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[40].

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 por NTP en fecha y hora, a fin de evitar incoherencias y permitir establecer correlaciones entre los registros de actividad (lo que implica eventos de auditoría) grabados en los diferentes sistemas. Los NTP`s refrescan el tiempo del sistema en periodos inferiores a una (1) hora.

Dicha sincronización se realizará de forma automática mediante al menos dos servicios externos de referencia horaria precisa, conforme al estándar Greenwich Mean Time (GMT) y que ofrezca garantía de disponibilidad.

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.

10.1.2 Aspectos relevantes del servicio cualificado de sello de tiempo

Los tokens de sellado de tiempo se sellan con los certificados EADTrust de TSU, emitidos bajo la Cadena de Certificación descrita. 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 Política de Sellado de Tiempo (best practices policy for time-stamp) se identifica y referencia en ETSI OID 0.4.0.2023.1.1

El OID del proveedor de servicios de confianza con respecto al servicio de sellado de tiempo es:

[40]RFC 5905 - Network Time Protocol Version 4: Protocol and Algorithms Specification

- TimeStamping: 1.3.6.1.4.1.501.2.2
- No cualificado: 1.3.6.1.4.1.501.2.2.0
- Cualificado: 1.3.6.1.4.1.501.2.2.1

Este árbol OID se identifica con el nombre de la plataforma de EATrust 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.

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 (timestampin Unit), que podrán desplegarse en las infreatructuras propias o en las instalaciones de las entidades cliente.

Las características del sello de tiempo son las siguientes:

- Los algoritmos de hash soportados son SHA-1, SHA-256 y SHA-512, a petición del cliente
- 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 organismo 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 electríca 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.

10.2 Servicio de voto electrónico

EADTrust ofrece servicios de voto electrónico societario (servicio no cualificado por no estar contemplado en el Reglamento eIDAS). Este servicio permite registrar el voto en consejos de administración, juntas de accionistas, asambleas de socios, o elecciones en órganos participativos.

El servicio permite acreditar la identidad de los votantes y recoger información sobre su participación como socio o accionista, disociando o no según corresponda la información del voto respecto a la del votante.

10.3 Servicio de comprobación fehaciente de contenidos en páginas web.

EADTrust ofrece un servicio de Comprobación fehaciente de publicación en páginas web (servicio no cualificado por no estar contemplado en el Reglamento eIDAS). Este servicio resuelve la necesidad de los administradores de las sociedades de capital de acreditar la publicación en la página web de la sociedad de la convocatoria y otros documentos asociados a la Junta de Accionistas.

Este servicio también permite generar testimonio de publicación de contenidos en páginas web concretas en caso de que se consideren beneficiosos o perjudiciales para el solicitante, y este los requiera como prueba para ejercitar sus derechos.

10.4 Foro electrónico de accionistas

EADTrust ofrece servicios de foro electrónico de accionistas (servicio no cualificado por no estar contemplado en el Reglamento eIDAS). Este servicio permite acreditar la identidad de los usuarios del foro y recoger información sobre su participación como socio o accionista como requisito de participación.

La obligatoriedad de creación de Foros de Accionistas para sociedades anónimas cotizadas en España se recoge en el artículo 539 (Instrumentos especiales de información) de la Ley de Sociedades de Capital[41].

10.5 Generación y custodia de claves

EADTrust ofrece servicios de generación y custodia de claves (servicio no cualificado por no estar contemplado en el Reglamento eIDAS). Este se lleva a cabo a partir de un proceso de generación de una o varias parejas de claves (ceremonia de generación de claves) para uso en sistemas de firma biométrica (fima digitalizada manuscrita o vocal).

La entidad recibe las claves públicas para su uso en el software de la plataforma.

Las claves privadas las custodia el Prestador de Servicios de Confianza Digital, que las tendrá a disposición de quienes acrediten interés legítimo para extraer la información biométrica de los documentos firmados. La entidad solicitante debe aportar el software que permite la extracción de datos adecuada a la forma en que codifique la información en su propio formato.

Los firmantes de documentos electrónicos con firma biométrica suelen recibir de la entidad que gestiona las firmas electrónicas información del custodio al que acudir para descifrar la información biométrica de los documentos que enntregan. Pueden acudir personalmente o través de un mandatario o apoderado.

[41] https://www.boe.es/buscar/act.php?id=BOE-A-2010-10544

La comprobación de la información biométrica de una firma cuestionada comparándola con varias indubitadas las realizan peritos especializados, dado que esa tarea no corresponde a la entidad que custodia las claves.

10.6. Servico de custodia digital "Cartulario"

"Cartulario" es un servicio gestionado a través de webservice, para entornos de alto volumen de custodia de documentos. (Servicio no cualificado por no estar contemplado en el Reglameno eIDAS). El servicio permite:

- La asignación de códigos <CSV> (Código Seguro de verificación).
- Envío a custodia de documentos con el código asignado
- Inclusión de sellado de tiempo en el momento de archivado
- Obtención de documentos a partir de su código.

Una variante de uso de "Cartulario" permite gestionar el servicio cualificado de conservación de firmas electrónicas y sellos electrónicos. Este servicio cumple todos los requisitos para ser cualificado, condición que adquirirá luego de superar la evaluación correspondiente.

10.7 Servicio de notificaciones certificadas "Noticeman"

Noticeman es la plataforma de gestión de notificaciones por e-mail y SMS que permite dejar constancia de la identidad del remitente, del destinatario, del contenido de la comunicación y de los momentos en los que se produjo su puesta a disposición y el acceso a dicho contenido. Este sistema incluye un módulo para gestionar la prestación del consentimiento y permite el perfeccionamiento de contratos (firma avanzada).

Se puede utilizar por diferentes profesionales y organismos tales como administraciones públicas, ya que cumple la normativa aplicable, en España: Ley 18/2011, Ley 39/2015, Ley 40/2015 y Ley 42/2015. Sustituye ventajosamente al Burofax.

Las notificaciones completas incluyen:

- Acta (justificante de la notificación).
- Avisos de no recepción
- 5 sellados de tiempo de los distintos eventos de la notificación.
- 6 años de custodia en servicio Cartulario (ampliables)

De indicarse expresamente permiten envíos de SMS con efecto de notificación o con efecto de autenticación. (OTP, One Time Password). Son válidas en cualquier jurisdicción, ya que no requieren "Apostilla de la Haya".

Este servicio cumple todos los requisitos para ser cualificado, condición que adquirirá luego de superar la evaluación correspondiente.

