

28-10-2020

# Declaración de Prácticas de Servicios de Confianza (DPC)

Servicios y Certificados

Versión 4.2



European Agency  
of Digital Trust

EADTrust Policy Committee

EADTRUST EUROPEAN AGENCY OF DIGITAL TRUST



### **Nota sobre derechos de autor**

Este documento está protegido por derechos de autor que restringen su uso, copia, distribución y descompilación. No se puede reproducir ninguna parte de este documento de ninguna forma ni por ningún medio sin la autorización previa por escrito de European Agency of Digital Trust (EADTrust).

Todos los nombres de productos mencionados en este documento son marcas comerciales de sus respectivos propietarios.

### **Versiones del documento**

Esta publicación podría incluir inexactitudes técnicas o errores tipográficos.

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

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

## Certificación ISO 9001. ISO 27001 e ISO 20000-1

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

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

### Certificados

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



## Tabla de Contenidos

1	Control documental .....	13
2	Introducción .....	15
2.1	Tipo de Soporte y nivel de seguridad de los certificados .....	16
2.1.1	Tipo de Certificado: Persona Física / Persona Natural .....	16
2.1.2	Tipo de Certificado: Entidad legal / Persona Jurídica / Entidad sin personalidad Jurídica / Sello de Órgano .....	17
2.1.3	Tipo de Certificado: Autenticación de sitio web .....	18
2.1.4	Tipo de Certificado: Certificados PSD2 .....	19
2.2	Normativa de especificaciones y de evaluación .....	19
2.3	Resumen de la DPC .....	21
2.4	Nombre e identificación del documento .....	21
2.5	Participantes de la PKI .....	22
2.5.1	Autoridades de certificación .....	22
2.5.2	Autoridades de registro .....	28
2.5.3	Suscriptores .....	29
2.5.4	Partes que confían .....	31
2.6	Uso del certificado .....	31
2.6.1	Usos adecuados del certificado .....	31
2.6.2	Usos prohibidos del certificado .....	32
2.7	Administración de políticas .....	32
2.7.1	Organización que administra el documento .....	32
2.7.2	Contacto .....	32
2.7.3	Procedimiento de aprobación de las políticas de certificados .....	33
2.8	Definiciones y acrónimos .....	33
2.8.1	Acrónimos .....	38
2.8.2	Referencias .....	39
2.8.3	Convenciones .....	41
3	Responsabilidades de publicación y repositorio .....	41
3.1	Repositorios .....	41
3.2	Publicación de la información de certificación .....	41
3.3	Tiempo o frecuencia de publicación .....	43
4	Identificación y autenticación .....	43
4.1	Nombre .....	43
4.1.1	Tipos de nombres .....	43

4.1.2	Necesidad de que los nombres sean significativos .....	44
4.1.3	Anonimidad o pseudonimidad de los titulares de certificados.....	44
4.1.4	Tratamientos de datos excluidos en los certificados .....	45
4.1.5	Normas para interpretar diferentes formas de nombres .....	45
4.1.6	Singularidad de los nombres .....	45
4.2	Validación inicial de la identidad.....	45
4.2.1	Método para probar la posesión de la clave privada.....	45
4.2.2	Autenticación de la organización e identidad del dominio .....	46
4.2.3	Autenticación de la identidad individual.....	47
4.3	Identificación y autenticación para la solicitud de revocación .....	47
5	Requisitos operacionales del ciclo de vida del certificado.....	48
5.1	Solicitud del certificado .....	48
5.1.1	Quién puede enviar una solicitud del certificado .....	49
5.1.2	Proceso de inscripción y responsabilidades.....	49
5.2	Procedimiento de solicitud de certificado .....	50
5.2.1	Realización de funciones de identificación y autenticación.....	50
5.2.2	Aprobación o rechazo de solicitudes de certificado .....	51
5.2.3	Tiempo para procesar las solicitudes de certificado .....	52
5.3	Emisión del certificado .....	52
5.3.1	Acciones de la CA durante la emisión del certificado .....	52
5.3.2	Notificación al suscriptor sobre la emisión del certificado por la CA.....	53
5.4	Aceptación del certificado.....	54
5.4.1	Conducta que constituye la aceptación del certificado .....	54
5.4.2	Publicación del certificado por la CA.....	54
5.4.3	Notificación de la emisión del certificado por la CA a otras entidades.....	54
5.5	Par de claves y uso del certificado .....	54
5.5.1	Clave privada del titular y uso del certificado .....	54
5.5.2	Uso de la clave pública por la parte que confía y uso del certificado .....	56
5.6	Renovación del certificado .....	56
5.6.1	Circunstancias para la renovación del certificado.....	57
5.6.2	Quién puede solicitar la renovación.....	57
5.6.3	Procesamiento de solicitudes de renovación de certificados.....	57
5.6.4	Notificación de una nueva emisión de certificado al suscriptor .....	57
5.6.5	Conducta que constituye la aceptación de un certificado de renovación .....	57
5.6.6	Publicación del certificado de renovación por la CA.....	57

5.6.7	Notificación de la emisión del certificado por la CA a otras entidades.....	57
5.7	Modificación del certificado.....	57
5.7.1	Circunstancias para la modificación del certificado .....	57
5.7.2	Quién puede solicitar la modificación del certificado.....	57
5.7.3	Procesamiento de las solicitudes de modificación del certificado.....	57
5.7.4	Notificación de la emisión de un nuevo certificado al suscriptor .....	58
5.7.5	Conducta que constituye la aceptación de un certificado modificado .....	58
5.7.6	Publicación del certificado modificado por la CA.....	58
5.7.7	Notificación de la emisión del certificado por la CA a otras entidades.....	58
5.8	Revocación y suspensión del certificado.....	58
5.8.1	Circunstancias para la revocación .....	58
5.8.2	Quién puede solicitar la revocación .....	59
5.8.3	Procedimiento para la solicitud de revocación .....	59
5.8.4	Periodo de gracia para comprobar certificados revocados .....	60
5.8.5	Tiempo en el que una CA debe procesar la solicitud de revocación.....	61
5.8.6	Requisitos de comprobación de revocación para las partes que confían.....	61
5.8.7	Frecuencia de emisión de la CRL .....	61
5.8.8	Actualización de las CRLs.....	61
5.8.9	Servicios de estado de certificado.....	62
5.9	Recuperación de Certificados.....	62
6	Controles de instalaciones, de gestión y operacionales .....	62
6.1	Controles físicos .....	62
6.1.1	Localización y construcción de las instalaciones .....	63
6.1.2	Acceso físico .....	63
6.1.3	Electricidad y aire acondicionado.....	63
6.1.4	Exposición al agua .....	64
6.1.5	Prevención y protección contra incendios .....	64
6.1.6	Almacenamiento de soportes .....	64
6.1.7	Eliminación de residuos.....	64
6.1.8	Copia de seguridad externa.....	64
6.2	Controles de procedimiento.....	64
6.2.1	Puestos de confianza.....	64
6.2.2	Número de personas requeridas por tarea.....	65
6.2.3	Identificación y autenticación para cada puesto.....	65
6.2.4	Puestos que requieren separación de deberes.....	65

6.3	Controles de personal .....	65
6.3.1	Antecedentes, cualificaciones, experiencia y requisitos de aplicación.....	65
6.3.2	Procedimientos de comprobación de antecedentes penales.....	65
6.3.3	Requisitos de formación.....	66
6.3.4	Frecuencia y requisitos de cursos de perfeccionamiento .....	66
6.3.5	Rotación y secuencia laboral.....	66
6.3.6	Sanciones para acciones no autorizadas .....	66
6.3.7	Requisitos de contratación del personal.....	66
6.3.8	Documentación proporcionada al personal.....	67
6.4	Procedimientos de registro de auditoría.....	67
6.4.1	Tipos de eventos registrados.....	67
6.4.2	Frecuencia de procesamiento del registro.....	68
6.4.3	Periodo de retención del registro de auditoría .....	68
6.4.4	Procedimientos de copia de seguridad para registros de auditoría .....	68
6.4.5	Evaluaciones de vulnerabilidades .....	68
6.4.6	Cambio de clave .....	69
6.4.7	Terminación o cese de la CA o RA .....	69
6.4.8	Compromiso de claves y Plan de contingencias y de continuidad de negocio .....	70
7	Controles técnicos de seguridad .....	71
7.1	Generación e instalación del par de claves .....	71
7.1.1	Generación del par de claves .....	71
7.1.2	Entrega de la clave privada al suscriptor/titular de la clave .....	71
7.1.3	Entrega de la clave pública al emisor del certificado .....	72
7.1.4	Entrega de la clave pública de la CA a los terceros que confían .....	72
7.1.5	Tamaños de clave .....	72
7.1.6	Generación y comprobación de calidad de los parámetros de clave pública .....	72
7.1.7	Propósitos de uso de la clave (según el campo de uso clave X.509 v3).....	72
7.2	Protección de la clave privada en módulo criptográfico.....	73
7.2.1	Normas y controles del módulo criptográfico.....	73
7.2.2	Control multi-persona (n de m) de la clave privada.....	74
7.2.3	Escrow de clave privada de la CA .....	74
7.2.4	Copia de seguridad de la clave privada .....	74
7.2.5	Archivo de la clave privada.....	74
7.2.6	Transmisión de la clave privada a módulo criptográfico.....	74
7.2.7	Almacenamiento de la clave privada en un módulo criptográfico .....	74



7.2.8	Método de activación de una clave privada .....	75
7.2.9	Método de desactivación de una clave privada .....	75
7.2.10	Método de destrucción de una clave privada .....	75
7.2.11	Calificación del módulo criptográfico .....	75
7.3	Otros aspectos de la gestión del par de claves .....	75
7.3.1	Archivo de la clave pública .....	75
7.3.2	Periodos operacionales del certificado y del par de claves .....	75
7.4	Datos de activación .....	76
7.4.1	Generación e instalación de datos de activación .....	76
7.4.2	Protección de los datos de activación .....	76
7.4.3	Otros aspectos de los datos de activación .....	76
7.5	Controles de seguridad informática .....	76
7.5.1	Requisitos técnicos específicos de seguridad informática .....	76
7.5.2	Calificación de la seguridad informática .....	77
7.6	Controles técnicos del ciclo de vida .....	77
7.6.1	Controles de desarrollo del sistema .....	77
7.6.2	Controles de gestión de seguridad .....	78
7.6.3	Controles de seguridad del ciclo de vida .....	78
7.7	Controles de seguridad de red .....	78
7.8	Timestamping .....	78
8	Perfiles de certificado .....	78
8.1	Número de versión .....	79
8.2	Extensiones de certificado .....	80
8.3	Perfiles de Root y SubCA .....	80
8.3.1	Perfil de certificado de root CA para emisión de certificados cualificados .....	80
8.3.2	Perfil de certificado de root CA para emisión de certificados web y PSD2 .....	81
8.3.3	Perfil de certificado de root CA para emisión de certificados no cualificados .....	81
8.3.4	Perfil de certificado de subCA para emisión de certificados cualificados .....	82
8.3.5	Perfil de certificado de subCA para emisión de certificados web y PSD2 .....	83
8.3.6	Perfil de certificado de subCA para emisión de certificados no cualificados .....	84
8.4	Perfiles de certificados de Entidad Final .....	85
8.4.1	Perfil de certificado cualificado de persona jurídica para sello de tiempo cualificado .....	85
8.4.2	Perfil de certificado no cualificado de persona jurídica para sello de tiempo cualificado y no cualificado .....	86
8.4.3	Perfil de certificado cualificado de persona física .....	87

8.4.4	Perfil de certificado cualificado de representante de persona jurídica .....	88
8.4.5	Perfil de certificado cualificado de web “domain validated” (QWAC).....	89
8.4.6	Perfil de certificado cualificado de web “organization validated” (QWAC).....	90
8.4.7	Perfil de certificado cualificado de web “Extended Validation” (QWAC) .....	91
8.4.8	Perfil de certificado cualificado de empleado público con nivel de aseguramiento sustancial/medio .....	92
8.4.9	Perfil de certificado cualificado de empleado público con seudónimo con nivel de aseguramiento Alto (Firma) .....	94
8.4.10	Perfil de certificado cualificado de empleado público con seudónimo con nivel de aseguramiento Alto (Autenticación) .....	95
8.4.11	Perfil de certificado cualificado de web PSD2 (QWAC).....	97
8.4.12	Perfil de certificado cualificado de sello electrónico para persona jurídica .....	98
8.4.13	Perfil de certificado cualificado PSD2 de persona jurídica para sello electrónico .....	99
8.4.14	Perfil de certificado cualificado de sede electrónica administrativa “Organization Validated” (QWAC) con nivel de aseguramiento medio/sustancial .....	100
8.4.15	Perfil de certificado cualificado de sede electrónica administrativa “Extended Validation” (QWAC) con nivel de aseguramiento Alto.....	102
8.4.16	Perfil de certificado cualificado de sello de órgano Nivel Medio/Sustancial .....	104
8.4.17	Perfil de certificado cualificado de sello de órgano Nivel Alto.....	107
8.5	Perfil de CRL (Certificate Revocation List).....	111
8.6	Perfil de certificado para respondedor OCSP.....	111
9	Auditoría de cumplimiento y otras evaluaciones.....	112
10	Otros servicios electrónicos de confianza .....	113
10.1	Servicio de sello de tiempo .....	113
10.1.1	Fuentes de tiempo.....	113
10.1.2	Aspectos relevantes del servicio cualificado de sello de tiempo .....	114
10.2	Servicio de voto electrónico .....	115
10.3	Servicio de comprobación fehaciente de contenidos en páginas web. ....	115
10.4	Foro electrónico de accionistas.....	116
10.5	Generación y custodia de claves .....	116
10.6	Servicio de custodia digital “Cartulario” .....	116
10.7	Servicio de notificaciones certificadas “Noticeman” .....	117
10.8	Servicio de comprobación de validez de certificados .....	117
11	Otras cuestiones empresariales y legales .....	118
11.1	Tarifas .....	118
11.1.1	Tarifas de emisión de certificados.....	118