10.8 Servicio de comprobación de validez de certificados

Servicio de comprobación de firmas electrónicas y de certificados de la forma prevista en los artículos 32 y 33 del Reglamento UE 910/2014 (eIDAS), mediante el protocolo Digital Signature Services (DSS) de OASIS.

- El usuario envía una petición de Validación de Certificado y/o Firma al servidor de Validación de EADTrust.
- La Autoridad de Validación de EADTrust, una vez consultadas las fuentes OCSP (Online Certificate Status Protocol) o la CRL (Certificate Revocation List) del emisor de los certificados presentados, recibe la información relativa al estado actual del Certificado y/o Firma.
- El Usuario recibe la respuesta del estado actual del Certificado y/o Firma a través del Web Services.
- Se informa sobre el tipo de firma implementado y ofrece la posibilidad de ampliar la firma (P.Ej. a ADES-T añadiendo un Timestamping)

Este servicio cumple todos los requisitos para ser cualificado, condición que adquirirá luego de superar la evaluación correspondiente.

11 Otras cuestiones empresariales y legales

11.1 Tarifas

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

11.2 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.

11.3 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.

11.4 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.

11.4.1 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.

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/

11.4.2 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.

11.5 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 Root de la CA será responsable del desempeño y las garantías de la CA subordinada, para el cumplimiento de la CA subordinada con estos requisitos, y para todas las responsabilidades y obligaciones de indemnización de la CA subordinada bajo estos requisitos, así como si la root de la CA fuera la CA subordinada emitiendo los certificados.

11.6 Garantías del suscriptor

EADTrust exigirá, como parte del Acuerdo del Suscriptor o los Términos de Uso, que el Solicitante realice los compromisos y garantías en esta sección para el beneficio de la CA y los Beneficiarios del Certificado. Antes de la emisión de un Certificado, la CA obtendrá, para beneficio expreso de la CA y los beneficiarios del certificado, ya sea:

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 contra el 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 que el Solicitante haya hecho en nombre de su director o agente bajo una relación de subcontratación o servicio de alojamiento) 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 certificado/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 y garantía de instalar el Certificado solo en servidores a los que se pueda acceder mediante el subjetAltName listado en el Certificado, y usar el Certificado únicamente conforme a todas 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.

11.7 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.

11.8 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.

11.8.1 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 de la extinción o suspensión de la vigencia del certificado electrónico.

EADTrust como prestador de servicios de certificación asumirá toda la responsabilidad frente a terceros por la actuación de las personas en las que deleguen la ejecución de alguna o algunas de las funciones necesarias para la prestación de servicios de confianza.

11.8.2 Entidad de registro

La Autoridad de Registro asumirá toda la responsabilidad sobre la correcta identificación de los solicitantes y la comprobación de sus datos, con las mismas limitaciones que se establecen para la Autoridad de Certificación.

11.8.3 Responsabilidades del titular de los certificados

El titular de los certificados asumirá toda la responsabilidad y riesgos derivados de la fiabilidad y seguridad del puesto de trabajo, equipo informático o medio desde el cual emplee su certificado.

Así mismo el titular de los certificados se responsabilizará de los riesgos derivados de la aceptación de una conexión segura sin haber realizado previamente la preceptiva verificación de la validez del certificado exhibido por el prestador de servicios.

Los procedimientos para contrastar la seguridad de la conexión con dicho prestador de servicios deberán ser proporcionados por éste al titular del certificado, por ejemplo, mediante técnicas de OCSPStapling (es decir haciendo uso de la extensión "TLS CertificateStatusRequest" descrita en la sección 8 de la norma **RFC 6066**)[42]

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.

11.9 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.

[42]La norma RFC 6961 "TheTransportLayer Security (TLS) - MultipleCertificate Status RequestExtension" contempla múltipes respuestas, en el establecimiento de sesiones TLS, lo que permite validar los certificados de las CAs intermedias de la cadena de confianza.

- 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.

11.9.1 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.

11.9.2 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.

11.10 Enmiendas y cambios

11.10.1 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 http://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.

11.10.2 Mecanismo y periodo 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.

11.10.3 Circunstancias bajo las cuales debe modificarse el OID

Se asignarán OID específicos para las funciones y significados de información que sean significativos para los suscriptores y para los terceros que confían.

Cuando se realicen cambios en una CP específica que afecte a su aplicabilidad, se procederá a cambiar el OID de esta.

11.11 Quejas. Reclamaciones y jurisdicción

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

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

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

En caso de que el usuario no esté conforme con la resolución de la queja. Este podrá presentar una solicitud de recurso de apelación ante la Dirección General de EADTrust. Para ello solo deberá

comunicarse vía e mail a info@eadtrust.eu , indicando en el asunto que se trata de un recurso de apelación, también podrá emplearse la vía del correo postal.

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

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

La actividad de EADTrust se rije 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.

12 Referencias

12.1 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.[43]
- 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.[44]
- 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.[45]
- 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.[46]
- 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.[47]
- 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)

[43] http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679
[44] http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32014R0910&from=EN
[45] http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:JOL_2015_053_R_0006&from=EN
[46] http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:JOL_2015_128_R_0006&from=ES
[47] 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.[48]

- 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.[49]
- 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].[50]
- 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.[51]
- 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

En relación con los certificados de seudónimo:

- Real Decreto 668/2015, de 17 de julio, por el que se modifica el Real Decreto 1671/2009, 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.[52]

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.
- Ley 32/2014, de 22 de diciembre, de Metrología.

12.2 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:

- Real Decreto 1671/2009, 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.

[48] http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:JOL_2015_235_R_0002&qid=1441792087678&from=ES
[49] http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:JOL_2015_235_R_0006&qid=1441792087678&from=ESEnlaces-Legislacion
[50] http://www.boe.es/doue/2015/289/L00018-00025.pdf
[51] http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016D0650&from=EN
[52] https://www.boe.es/buscar/doc.php?id=BOE-A-2015-8048

- Real Decreto 668/2015, de 17 de julio, por el que se modifica el Real Decreto 1671/2009, 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.
- 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 Garantia 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.

13 Anexos

13.1 Sello de tiempo electrónico de confianza

A menudo, las formalidades y los procedimientos exigen una prueba no sólo del estado de validez del certificado en el momento de la firma, sino también del momento en que se emitió. El servicio de sello de tiempo de EADTrust es el elemento gracias al cual se puede garantizar la fecha y hora de cualquier operación. Este servicio de sello de tiempo (o TSA, TimeStamping Authority en inglés) está diseñado según las recomendaciones y estándares internacionales:

- Cumple con la recomendación RFC 3161 del grupo EngineeringTaskForce PKIX "Protocolo de sello de tiempo (TSP)" (http://www.ietf.org/html.charters/pkix-charter.html).
- Los requisitos establecidos por ETSI (Organización Europea de Normalización por la Comisión Europea) en sus documentos ETSI EN 319 421 y ETSI EN 319 422.
- Tomando como fuente de tiempo el Real Instituto y Observatorio de la Armada Española, que se encarga de calcular y establecer el tiempo legal oficial en España (conocido como ROA Time) aunque sincronizado preferentemente a la fuente de tiempo de satélites GPS y Galileo.
- Bajo las directivas de la "Oficina Internacional de Pesos y Medidas", que tiene la función de garantizar la uniformidad de las medidas y su trazabilidad en el sistema internacional de unidades.

13.2 Usos de OIDS por EADTRUST

13.2.1 Arcos 19126 y 501

En el pasado, EADTrust ha utilizado el OID 1.3.6.1.4.1.19126 para los servicios de confianza desplegados con anterioridad a la entrada en vigor del Reglamento UE 910/2014 (AECODI, Agencia Europea de Confianza Digital, European Agency of Digital Trust).

A partir de 2016, el OID utilizado es **1.3.6.1.4.1.501** correspondiente al Proyecto SPRITEL[53]de EADTrust. En este efoque, los servicios que se desarrollan por EADTrust enfatizan la gestión de identidades (eId) y representación (PoA: Power of Attorney) además de la gestión de evidencias electrónicas en formas afines a Blockchain (Electronic Ledger).

13.2.2 OID basados en 19126

Aunque en la fecha de edición de esta versión de la DPC no existen certificados expedidos no caducados basados en este arco, se incluyen los significados de OID subordinados al arco 1.3.6.1.4.1.19126 como referencia histórica.

13.2.2.1 Tabla de asignación de OID para el arco 1 (root-raíz)

OID	Asignación
1.50	Policy Framework
1.60	BINUM (bool)
1.61	BINUM (human readable explanation)
1.62	BINUM (serial number)

13.2.2.2 Tabla de asignación de OID para el arco 2 (Policy)

OID	Asignación
2.1	**Certificate Policy**
2.1.0	Demo Certificate
2.1.1	Timestamp Certificate
2.1.2	Validation Certificate
2.1.3	SSL Certificate
2.1.4	ACL Device
2.1.5	Personal Certificate
2.1.6	Subsidiary Root Certificate

[53] Secure Platform for Registered Identities and Trusted Electronic Ledger

Variantes:

OID	Asignación
2.2	**Timestamp Policy**

El siguiente nodo codifica la versión, empezando por 1:

OID	Asignación
2.2.0	Integration Test
2.2.1	Reservado
2.2.2	Best Effort
2.2.3	Resilient
2.2.4	Timestamp Unit (TSU)

Variantes:

OID	Asignación
2.3	**Authentication Policy**

El siguiente nodo codifica la versión, empezando por 1:

OID	Asignación
2.3.1	Enrollment
2.3.2	Identity verification
2.3.3	Role accreditation

Variantes:

OID	Asignación
2.3.1.0	Integration Test
2.3.1.1	Reservado
2.3.1.2	Face to face enrollment
2.3.1.3	Remote enrollment (Video conferencing)
2.3.1.4	Remote enrollment (Video recording)
2.3.1.5	Remote enrollment (reinforced verification) Biometrics, Banck account checking

Variantes de **Enrollment**:
El siguiente nodo codifica la versión, empezando por 1:

OID	Asignación
2.3.2.0	Claimed identity – Identidad declarada
2.3.2.1	LoA 1 - ISO/IEC 29115:2013
2.3.2.2	LoA 2 - ISO/IEC 29115:2013
2.3.2.3	LoA 3 - ISO/IEC 29115:2013
2.3.2.4	LoA 4 - ISO/IEC 29115:2013
2.3.2.5	Broker oriented
2.3.2.6	Integration Test

Variantes de **Identity verification**
El siguiente nodo codifica la versión, empezando por 1:

Variantes de **Role accreditation**

OID	Asignación
2.3.3.0	Integration Test
2.3.3.1	Identity “Role-based” Claims

Identity “Role-based” Claims

El siguiente nodo codifica la versión, empezando por 1

13.2.2.3 Tabla de asignación de OID para el arco 3 (Trust Services)

OID	Asignación
3.1	Digital Custody
3.2	Electronic delivery
3.3	Web Attestation
3.4	Handwritten Electronic Signature
3.5	Electronic vote
3.6	Remote signature
3.7	Contract platform

El siguiente nodo codifica la variante, empezando por 1.

El nodo posterior codifica la versión, empezando por 1.

13.2.3 OID basados en 501

1.3.6.1.4.1.501 Spritel base OID

13.2.3.1 Tabla de asignación de OID para el arco 2 (Policy)

OID	Asignación
2.0	Test
2.1	Certificate
2.2	Timestamping
2.3	Identity Management
2.4	Electronic delivery
2.1.0	**Non qualified Certificate**

OID	Asignación
2.1.0.0	non-QSCD Cert; key generated by TSP
2.1.0.1	QSCD-based Cert; key generated by TSP
2.1.0.2	non-QSCD server-based; key generated by TSP
2.1.0.3	QSCD server-based; key generated by TSP
2.1.0.4	non-QSCD Crt; key generated by USR
2.1.0.5	QSCD-based Crt; key generated by USR
2.1.0.6	non-QSCD server-based; key generated by USR
2.1.0.7	QSCD server-based; key generated by USR (non-available/reserved)
2.1.1	**Qualified Certificate**
2.1.1.0	non-QSCD QC; key generated by TSP
2.1.1.1	QSCD-based QC; key generated by TSP
2.1.1.2	non-QSCD server-based; key generated by TSP
2.1.1.3	QSCD server-based; key generated by TSP
2.1.1.4	non-QSCD QC; key generated by USR
2.1.1.5	QSCD-based QC; key generated by USR
2.1.1.6	non-QSCD server-based; key generated by USR
2.1.1.7	QSCD server-based; key generated by USR (non-available/reserved)
2.2	**Timestamping**
2.2.0	Non-qualified Timestamping
2.2.1	Qualified Timestamping