11.1.2	Tarifas de consulta OCSP .....	118
11.2	Consideraciones de protección de datos de carácter personal .....	118
11.2.1	Consentimiento para usar datos de carácter personal .....	119
11.2.2	Comunicación a terceros de datos de carácter personal .....	120
11.3	Garantías de la CA .....	120
11.4	Garantías del suscriptor .....	121
11.5	Responsabilidad contractual y extracontractual.....	122
11.5.1	Limitación de responsabilidad.....	122
11.5.2	Responsabilidades .....	123
11.5.3	Entidad de registro .....	124
11.5.4	Responsabilidades del titular de los certificados .....	124
11.6	Exención de responsabilidades de EADTrust .....	124
11.6.1	Perjuicios derivados del uso de servicios y certificados.....	125
11.6.2	Seguro de responsabilidad civil .....	125
11.7	Enmiendas y cambios .....	125
11.7.1	Procedimiento para realizar cambios.....	125
11.7.2	Mecanismo y periodo de modificación .....	125
11.7.3	Circunstancias bajo las cuales debe modificarse el OID.....	126
11.8	Quejas. Reclamaciones y jurisdicción.....	126
12	Referencias .....	128
12.1	Referencias normativas.....	128
12.2	Referencias informativas.....	129
13	Anexos .....	130
13.1	Sello de tiempo electrónico de confianza .....	130
13.2	Usos de OIDs por EADTRUST .....	130
13.2.1	Arcos 19126 y 501 .....	130
13.2.2	OID basados en el arco PEN 501 .....	131
13.2.3	OID definidos por normas técnicas .....	132
13.2.4	OID definidos en normas españolas de administración pública .....	134
13.3	Listado completo de los certificados vigentes de EADTrust (Root CA y Sub-CA).....	135
13.3.1	EADTrust ECC 256 Root CA For Qualified Web DV/OV Cert 2019.....	135
13.3.2	EADTrust ECC 256 Root CA For Qualified Web EV/PSD2 Cert 2019.....	135
13.3.3	EADTrust ECC 256 Root CA For Qualified Certificates 2019.....	136
13.3.4	EADTrust ECC 384 Root CA For Qualified Web DV/OV Cert 2019.....	136
13.3.5	EADTrust ECC 384 Root CA For Qualified Web EV/PSD2 Cert 2019.....	136

13.3.6	EADTrust ECC 384 Root CA For Qualified Certificates 2019.....	137
13.3.7	EADTrust RSA 2048 Root CA For Non-Qualified Certificates 2019.....	137
13.3.8	EADTrust RSA 2048 Root CA For Qualified Certificates 2019.....	138
13.3.9	EADTrust RSA 4096 Root CA For Qualified Web DV/OV Cert 2019.....	139
13.3.10	EADTrust RSA 4096 Root CA For Qualified Web EV/PSD2 Cert 2019.....	139
13.3.11	EADTrust RSA 4096 Root CA For Qualified Certificates 2019.....	140
13.3.12	EADTrust RSA 8192 Root CA For Qualified Web DV/OV Cert 2019.....	141
13.3.13	EADTrust RSA 8192 Root CA For Qualified Web EV/PSD2 Cert 2019.....	142
13.3.14	EADTrust RSA 8192 Root CA For Qualified Certificates 2019.....	143
13.3.15	EADTrust ECC 256 SubCA For Qualified Web DV/OV Cert 2019 .....	144
13.3.16	EADTrust ECC 256 SubCA For Qualified Web EV/PSD2 Cert 2019 .....	145
13.3.17	EADTrust ECC 256 SubCA For Qualified Certificates 2019 .....	145
13.3.18	EADTrust ECC 256 SubCA For Qualified Certificates 2019 .....	146
13.3.19	EADTrust ECC 384 SubCA For Qualified Web DV/OV Cert 2019 .....	147
13.3.20	EADTrust ECC 384 SubCA For Qualified Web EV/PSD2 Cert 2019 .....	147
13.3.21	EADTrust ECC 384 SubCA For Qualified Certificates 2019 .....	148
13.3.22	EADTrust ECC 384 SubCA For Qualified Certificates 2019 .....	148
13.3.23	EADTrust RSA 2048 SubCA For Qualified Certificates 2019 .....	149
13.3.24	EADTrust RSA 2048 SubCA For Qualified Certificates 2019 .....	150
13.3.25	EADTrust RSA 2048 SubCA For Non-Qualified Certificates 2019 .....	151
13.3.26	EADTrust RSA 4096 SubCA For Qualified Web DV/OV Cert 2019 .....	151
13.3.27	EADTrust RSA 4096 SubCA For Qualified Web EV/PSD2 Cert 2019 .....	152
13.3.28	EADTrust RSA 4096 SubCA For Qualified Certificates 2019 .....	153
13.3.29	EADTrust RSA 4096 SubCA For Qualified Certificates 2019 .....	154
13.3.30	EADTrust RSA 8192 SubCA For Qualified Web DV/OV Cert 2019 .....	155
13.3.31	EADTrust RSA 8192 SubCA For Qualified Web EV/PSD2 Cert 2019 .....	156
13.3.32	EADTrust RSA 8192 SubCA For Qualified Certificates 2019 .....	158
13.3.33	EADTrust RSA 8192 SubCA For Qualified Certificates 2019 .....	159
13.4	Declaración de cumplimiento del Reglamento UE 910/2014 (eIDAS). .....	160
13.4.1	Artículo 8. Niveles de Seguridad de los sistemas de Identificación electrónica .....	160
13.4.1	Artículo 13. Responsabilidad y carga de la prueba .....	161
13.4.2	Artículo 15. Accesibilidad para las personas con discapacidad.....	161
13.4.3	Artículo 19. Requisitos de seguridad aplicables a los prestadores de servicios de confianza 161	
13.4.4	Artículo 20. Supervisión de los prestadores cualificados de servicios de confianza.....	162

13.4.5	Artículo 21. Inicio de un servicio de confianza cualificado.....	163
13.4.6	Artículo 24. Requisitos para los prestadores cualificados de servicios de confianza.....	164
13.4.7	Anexo I. Requisitos de los certificados cualificados de firma electrónica.....	165
13.4.8	Anexo II. Requisitos de los dispositivos cualificados de creación de firma electrónica ...	166
13.4.9	Anexo III. Requisitos de los certificados cualificados de sello electrónico.....	166
13.4.10	Anexo IV. Requisitos de los certificados cualificados de sitios web.....	167

## 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. Corrección 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. Corrección de errores tipográficos.
2.4	05/05/2019	Versión 2.3	Adición de otros servicios no cualificados de comprobación fehaciente de contenidos de páginas web; generación y custodia de claves; custodia documental Cartulario, servicio de notificaciones fehacientes Noticeman y servicio de comprobación de validez de certificados.
2.5	01/07/2019	Versión 2.4	Revisión para incluir los certificados para PSD2 el resultado del Ballot SC 17 de CAB Forum relativo a organizationIdentifier
2.6	02/09/2019	Versión 2.5	Revisión para incluir mejoras identificadas en la auditoría eIDAS
2.7	03/10/2019	Versión 2.6	Revisión para incluir mejoras identificadas en la auditoría eIDAS
3.0	22/11/2019	Versión 2.7	Revisión para consolidar todas las mejoras identificadas en la auditoría interna eIDAS y las versiones internas de este documento.
4.0	23/04/2020	Versión 3.0	Revisión como parte del proceso de mejora continua e inclusión de la videoconferencia como medio de verificación y autenticación de identidad en la RA.
4.1	06 /05/2020	Versión 4.0	Revisión para incluir recomendaciones de auditores eIDAS
4.2	12/06/2020	Versión 4.1	Se introducen los oid's de test en el servicio de timestamping
5	28/10/2020	Version 4.2	Se introducen los perfiles de certificado de sede electrónica y sello de órgano alineados con el documento "Perfiles de Certificados Electrónicos 2.0" de la AAPP. Se ha eliminado la información histórica del arco de OID 19126.

TABLA2. DATOS DEL DOCUMENTO.

Propiedades del documento.	
Propietario	EADTrust European Agency of Digital Trust, S.L.
Fecha	28 de octubre de 2020
Distribución	Público
Nombre / Código	OPR-PG- v.5 - 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), 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 Asuntos Económicos y Transformación Digital (Secretaría de Estado de Digitalización e Inteligencia Artificial), 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<sup>1</sup>.

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 Infrastructure).

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 validación y revocación 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 validación y revocación de certificados cualificados de autenticación y firma electrónica de representantes **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.

<sup>1</sup> <https://www.un.org/sustainabledevelopment/es/objetivos-de-desarrollo-sostenible/>



- La creación, comprobación validación y revocación 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 validación y revocación 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. Si el titular del certificado es una administración pública el certificado cualificado de Persona Jurídica se denomina “Certificado de Sello de Órgano”..
- La creación, comprobación validación y revocación de certificados cualificados de autenticación y sello electrónico de **persona jurídica** sujeta a la normativa PSD2<sup>2</sup> 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 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 validación y revocación de certificados electrónicos orientados a **firmas de aplicación y código**,
- La creación, comprobación, validación y revocación de certificados para la autenticación de **sitios web**, en particular, los de sede electrónica de administración pública.
- La **conservación** de firmas electrónicas, sellos o certificados para estos servicios
- **Servicios de entrega electronica certificada.**

## 2.1 Tipo de Soporte y nivel de seguridad de los certificados

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

### 2.1.1 Tipo de Certificado: Persona Física / Persona Natural

Certificado	Standard Policy Identifier	EAD Trust Policy OID	Formato	Nivel de seguridad
<b>Individuo</b>	0.4.0.194112.1.0 (ETSI QCP-n)	1.3.6.1.4.1.501.2.1.1.0.41221	Software	Sustancial Presencial**
	0.4.0.194112.1.2 (ETSI QCP-n-QSCD)	1.3.6.1.4.1.501.2.1.1.1.41221	Dispositivo*	Alto Presencial**
	0.4.0.194112.1.0 (ETSI QCP-n)	1.3.6.1.4.1.501.2.1.1.3.41221	Software	Sustancial Distancia***
	0.4.0.194112.1.2 (ETSI QCP-n-QSCD)	1.3.6.1.4.1.501.2.1.1.4.41221	Dispositivo*	Alto Distancia***
<b>Representante</b>	0.4.0.194112.1.0 (ETSI QCP-n)	1.3.6.1.4.1.501.2.1.1.0.41222	Software	Sustancial Presencial**
	2.16.724.1.3.5.8 (OID MPR)			

<sup>2</sup>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

Certificado	Standard Policy Identifier	EAD Trust Policy OID	Formato	Nivel de seguridad
	0.4.0.194112.1.2 (ETSI QCP-n-QSCD) 2.16.724.1.3.5.8 (OID MPR)	1.3.6.1.4.1.501.2.1.1.1.41222	Dispositivo*	Alto Presencial**
	0.4.0.194112.1.0 (ETSI QCP-n) 2.16.724.1.3.5.8 (OID MPR)	1.3.6.1.4.1.501.2.1.1.3.41222	Software	Sustancial Distancia***
	0.4.0.194112.1.2 (ETSI QCP-n-QSCD) 2.16.724.1.3.5.8 (OID MPR)	1.3.6.1.4.1.501.2.1.1.4.41222	Dispositivo*	Alto Distancia***
<b>Empleado Público<sup>3</sup></b>	0.4.0.194112.1.0 (ETSI QCP-n) 2.16.724.1.3.5.7.2 (OID MPR)	1.3.6.1.4.1.501.2.1.1.0.41223	Software	Sustancial Presencial**
	0.4.0.194112.1.2 (ETSI QCP-n-QSCD) 2.16.724.1.3.5.7.2 (OID MPR)	1.3.6.1.4.1.501.2.1.1.1.41223	Dispositivo*	Alto Presencial**
	0.4.0.194112.1.0 (ETSI QCP-n) 2.16.724.1.3.5.7.2 (OID MPR)	1.3.6.1.4.1.501.2.1.1.3.41223	Software	Sustancial Distancia***
	0.4.0.194112.1.2 (ETSI QCP-n-QSCD) 2.16.724.1.3.5.7.2 (OID MPR)	1.3.6.1.4.1.501.2.1.1.4.41223	Dispositivo*	Alto Distancia***
<b>Empleado público (Seudónimo/ Firma)</b>	0.4.0.194112.1.2 (ETSI QCP-n-qscd) 2.16.724.1.3.5.4.1 (OID MPR)	1.3.6.1.4.1.501.2.1.1.1.41224	Dispositivo*	Alto Presencial**
	0.4.0.194112.1.2 (ETSI QCP-n-qscd) 2.16.724.1.3.5.4.1 (OID MPR)	1.3.6.1.4.1.501.2.1.1.4.41224	Dispositivo*	Alto Distancia***
<b>Empleado público (Seudónimo/ Autenticación)<sup>3</sup></b>	0.4.0.194112.1.2 (ETSI QCP-n-qscd) 2.16.724.1.3.5.4.1 (OID MPR)	1.3.6.1.4.1.501.2.1.1.1.41225	Dispositivo*	Alto Presencial**
	0.4.0.194112.1.2 (ETSI QCP-n-qscd) 2.16.724.1.3.5.4.1 (OID MPR)	1.3.6.1.4.1.501.2.1.1.4.41225	Dispositivo*	Alto Distancia***

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

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

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

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

Certificado	Standard Policy Identifier	EAD Trust Policy OID	Formato	Nivel de seguridad
<b>Sello corporativo (Timestamp)</b>	4.0.194112.1.1 (OID ETSI QCP-I) 0.4.0.194112.1.3 (OID ETSI QCP-I-QSCD)	1.3.6.1.4.1.501.2.1.1.0.421 1.3.6.1.4.1.501.2.1.1.1.421	Software Dispositivo*	Sustancial Alto
<b>Sello corporativo (Timestamp)</b>	No se indica Política asociada a RFC3161	1.3.6.1.4.1.501.2.1.1.0.3161	Software Dispositivo*	No cualificado Distancia***
<b>Sello Corporativo</b>	0.4.0.194112.1.1 (ETSI QCP-I)	1.3.6.1.4.1.501.2.1.1.0.41231	Software	Sustancial Presencial**

<sup>3</sup> 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 Público (LRJ) y al Reglamento (UE) 910/2014.

Certificado	Standard Policy Identifier	EAD Trust Policy OID	Formato	Nivel de seguridad
	0.4.0.194112.1.3 (ETSI QCP-I-QSCD)	1.3.6.1.4.1.501.2.1.1.1.41231	Dispositivo*	Alto
	0.4.0.194112.1.1 (ETSI QCP-I)	1.3.6.1.4.1.501.2.1.1.3.41231	Software	Presencial**
	0.4.0.194112.1.3 (ETSI QCP-I-QSCD)	1.3.6.1.4.1.501.2.1.1.4.41231	Software	Sustancial
	0.4.0.194112.1.3 (ETSI QCP-I-QSCD)	1.3.6.1.4.1.501.2.1.1.4.41231	Dispositivo*	Distancia***
<b>Sello Corporativo PSD2 (QSeal)</b>	0.4.0.194112.1.1 (ETSI QCP-I)	1.3.6.1.4.1.501.2.1.1.0.41232	Software	Alto
	0.4.0.194112.1.3 (ETSI QCP-I-QSCD)	1.3.6.1.4.1.501.2.1.1.1.41232	Dispositivo*	Distancia***
<b>Sello de órgano</b>	0.4.0.194112.1.1 (ETSI QCP-I)	1.3.6.1.4.1.501.2.1.1.0.41233	Software	Sustancial
	0.4.0.194112.1.3 (ETSI QCP-I-QSCD)	1.3.6.1.4.1.501.2.1.1.1.41233	Dispositivo*	Presencial**
	0.4.0.194112.1.3 (ETSI QCP-I-QSCD)	1.3.6.1.4.1.501.2.1.1.1.41233	Dispositivo*	Alto
	0.4.0.194112.1.3 (ETSI QCP-I-QSCD)	1.3.6.1.4.1.501.2.1.1.1.41233	Dispositivo*	Presencial**