2017 Oriented Qualified Policies (Related to standard number)

OID de Políticas

2.1.1.1.401	oidPolicyQcCA- EADTrust's base certificate policy w/ QSCD (used in Roots &SubCAs) – EN 319 401
2.1.1.1.421	oidPolicyQcTS- Eadtrust's qualified TimeStamping certificate policy w/ QSCD – EN 319 421
2.1.1.1.4122	oidPolicyQcNP- Eadtrust's qualified natural person certificate policy w/ QSCD – EN 319 412-2
2.1.1.1.4123	oidPolicyQcLP- Eadtrust's qualified legal person certificate policy w/ QSCD – EN 319 412-3
2.1.1.1.4124	oidPolicyQcLP- Eadtrust's qualified web site certificate policy w/ QSCD – EN 319 412-4

13.2.4 OID definidos por normas técnicas

Los certificados cualificados pueden incluir diferentes informaciones, más allá de la propia condición de **cualificado** del certificado, para lo que se emplean valores específicos de OID.

La codificación de ciertas características de los certificados **cualificados** se señala mediante campos OID (ObjectIdentifier) específicos.

La norma técnica que los indicaba era hasta hace unos meses la ETSI TS 101 862, que los reflejaba trayendo a colación el arco (hoy obsoleto):

- 1.3.6.1.5.5.7.0.11

Y definiendo la información de la declaración de certificado cualificado (QC-Statement) con el arco:

- 0.4.0.1862

En la actualidad, la norma de aplicación es la **ETSI EN 319 412-1** lo que ha dado lugar a que la información sobre certificados cualificados no incluidos en la norma anterior se refleje con un nuevo arco OID:

- 0.4.0.194121

Por tanto, los certificados cualificados podrán indicar ciertas características de los certificados con OIDs que comienzan con 0.4.0.1862 (originalmente diseñados para firma electrónica de personas físicas según la Directiva 1999/93, pero hoy en día adecuados también para personas jurídicas por la ampliación de conceptos como el sello electrónico del Reglamento UE 910/2014 - eIDAS) y otras con OID que comienzan con 0.4.0.194121 (específicamente para diferenciar los certificados de persona física y jurídica tal como lo hace el Reglamento UE 910/2014 - eIDAS).

También el arco 0.4.0.1456 tiene su interés debido a la norma pre-eIDAS TS 101 456

Estos son los principales OIDs para los certificados cualificados:

- 0.4.0.1456.1.1 – qcp-public-with-sscd – A certificate policy for qualified certificates issued to the public, requiring use of secure signature-creationdevices. Defined in TS 101 456.

- 0.4.0.1456.1.2 – qcp-public – A certificate policy for qualified certificates issued to the public, Defined in TS 101 456.
- 0.4.0.1862.1.1 – qcStatement – QcCompliance (**Obligatorio**).
- 0.4.0.1862.1.2 – qcStatement – QcLimitValue.
- 0.4.0.1862.1.3 – qcStatement – QcRetentionPeriod.
- 0.4.0.1862.1.4 – qcStatement – QcSSCD.
- 0.4.0.1862.1.5 – qcStatement – QcPDS (**Opcional**). Proporcionará al menos una URL a un PDS (**PKI DisclosureStatements**) en inglés. Se pueden referenciar otros documentos PDS en otros idiomas con este QCStatement siempre que sean equivalentes al PDS en inglés. No se debe hacer referencia a más de un PDS por idioma.
- 0.4.0.1862.1.6 – qcStatement – QcType.
  - 0.4.0.1862.1.6.1 – id-etsi-qct-esign.
  - 0.4.0.1862.1.6.2 – id-etsi-qct-eseal.
  - 0.4.0.1862.1.6.3 – id-etsi-qct-web.
- 0.4.0.194121.1.1 -> id-etsi-qcs-semanticsId-Natural ->**Natural personsemantics** (para certificados de persona física – firma electrónica).
- 0.4.0.194121.1.2 -> id-etsi-qcs-SemanticsId-Legal -> **Legal personsemantics** (para certificados de persona jurídica – sello electrónico).
- 0.4.0.194112.1.0 -> QCP-n ->qcp-natural: certificate policy for European Union (EU) qualifiedcertificatesissuedto natural persons.
- 0.4.0.194112.1.1 -> QCP-l ->qcp-legal: certificate policy for European Union (EU) qualifiedcertificatesissuedto legal persons.
- 0.4.0.194112.1.2 -> QCP-n-qscd ->qcp-natural-qscd: certificate policy for European Union (EU) qualified certificates issued to natural persons with private key related to the certified publickey in a Qualified electronic Signature/sealCreationDevice (QSCD)
- 0.4.0.194112.1.3 -> QCP-l-qscd ->qcp-legal-qscd: certificate policy for European Union (EU) qualified certificates issued to legal persons with private key related to the certified public key in a Qualified electronic Signature/sealCreationDevice (QSCD)
- 0.4.0.194112.1.4 -> QCP-w -> QCP-web: certificate policy for European Union (EU) qualified web site authentication certificates.

El conocimiento de estos OID es esencial para comprobar si los perfiles de los certificados cualificados expedidos por los Prestadores de Servicios Electrónicos de Confianza están correctamente diseñados.

13.2.5 OID definidos en normas españolas de administración pública

Para los certificados de empleado público y para los de persona jurídica y representante, la Administración Española ha definido unos perfiles[54] que conviene cumplir.

Como parte de la estandarización, los campos, principalmente alineados a la RFC 5280 (X509 v3), las normas europeas (EN 319 412) y las Guías del CAB Forum, tienen OIDs (object identifiers, secuencia de números para identificar un campo) los cuales son unívocos internacionalmente.

Los prestadores de servicios de certificación deberán identificar cada tipo de certificado (Sede, sello, empleado público) con un OID específico, que deberá ser unívoco y que no podrá emplearse para identificar tipos diferentes, políticas o versiones de certificados, emitidos por dicho prestador.

[54] https://administracionelectronica.gob.es/ctt/politicafirma/descargas

Dentro de los certificados existirán campos comunes a los ya vigentes o estandarizados, ej: commonName (cuyo OID es 2.5.4.3) o serialNumber (cuyo OID es 2.5.4.5). También disponen de un conjunto de campos nuevos o "propietarios" llamados Identidad Administrativa, la cual identifica al Suscriptor del certificado de forma unívoca y completa.