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

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

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

### 2.1.3 Tipo de Certificado: Autenticación de sitio web

Certificado	Standard Policy Identifier	EAD Trust Policy OID	Formato	Nivel de seguridad
<b>SSL DV (QWAC)</b>	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
<b>SSL OV (QWAC)</b>	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
<b>SSL EV PSD2 (QWAC)</b>	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
				Distancia***
<b>SSL EV (QWAC)</b>	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
<b>SSL OVEH Sede (QWAC)</b>	0.4.0.194112.1.4 (ETSI QCP-w) 2.23.140.1.2.2 (CAB/FORUM OV)	1.3.6.1.4.1.501.2.1.1.0.41245	Software	Sustancial
				Distancia***
<b>SSL EVEH Sede (QWAC)</b>	0.4.0.194112.1.4 (ETSI QCP-w) 2.23.140.1.1 (CAB/FORUM EV)	1.3.6.1.4.1.501.2.1.1.0.41246	Software	Alto
				Distancia***

(\*) Los dispositivos habituales son HSM (Hardware Security Module), token seguro y tarjeta chip. Los tokens USB se consideran equivalentes al uso de tarjetas inteligentes considerando que incorporan la tarjeta y la chaqueta lectora en el mismo dispositivo.

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

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

### 2.1.4 Tipo de Certificado: Certificados PSD2

Certificado	Standard Policy Identifier	EAD Trust Policy OID	Formato	Nivel de seguridad
<b>Sello Corporativo PSD2 (QSeal)</b>	0.4.0.194112.1.1 (ETSI QCP-I)	1.3.6.1.4.1.501.2.1.1.0.41232	Software	Sustancial Distancia***
<b>PSD2 (QSeal)</b>	0.4.0.194112.1.3 (ETSI QCP-I-QSCD)	1.3.6.1.4.1.501.2.1.1.1.41232	Dispositivo*	Alto Distancia***
<b>SSL EV PSD2 (QWAC)</b>	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 Distancia***

(\*) Los dispositivos habituales son HSM (Hardware Security Module), token seguro y tarjeta chip. Los tokens USB se consideran equivalentes al uso de tarjetas inteligentes considerando que incorporan la tarjeta y la chaqueta lectora en el mismo dispositivo.

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

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

La denominación PSD2 hace referencia a a la Segunda Directiva de Pagos “Payment Services Directive (EU) 2015/2366”

## 2.2 Normativa de especificaciones y de evaluación

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
<b>Firma electrónica</b>	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
<b>Sellos electrónicos</b>	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
<b>Sello de tiempo electrónico</b>	EN 319 401 v2.2.1	EN 319 421 v1.1.1	EN 319 422 v1.1.1
<b>Autenticación de sitio web</b>	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
<b>PSD2</b>	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 319 412-4 v1.1.1 EN 319 412-5 v2.2.1 TS 119 495 V1.4.1

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 necesarios 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 los perfiles de los certificados son:

- Perfil de certificados 2.0<sup>4</sup> en el marco de la Leyes españolas 39/2015 y 40/2015. Incluye el perfil de certificado de representante, de empleado público, de sede electrónica y de sello de órgano. Se identifican con los (OID MPR)
- 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 solicitantes:

- inscripción en persona con personación ante una agente de RA
- inscripción a distancia, en las variantes siguientes:
  - videoconferencia (también descrita como telepresencia) o videograbación verificada.
  - Alternativamente *Firma Electrónica Cualificada* (aseguramiento sustancial o alto) En el caso en el que se utiliza una firma electrónica cualificada como parte de una solicitud de certificado.

El primer mecanismo de identificación a distancia nos permite video identificar a la persona física con documento físico. El segundo mecanismo nos permite identificar a la persona física que ya dispone de un

---

<sup>4</sup>[https://administracionelectronica.gob.es/pae/Home/dam/jcr:474ae40a-fe06-45fa-aa8f-113049e9c889/2016\\_Perfiles\\_de\\_certificados\\_1-ed.pdf](https://administracionelectronica.gob.es/pae/Home/dam/jcr:474ae40a-fe06-45fa-aa8f-113049e9c889/2016_Perfiles_de_certificados_1-ed.pdf)

certificado electrónico y usar el mismo nivel de aseguramiento que el certificado emitido para otras tipologías de certificados.

Además, EADTrust también proporciona servicios de confianza más allá del ámbito actual del Reglamento eIDAS, que, están igualmente sujetos a supervisión por el organismo supervisor:

- 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

### 2.3 Resumen de la DPC

---

Esta DPC describe:

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

Esta PKI (infraestructura de clave pública) abarca varios tipos de certificados (ver Sección 2.4] 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.

### 2.4 Nombre e identificación del documento

---

El nombre de este documento es "Declaración de Prácticas de Servicios Electrónicos 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](http://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 Electrónicos 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).

## 2.5 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.

### 2.5.1 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 los 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.

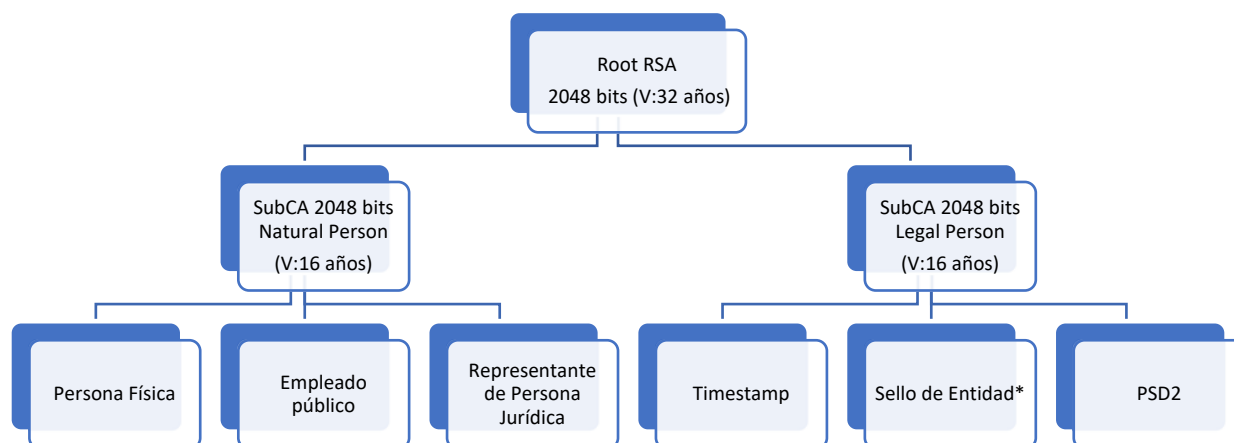
### Para certificados no cualificados

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

### Gráficamente:

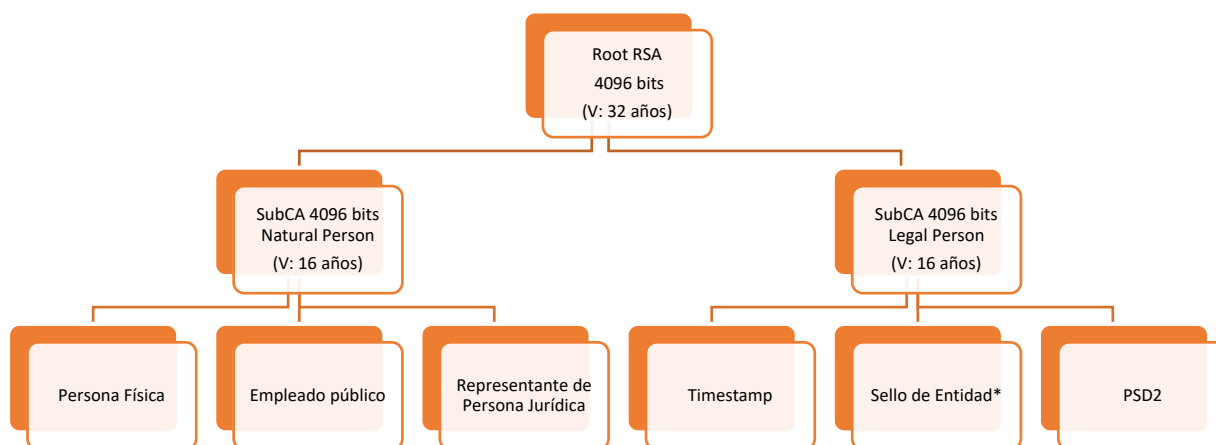
#### Root's Cualificadas para Certificados:

- Algoritmo RSA, tamaño 2048 bits



(\* ) Entre los sellos de entidad se incluyen los sellos de órgano con perfil propio.

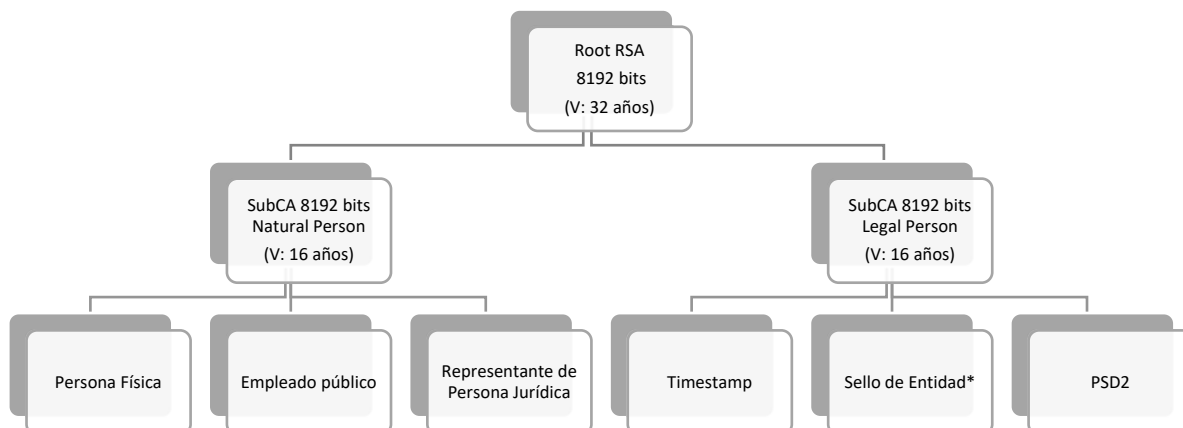
- Algoritmo RSA, tamaño 4096 bits



(\* ) Entre los sellos de entidad se incluyen los sellos de órgano con perfil propio.

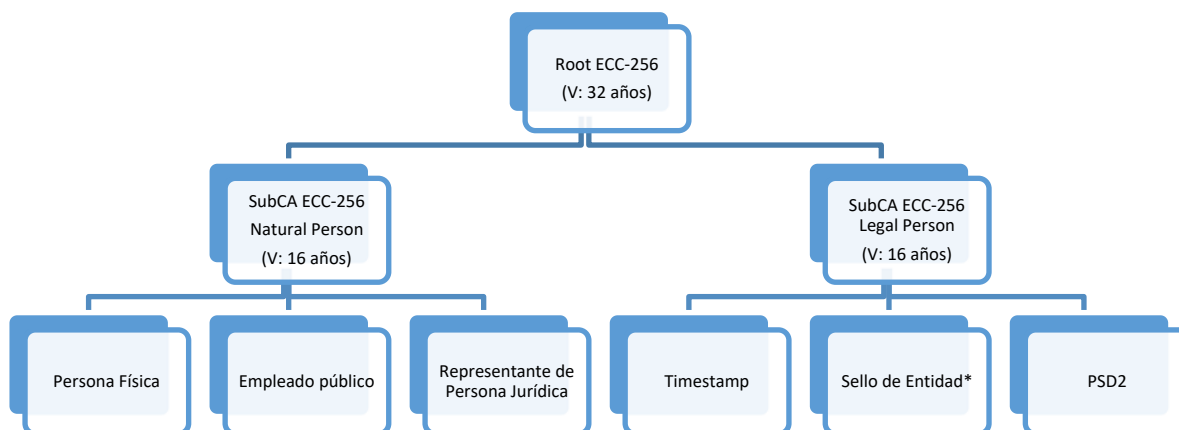


- Algoritmo RSA, tamaño 8192 bits



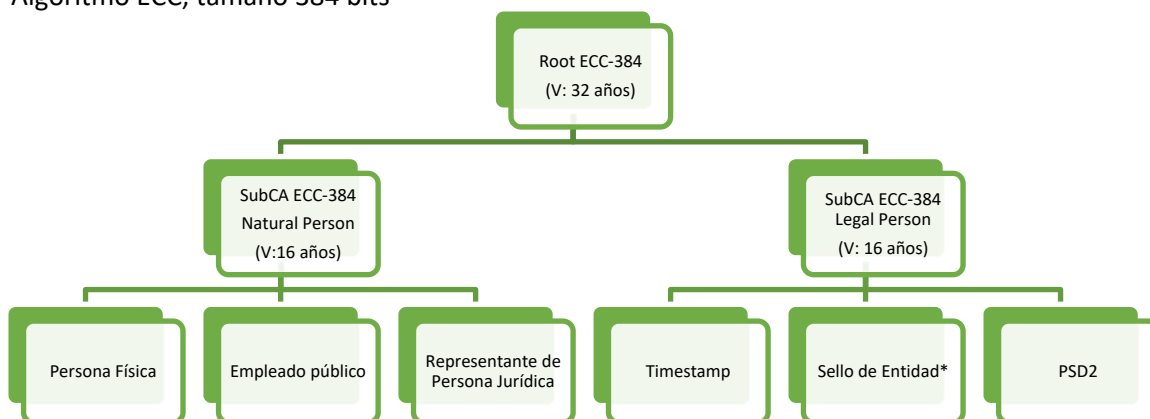
(\*) Entre los sellos de entidad se incluyen los sellos de órgano con perfil propio.