Para el objeto Identidad Administrativa, al tratarse de un conjunto de campos completamente nuevos, se ha optado por la siguiente opción para asignarles los OID:

Se utilizará el número ISO/IANA del MPR 2.16.724.1.3.5.X.X como base para identificarlo, de este modo se establecería un identificador unívoco a nivel internacional, haciendo que cualquier prestador pueda utilizarlo:

En base a esta norma se definen los siguientes OID:

- 2.16.724.1.3.5.4.1= CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO (Nivel Alto).
- 2.16.724.1.3.5.4.2= CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO (Nivel Medio/Sustancial)).
- 2.16.724.1.3.5.5.1=SEDE ELECTRONICA (Nivel Alto).
- 2.16.724.1.3.5.5.2=SEDE ELECTRONICA (Nivel Medio/Sustancial)).
- 2.16.724.1.3.5.6.1=SELLO ELECTRONICO PARA LA ACTUACION AUTOMATIZADA (Nivel Alto).
- 2.16.724.1.3.5.6.2=SELLO ELECTRONICO PARA LA ACTUACION AUTOMATIZADA (Nivel Medio/Sustancial)).
- 2.16.724.1.3.5.7.1=CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO (Nivel Alto).
- 2.16.724.1.3.5.7.2=CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO (Nivel Medio/Sustancial)).
- OID = 2.16.724.1.3.5.8. Indica que el certificado es un **certificado de representante de persona jurídica, con poderes totales**, administrador único o solidario de la organización, o al menos con poderes específicos generales para actuar ante las AAPP.

Esto no aplica a los certificados de Sede, ya que para ajustarse a las directivas del **CAB Forum** no contienen el objeto Identidad Administrativa, aunque si utilizarán los mencionados OIDs para identificar el tipo de certificado en la extensión Certifícate Policies.

El documento Perfiles de certificados electrónicos 2.0 contiene más información de interés sobre la codificación de OIDs y perfiles de certificados.

13.3 Listado completo de los certificados vigentes de EADTrust

13.3.1 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-----

13.3.2 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-----

13.3.3 EADTRUST ECC 256 ROOT CA FOR QUALIFIED CERTIFICATES 2019

-----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-----

13.3.4 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-----
```


13.3.5 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-----
```


13.3.6 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-----

13.3.7 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-----

13.3.8 EADTRUST RSA 2048 ROOT CA FOR QUALIFIED CERTIFICATES 2019

-----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-----

13.3.9 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-----

13.3.10 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-----

13.3.11 EADTRUST RSA 4096 ROOT CA FOR QUALIFIED CERTIFICATES 2019

-----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-----

13.3.12 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-----

13.3.13 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
TapoXnJcBWYOb10GYCk2H93WCJ14rGfuZczwzBdiHGjE9Gi1vVzBPb9+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-----

13.3.14 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-----
```


13.3.15 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-----
```


13.3.16 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-----

13.3.17 EADTRUST ECC 256 SUBCA FOR QUALIFIED CERTIFICATES 2019

-----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-----

13.3.18 EADTRUST ECC 256 SUBCA FOR QUALIFIED CERTIFICATES 2019

-----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-----

13.3.19 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-----

13.3.20 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-----

13.3.21 EADTRUST ECC 384 SUBCA FOR QUALIFIED CERTIFICATES 2019

-----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-----

13.3.22 EADTRUST ECC 384 SUBCA FOR QUALIFIED CERTIFICATES 2019

-----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-----

13.3.23 EADTRUST RSA 2048 SUBCA FOR QUALIFIED CERTIFICATES 2019

-----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-----

13.3.24 EADTRUST RSA 2048 SUBCA FOR QUALIFIED CERTIFICATES 2019

-----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/p1E3YhqlAckr8hGmz4ILCNkssePtORbFdR3jh4FtU
cka3JrUxJgQ0PEk2lCdWrtRrJywKValDWs0E3w==
-----END CERTIFICATE-----

13.3.25 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-----

13.3.26 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-----

13.3.27 EADTRUST RSA 4096 SUBCA FOR QUALIFIED WEB EV/PSD2 CERT 2019

-----BEGIN CERTIFICATE-----
MIIHMzCCBRugAwIBAgIIRhJxmAQWRCYwDQYJKoZIhvcNAQELBQAwgYYxRjBEBgNV
BAMMPUVBRFRydXN0IFJTQSA0MDk2IFJvb3QgQ0EgRm9yIFF1YWxpZmllZCBXZWIg
RVYvUFNEMiBDZXJ0IDIwMTkxLzAtBgNVBAoMJkV1cm9wZWFuIEFnZW5jeSBvZiBE
aWdpdGFsIFRydXN0LCBTLkwuMQswCQYDVQQGEwJFUzAeFw0xOTA2MDYxMTM3MDJa
Fw0zMTA2MDMxMTM3MDJaMIGEMUQwQgYDVQQDDDtFQURUcnVzdCBSU0EgNDA5NiBT
dWJDQSBGb3IgUXVhbGlmaWVkIFdlYiBFViA9QU0QyIENlcnQgMjAxOTEvMC0GA1UE
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-----

13.3.28 EADTRUST RSA 4096 SUBCA FOR QUALIFIED CERTIFICATES 2019

-----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-----

13.3.29 EADTRUST RSA 4096 SUBCA FOR QUALIFIED CERTIFICATES 2019

-----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-----

13.3.30 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-----

13.3.31 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
c0nzXfcwTgYDVR0fBEcwRTBDoEGgP4Y9aHR0cDovL2NybC5lYWR0cnVzdC5ldS9l
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-----

13.3.32 EADTRUST RSA 8192 SUBCA FOR QUALIFIED CERTIFICATES 2019

-----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-----

13.3.33 EADTRUST RSA 8192 SUBCA FOR QUALIFIED CERTIFICATES 2019

-----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
FWh0dHA6Ly9jYS5lYWR0cnVzdC5ldYYZaHR0cDovL3BvbGljeS5lYWR0cnVzdC5l
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-----

13.4 Declaración de cumplimiento del Reglamento UE 910/2014 (EIDAS).

EADTrust da cumplimiento al Reglamento UE 910/2014 (eIDAS). Seguidamente se indican aspectos concretos de la norma de modo que el requisito legal esté contemplado en la Declaración de Prácticas de Certificación:

13.4.1 Artículo 8. Niveles de Seguridad de los sistemas de Identificación electrónica

EADTrust ha instrumentado un sistema de identificación electrónica atemperado a lo establecido en el Reglamento eIDAS, para ello ha identificado los niveles de seguridad diseñados para cada servicio y tomado medidas técnicas, operacionales y organizativas que garantizan la fiabilidad y calidad de los servicios cualificados prestados, particularmente los relacionados con la identificación, autenticación, validación de la identidad declarada por los solicitantes de certificados.

En consecuencia, se han instrumentado varios procedimientos que regulan el ciclo de vida de los certificados, que involucran además cuestiones técnicas, organizativas y operacionales para garantizar la fiabilidad de los servicios prestados.

13.4.1 Artículo 13. Responsabilidad y carga de la prueba

1. Sin perjuicio de lo dispuesto en el apartado 2, los prestadores de servicios de confianza serán responsables de los perjuicios causados de forma deliberada o por negligencia a cualquier persona física o jurídica debido al incumplimiento de las obligaciones establecidas en el presente Reglamento.

La carga de la prueba de la intencionalidad o la negligencia de un prestador no cualificado de servicios de confianza corresponderá a la persona física o jurídica que alegue los perjuicios a que se refiere el primer párrafo.

Se presumirá la intencionalidad o la negligencia de un prestador cualificado de servicios de confianza salvo cuando ese prestador cualificado de servicios de confianza demuestre que los perjuicios a que se refiere el párrafo primero se produjeron sin intención ni negligencia por su parte.

2. Cuando un prestador de servicios informe debidamente a sus clientes 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.

3. Los apartados 1 y 2 se aplicarán con arreglo a las normas nacionales sobre responsabilidad.

13.4.2 Artículo 15. Accesibilidad para las personas con discapacidad

Siempre que sea factible, los servicios de confianza prestados y los productos para el usuario final utilizados en la prestación de estos servicios deberán ser accesibles para las personas con discapacidad.

13.4.3 Artículo 19. Requisitos de seguridad aplicables a los prestadores de servicios de confianza

1. Los prestadores cualificados y no cualificados de servicios de confianza adoptarán las medidas técnicas y organizativas adecuadas para gestionar los riesgos para la seguridad de los servicios de confianza que prestan. Habida cuenta de los últimos avances tecnológicos, dichas medidas garantizarán un nivel de seguridad proporcionado al grado de riesgo. En particular, se adoptarán medidas para evitar y reducir al mínimo el impacto de los incidentes de seguridad e informar a los interesados de los efectos negativos de cualquiera de tales incidentes.

2. Los prestadores cualificados y no cualificados de servicios de confianza, sin demoras indebidas pero en cualquier caso en un plazo de 24 horas tras tener conocimiento de ellas, notificarán al organismo de supervisión y, en caso pertinente, a otros organismo relevantes como el organismo nacional competente en materia de seguridad de la información, o la autoridad de protección de datos, cualquier violación de la seguridad o pérdida de la integridad que tenga un impacto significativo en el servicio de confianza prestado o en los datos personales correspondientes.

Cuando la violación de seguridad o la pérdida de integridad puedan atentar contra una persona física o jurídica a la que se ha prestado el servicio de confianza, el prestador de servicios de confianza notificará también a la persona física o jurídica, sin demora indebida, la violación de seguridad o la pérdida de integridad.

Cuando proceda, en particular si una violación de la seguridad o pérdida de la integridad afecta a dos o más Estados miembros, el organismo de supervisión notificado informará al respecto a los organismos de supervisión de los demás Estados miembros de que se trate y a la ENISA.

El organismo de supervisión notificado informará al público o exigirá al prestador de servicios de confianza que lo haga, en caso de considerar que la divulgación de la violación de seguridad o la pérdida de integridad reviste interés público.

3. El organismo de supervisión facilitará a la ENISA anualmente un resumen de las notificaciones de violación de la seguridad y pérdida de la integridad recibidas de los prestadores de servicios de confianza.

4. La Comisión podrá, mediante actos de ejecución, establecer:

a) una mayor especificación de las medidas a que se refiere el apartado 1, y
b) la definición de los formatos y procedimientos, incluidos los plazos, aplicables a efectos del apartado 2.

Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

13.4.4 Artículo 20. Supervisión de los prestadores cualificados de servicios de confianza

1. Los prestadores cualificados de servicios de confianza serán auditados, al menos cada 24 meses, corriendo con los gastos que ello genere, por un organismo de evaluación de la conformidad. La finalidad de la auditoría será confirmar que tanto los prestadores cualificados de servicios de confianza como los servicios de confianza cualificados que prestan cumplen los requisitos establecidos en el presente Reglamento. Los prestadores cualificados de servicios de confianza enviarán el informe de evaluación de la conformidad correspondiente al organismo de supervisión en el plazo de tres días hábiles tras su recepción.

2. Sin perjuicio de lo dispuesto en el apartado 1, el organismo de supervisión podrá en cualquier momento auditar o solicitar a un organismo de evaluación de la conformidad que realice una evaluación de conformidad de los prestadores cualificados de servicios de confianza, corriendo con los gastos dichos prestadores de servicios de confianza, para confirmar que tanto ellos como los servicios de confianza cualificados que prestan cumplen los requisitos del presente Reglamento. En caso de posible infracción de las normas sobre protección de datos personales, el organismo de supervisión informará a las autoridades de protección de datos de los resultados de sus auditorías.

3. Cuando el organismo de supervisión requiera a un prestador cualificado de servicios de confianza que corrija el incumplimiento de requisitos del presente Reglamento y este prestador no actúe en consecuencia, en su caso, en el plazo fijado por el organismo de supervisión, el organismo de supervisión, teniendo en cuenta en particular el alcance, la duración y las consecuencias de este incumplimiento, podrá retirar la cualificación al prestador o al servicio que este presta e informar al organismo a que se refiere el artículo 22, apartado 3, a efectos de que se actualice la lista de confianza mencionada en el artículo 22, apartado 1. El organismo de supervisión comunicará al prestador cualificado de servicios de confianza la retirada de su cualificación o de la cualificación del servicio de que se trate.

4. La Comisión podrá, mediante actos de ejecución, establecer números de referencia de las siguientes normas:

a) para la acreditación de los organismos de evaluación de la conformidad y para el informe de evaluación de la conformidad a que se refiere el apartado 1;
b) sobre las disposiciones en materia de auditoría con arreglo a las cuales los organismos de evaluación de la conformidad realizarán la evaluación de la conformidad de los prestadores cualificados de servicios de confianza a que se refiere el apartado 1.

Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

13.4.5 Artículo 21. Inicio de un servicio de confianza cualificado

1. Cuando los prestadores de servicios de confianza, sin cualificación, tengan intención de iniciar la prestación de servicios de confianza cualificados, presentarán al organismo de supervisión una notificación de su intención junto con un informe de evaluación de la conformidad expedido por un organismo de evaluación de la conformidad.

2. El organismo de supervisión verificará si el prestador de servicios de confianza y los servicios de confianza que presta cumplen los requisitos establecidos en el presente Reglamento, y en particular, los

requisitos establecidos para los prestadores cualificados de servicios de confianza y para los servicios de confianza cualificados que estos prestan.

Si el organismo de supervisión concluye que el prestador de servicios de confianza y los servicios de confianza que este presta cumplen los requisitos a que se refiere el párrafo primero, el organismo de supervisión concederá la cualificación al prestador de servicios de confianza y a los servicios de confianza que este presta y lo comunicará al organismo a que se refiere el artículo 22, apartado 3, a efectos de actualizar las listas de confianza a que se refiere el artículo 22, apartado 1, a más tardar tres meses después de la notificación de conformidad con el apartado 1 del presente artículo.

Si la verificación no ha concluido en el plazo de tres meses, el organismo de supervisión informará al prestador de servicios de confianza especificando los motivos de la demora y el plazo previsto para concluir la verificación.

3. Los prestadores cualificados de servicios de confianza podrán comenzar a prestar el servicio de confianza cualificado una vez que la cualificación haya sido indicada en las listas de confianza a que se refiere el artículo 22, apartado 1.

4. La Comisión podrá, mediante actos de ejecución, definir los formatos y procedimientos a efectos de los apartados 1 y 2. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

13.4.6 Artículo 24. Requisitos para los prestadores cualificados de servicios de confianza

1. Al expedir un certificado cualificado para un servicio de confianza, un prestador cualificado de servicios de confianza verificará, por los medios apropiados y de acuerdo con el Derecho nacional, la identidad y, si procede, cualquier atributo específico de la persona física o jurídica a la que se expide un certificado cualificado.

La información a que se refiere el párrafo primero será verificada por el prestador de servicios de confianza bien directamente o bien por medio de un tercero de conformidad con el Derecho nacional:

a) en presencia de la persona física o de un representante autorizado de la persona jurídica, o
b) a 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 con respecto a los niveles de seguridad «sustancial» o «alto», o
c) por medio de un certificado de una firma electrónica cualificada o de un sello electrónico cualificado expedido de conformidad con la letra a) o b), o
d) utilizando 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.

2. Los prestadores cualificados de servicios de confianza que prestan servicios de confianza cualificados:

a) informarán al organismo de supervisión de cualquier cambio en la prestación de servicios de confianza cualificados, y de su intención de cesar tales actividades;
b) contarán con personal y, si procede, con subcontratistas, que posean los conocimientos especializados, la fiabilidad, la experiencia y las cualificaciones necesarias y hayan recibido la formación adecuada en materia de seguridad y normas de protección de datos personales y que

apliquen procedimientos administrativos y de gestión que correspondan a normas europeas o internacionales;

c) con respecto al riesgo de la responsabilidad por daños y perjuicios de conformidad con el artículo 13, mantendrán recursos financieros suficientes u obtendrán pólizas de seguros de responsabilidad adecuadas, de conformidad con la legislación nacional;

d) antes de entrar en una relación contractual, informarán, de manera clara y comprensible, a cualquier persona que desee utilizar un servicio de confianza cualificado acerca de las condiciones precisas relativas a la utilización de dicho servicio, incluidas las limitaciones de su utilización;

e) utilizarán sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad y la fiabilidad técnicas de los procesos que sustentan;

f) utilizarán sistemas fiables para almacenar los datos que se les faciliten de forma verificable, de modo que:

   i. estén a disposición del público para su recuperación solo cuando se haya obtenido el consentimiento de la persona a la que corresponden los datos,

   ii. solo personas autorizadas puedan hacer anotaciones y modificaciones en los datos almacenados,

   iii. pueda comprobarse la autenticidad de los datos;

g) tomarán medidas adecuadas contra la falsificación y el robo de datos;

h) registrarán y mantendrán accesible durante un período de tiempo apropiado, incluso cuando hayan cesado las actividades del prestador cualificado de servicios de confianza, toda la información pertinente referente a los datos expedidos y recibidos por el prestador cualificado de servicios de confianza, en particular al objeto de que sirvan de prueba en los procedimientos legales y para garantizar la continuidad del servicio. Esta actividad de registro podrá realizarse por medios electrónicos;

i) contarán con un plan de cese actualizado para garantizar la continuidad del servicio, de conformidad con las disposiciones verificadas por el organismo de supervisión con arreglo al artículo 17, apartado 4, letra i);

j) garantizarán un tratamiento lícito de los datos personales de conformidad con la Directiva 95/46/CE;

k) en caso de los prestadores cualificados de servicios de confianza que expidan certificados cualificados, establecerán y mantendrán actualizada una base de datos de certificados.

3. Cuando los prestadores cualificados de servicios de confianza que expidan certificados cualificados decidan revocar un certificado, registrarán su revocación en su base de datos de certificados y publicarán el estado de revocación del certificado oportunamente y, en todo caso, en un plazo de 24 horas después de la recepción de la solicitud. La revocación será efectiva inmediatamente después de su publicación.

4. Con respecto a lo dispuesto en el apartado 3, los prestadores cualificados de servicios de confianza que expidan certificados cualificados proporcionarán a cualquier parte usuaria información sobre el estado de validez o revocación de los certificados cualificados expedidos por ellos. Esta información deberá estar disponible al menos por cada certificado en cualquier momento y con posterioridad al período de validez del certificado en una forma automatizada que sea fiable, gratuita y eficiente.