- Algoritmo ECC, tamaño 256 bits



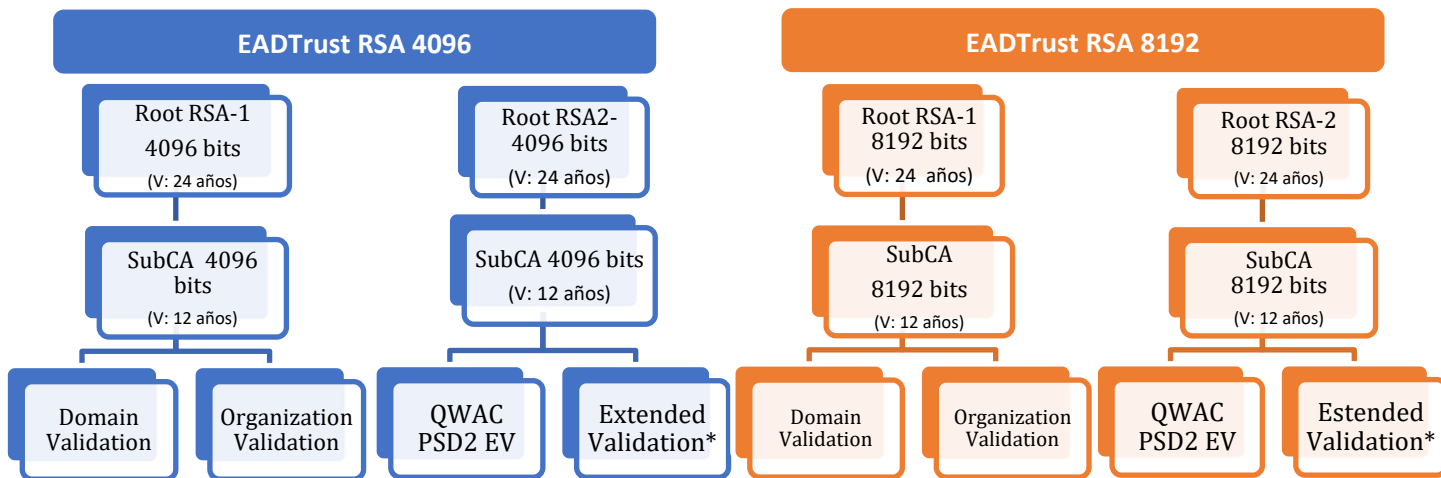
(\*) Entre los sellos de entidad se incluyen los sellos de órgano con perfil propio. (Pendiente de actualización de los perfiles de la administración pública).

- Algoritmo ECC, tamaño 384 bits

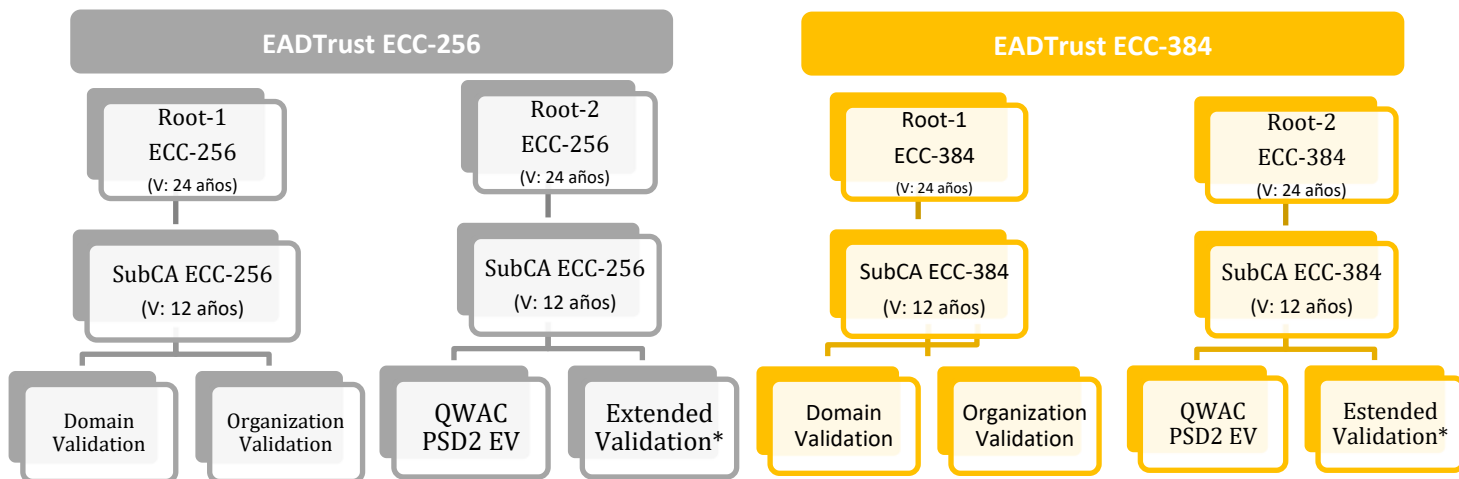


(\*) Entre los sellos de entidad se incluyen los sellos de órgano con perfil propio. (Pendiente de actualización de los perfiles de la administración pública).

- Root's Cualificadas para Web

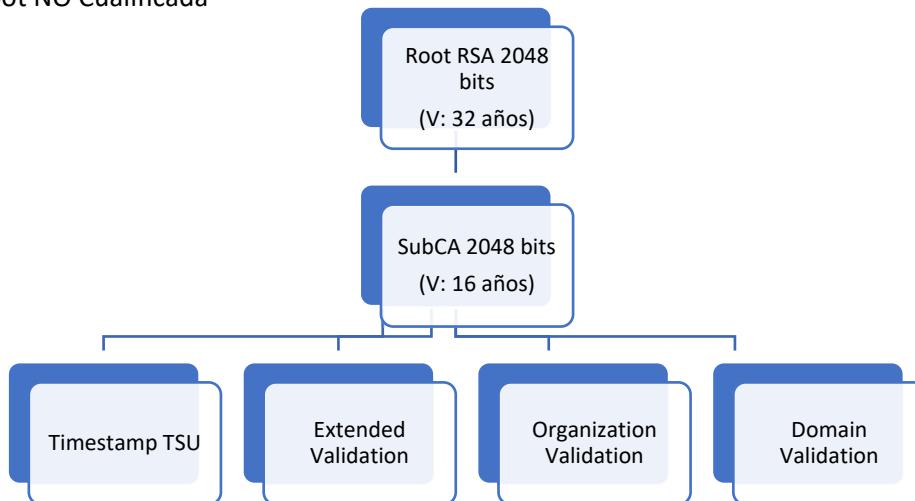


(\* ) Entre los certificados de extended validation se incluyen los de sede electrónica con perfil propio.



(\* ) Entre los certificados de extended validation se incluyen los de sede electrónica con perfil propio. (Pendiente de actualización de los perfiles de la administración pública, que todavía no conetemplan ECC).

- Root NO Cualificada



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

Pueden emitir Certificados bajo la jerarquía EADtrust las Autoridades de Certificación operadas por organizaciones externas cuyas Políticas o DPC (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 réúmen (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. Existe un perfil de certificado OCSP de uso opcional para servidores OCSP externos.

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
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

Denominación	Fingerprint SHA1	Tipo
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
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

Denominación	Fingerprint SHA1	Tipo
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

## 2.5.2 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 solicitantes: inscripción en persona con personación ante una agente de RA en persona y está previsto desarrollar la posibilidad de inscripción mediante videoconferencia (también descrita como mediante telepresencia) o videograbación (“digital onboarding”).

A la fecha de esta versión de la Declaración de Prácticas de Servicios de Confianza, sólo se están prestando las variantes del servicio que requieren personación ante la RA o mediante identificación remota por videoconferencia, en las variantes siguientes:

- videoconferencia (también descrita como telepresencia) o videograbación verificada.
- Alternativamente *Firma Electrónica Cualificada* (aseguramiento sustancial o alto) En el caso en el que se utiliza una firma electrónica cualificada como parte de una solicitud de certificado.

Para la videoconferencia<sup>5</sup> EADTrust cumple lo establecido en el Artículo 24. 1 apartado d) 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)

La Disposición Adicional Undécima. Medidas Provisionales para la expedición de certificados electrónicos cualificados del Real Decreto-ley 11/2020, de 31 de marzo, por el que se adoptan medidas urgentes complementarias en el ámbito social y económico para hacer frente al COVID-19.