5. La Comisión podrá, mediante actos de ejecución, establecer números de referencia de normas para sistemas y productos fiables que cumplan con los requisitos establecidos las letras e) y f) del apartado 2 del presente artículo. Se presumirá el cumplimiento de los requisitos establecidos en el presente artículo cuando los sistemas y productos fiables cumplan dichas normas. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

13.4.7 Anexo I. Requisitos de los certificados cualificados de firma electrónica

Los certificados cualificados de firma electrónica contendrán:

a) una indicación, al menos en un formato adecuado para el procesamiento automático, de que el certificado ha sido expedido como certificado cualificado de firma electrónica;
b) un conjunto de datos que represente inequívocamente al prestador cualificado de servicios de confianza que expide los certificados cualificados, incluyendo como mínimo el Estado miembro en el que dicho prestador está establecido, y
   - para personas jurídicas: el nombre y, cuando proceda, el número de registro según consten en los registros oficiales,
   - para personas físicas, el nombre de la persona;
c) al menos el nombre del firmante o un seudónimo; si se usara un seudónimo, se indicará claramente;
d) datos de validación de la firma electrónica que correspondan a los datos de creación de la firma electrónica;
e) los datos relativos al inicio y final del período de validez del certificado;
f) el código de identidad del certificado, que debe ser único para el prestador cualificado de servicios de confianza;
g) la firma electrónica avanzada o el sello electrónico avanzado del prestador de servicios de confianza expedidor;
h) el lugar en que está disponible gratuitamente el certificado que respalda la firma electrónica avanzada o el sello electrónico avanzado a que se hace referencia en la letra g);
i) la localización de los servicios que pueden utilizarse para consultar el estado de validez del certificado cualificado;
j) cuando los datos de creación de firma electrónica relacionados con los datos de validación de firma electrónica se encuentren en un dispositivo cualificado de creación de firma electrónica, una indicación adecuada de esto, al menos en una forma apta para el procesamiento automático.

13.4.8 Anexo II. Requisitos de los dispositivos cualificados de creación de firma electrónica

1. Los dispositivos cualificados de creación de firma electrónica garantizarán como mínimo, por medios técnicos y de procedimiento adecuados, que:
   a) esté garantizada razonablemente la confidencialidad de los datos de creación de firma electrónica utilizados para la creación de firmas electrónicas;
   b) los datos de creación de firma electrónica utilizados para la creación de firma electrónica solo puedan aparecer una vez en la práctica;
   c) exista la seguridad razonable de que los datos de creación de firma electrónica utilizados para la creación de firma electrónica no pueden ser hallados por deducción y de que la firma está protegida con seguridad contra la falsificación mediante la tecnología disponible en el momento;
   d) los datos de creación de la firma electrónica utilizados para la creación de firma electrónica puedan ser protegidos por el firmante legítimo de forma fiable frente a su utilización por otros.
2. Los dispositivos cualificados de creación de firmas electrónicas no alterarán los datos que deben firmarse ni impedirán que dichos datos se muestren al firmante antes de firmar.
3. La generación o la gestión de los datos de creación de la firma electrónica en nombre del firmante solo podrán correr a cargo de un prestador cualificado de servicios de confianza.

4. Sin perjuicio de la letra d) del punto 1, los prestadores cualificados de servicios de confianza que gestionen los datos de creación de firma electrónica en nombre del firmante podrán duplicar los datos de creación de firma únicamente con objeto de efectuar una copia de seguridad de los citados datos siempre que se cumplan los siguientes requisitos:
   a) la seguridad de los conjuntos de datos duplicados es del mismo nivel que para los conjuntos de datos originales;
   b) el número de conjuntos de datos duplicados no supera el mínimo necesario para garantizar la continuidad del servicio.

13.4.9 Anexo III. Requisitos de los certificados cualificados de sello electrónico

Los certificados cualificados de sello electrónico contendrán:

a) una indicación, al menos en un formato adecuado para el procesamiento automático, de que el certificado ha sido expedido como certificado cualificado de sello electrónico;
b) un conjunto de datos que represente inequívocamente al prestador cualificado de servicios de confianza que expide los certificados cualificados, incluyendo como mínimo el Estado miembro en el que dicho prestador está establecido, y
   - para personas jurídicas: el nombre y, cuando proceda, el número de registro según consten en los registros oficiales,
   - para personas físicas, el nombre de la persona;
c) al menos, el nombre del creador del sello y, cuando proceda, el número de registro, tal como se recojan en los registros oficiales;
d) los datos de validación del sello electrónico que correspondan a los datos de creación del sello electrónico;
e) los datos relativos al inicio y final del período de validez del certificado;
f) el código de identidad del certificado, que debe ser único para el prestador cualificado de servicios de confianza;
g) la firma electrónica avanzada o el sello electrónico avanzado del prestador de servicios de confianza expedidor;
h) el lugar en que está disponible gratuitamente el certificado que respalda la firma electrónica avanzada o el sello electrónico avanzado a que se hace referencia en la letra g);
i) la localización de los servicios que pueden utilizarse para consultar el estado de validez del certificado cualificado;
j) cuando los datos de creación del sello electrónico relacionados con los datos de validación del sello electrónico se encuentren en un dispositivo cualificado de creación de sellos electrónicos, una indicación adecuada de esto, al menos en una forma apta para el procesamiento automático.

13.4.10 Anexo IV. Requisitos de los certificados cualificados de sitios web

Los certificados cualificados de autenticación de sitios web contendrán:

a) una indicación, al menos en un formato adecuado para el procesamiento automático, de que el certificado ha sido expedido como certificado cualificado de autenticación de sitio web;
b) un conjunto de datos que represente inequívocamente al prestador cualificado de servicios de confianza que expide los certificados cualificados, incluyendo como mínimo el Estado miembro en el que dicho prestador está establecido, y

- para personas jurídicas: el nombre y, cuando proceda, el número de registro según consten en los registros oficiales,
- para personas físicas, el nombre de la persona;

c) para personas físicas: al menos el nombre de la persona a la que se expida el certificado, o un seudónimo; si se usara un seudónimo, se indicará claramente;
para personas jurídicas: al menos el nombre de la persona jurídica a la que se expida el certificado y, cuando proceda, el número de registro, tal como se recojan en los registros oficiales;

d) elementos de la dirección, incluida al menos la ciudad y el Estado, de la persona física o jurídica a quien se expida el certificado, y, cuando proceda, según figure en los registros oficiales;

e) el nombre o los nombres de dominio explotados por la persona física o jurídica a la que se expida el certificado;

f) los datos relativos al inicio y final del período de validez del certificado;

g) el código de identidad del certificado, que debe ser único para el prestador cualificado de servicios de confianza;

h) la firma electrónica avanzada o el sello electrónico avanzado del prestador de servicios de confianza expedidor;

i) el lugar en que está disponible gratuitamente el certificado que respalda la firma electrónica avanzada o el sello electrónico avanzado a que se hace referencia en la letra h);

j) la localización de los servicios que pueden utilizarse para consultar el estado de validez del certificado cualificado.

14 Tablas adicionales de contenido

14.1 Tabla