Los procedimientos autorizados por el Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias de fecha 1 de marzo de 2016 respecto a la Ley 10/2010, de 28 de

<sup>5</sup> [http://www.sepblac.es/espanol/sujetos\\_obligados/autorizacion\\_identificacion\\_mediante\\_videoconferencia.pdf](http://www.sepblac.es/espanol/sujetos_obligados/autorizacion_identificacion_mediante_videoconferencia.pdf).

abril, de prevención de blanqueo de capitales y de la financiación del terrorismo y su Reglamento el Real Decreto 304/2014, de 5 de mayo, por el que se aprueba el Reglamento de la Ley 10/2010, de 28 de abril, de prevención de blanqueo de capitales y de la financiación del terrorismo.

Así como, lo previsto en la Directiva (UE) 2015/2366 (PSD2) que se utiliza en los servicios de iniciación de pagos como medio para proporcionar autenticación fuerte de los clientes.

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

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

- Identificación y autenticación de los 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 requisito en la política de certificado específica). También de forma que permita su instalación en el servidor web (para certificados definidos en la política de autenticación de servidor web). Si se comprueba por parte de la RA o un auditor que una solicitud de certificado (PKCS#10) se ha generado en un dispositivo criptográfica adecuado (QSCD) se emitirá el certificado en soporte de fichero para permitir su inserción en el QSCD
- 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 RAs, EADTrust ha considerado la posibilidad de que otras empresas puedan prestarle otros servicios técnicos, lo cual no afectará al usuario.

---

## 2.5.3 Suscriptores

---

### 2.5.3.1 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.

#### 2.5.3.2 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.
- Entidad que solicita certificados para sus empleados.

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.

#### 2.5.3.3 Suscriptores del certificado

---

El suscriptor de un certificado es la persona física o jurídica que contrata el servicio de expedición de certificados.

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.

#### 2.5.3.4 Propietarios de la clave

---

El propietario de la clave es una persona física o jurídica que tiene y puede utilizar bajo su exclusivo control la clave privada asociada al certificado. Las personas físicas generan firmas electrónicas y las personas jurídicas generan sellos electrónicos.

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.

---

#### 2.5.3.5 Representante del solicitante

---

Una persona jurídica o una entidad sin personalidad jurídica pueden actuar a través de su representante, persona física. El representante deberá acreditar su identidad y la representación por cualquier medio admitido en Derecho, en particular mediante poderes notariales o la acreditación de nombramientos que se publique en un diario oficial.

---

#### 2.5.4 Partes que confían

---

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

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

Deben comprobar por el campo AIA (Authority Information Access) de los certificados que pueden reconstruir la cadena de confianza desde el certificado de entidad final hasta la autoridad Raíz, 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<sup>6</sup> y por el organismo europeo que consolida las TSL nacionales<sup>7</sup>.

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/>

---

### 2.6 Uso del certificado

---

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

---

#### 2.6.1 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

---

<sup>6</sup><https://sede.minetur.gob.es/es-ES/datosabiertos/catalogo/lista-prestadores-tsl>

<sup>7</sup><https://ec.europa.eu/digital-single-market/en/eu-trusted-lists-trust-service-providers>



ofrecer soporte a la firma electrónica cualificada; en otras palabras, una firma electrónica avanzada respaldada en un certificado cualificado y basada en un dispositivo cualificado equivale a una firma manuscrita sin necesidad de satisfacer requisitos adicionales.

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

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

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.

---

## 2.6.2 Usos prohibidos del certificado

---

Los certificados deberán utilizarse para el fin específico para el que fueron creados.

Asimismo, los certificados sólo deben utilizarse de conformidad con la legislación aplicable.

Los Certificados no se deben usar en equipos de control destinados 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**)

---

## 2.7 Administración de políticas

---

---

### 2.7.1 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).

---

### 2.7.2 Contacto

---

Los servicios de EADTrust están disponibles principalmente a través de su página web: <http://eadtrust.eu> si bien puede utilizar otras URL por especialización o posicionamiento.

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

Nombre del PSC	European Agency of digital Trust, S. L.
Dirección	C/ Alba,15, 28043 Madrid - Spain
Dirección de email (en relación con las políticas)	policy@eadtrust.eu
Dirección de email para PSD2 (para uso de las <b>Autoridades Nacionales</b> )	<a href="mailto:CA-request@eadtrust.eu">CA-request@eadtrust.eu</a>
Teléfono	(+34) 902365612 / (+34) 917160555

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

<b>Código LEI</b>	9598009UB0L0E8XB2R35
<b>Código D-U-N-S</b>	461509305
<b>CIF</b>	B85626240

### 2.7.3 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](mailto:policy@eadtrust.eu).

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

## 2.8 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, subdivisión 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 revocación 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 que actúa en nombre y en representación de una persona jurídica o de una entidad sin personalidad jurídica.

**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 carácter 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<sup>8</sup> 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.

---

<sup>8</sup>Fully qualified domain name

**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.

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

**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 (Policy 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.

---

### 2.8.1 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 estándar 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.

Las definiciones y acrónimos relacionados con la emisión de certificados QSEAL y QWAC para entidades PSD2 se han incorporado a la política específica cuya lectura se recomienda.

---

## 2.8.2 Referencias

---

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

ETSI TS 119 495 - Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366

ETSI EN 319 403, 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<sup>9</sup>.

CAB Forum - Baseline Requirements<sup>10</sup>. Ultima version consultada: BR1.6.9<sup>11</sup>

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.

---

<sup>9</sup><http://www.webtrust.org/principles-and-criteria/item83172.aspx>

<sup>10</sup><https://cabforum.org/baseline-requirements/>

<sup>11</sup> <https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.6.9.pdf>

X.520, Recommendation ITU-T X.520 (10/2016) | ISO/IEC 9594-6:2017, Information technology - Open Systems Interconnection - The Directory: Selected attribute types

“Article 19 Incident reporting (Incident reporting framework for eIDAS Article 19”, ENISA, December 2016.<sup>12</sup>

“Guidelines on termination of qualified trust services”, ENISA, December 2017.<sup>13</sup>

Perfil de certificados 2.0 en el marco de la Leyes españolas 39/2015 y 40/2015.<sup>14</sup>

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

---

### 2.8.3 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](https://ocsp.eadtrust.eu)

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

- [crl.eadtrust.eu](https://crl.eadtrust.eu)

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

- [policy.eadtrust.eu](https://policy.eadtrust.eu)

---

### 3.2 Publicación de la información de certificación

---

La CA divulga públicamente sus Políticas de Certificados (habitualmente, formando parte de la 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

---

<sup>12</sup> <https://www.enisa.europa.eu/publications/article19-incident-reporting-framework>

<sup>13</sup> <https://www.enisa.europa.eu/publications/tsp-termination>

<sup>14</sup> [https://administracionelectronica.gob.es/pae\\_Home/dam/jcr:474ae40a-fe06-45fa-aa8f-113049e9c889/2016\\_Perfiles\\_de\\_certificados\\_1-ed.pdf](https://administracionelectronica.gob.es/pae_Home/dam/jcr:474ae40a-fe06-45fa-aa8f-113049e9c889/2016_Perfiles_de_certificados_1-ed.pdf)

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](https://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-evsedemedio-tst.eadtrust.eu/>
- <https://rsa-4096-evsedealto-tst.eadtrust.eu/>
- <https://rsa-4096-ov-tst.eadtrust.eu/>
- <https://rsa-4096-psd2-tst.eadtrust.eu/>
- <https://rsa-8192-dv-tst.eadtrust.eu/>
- <https://rsa-8192-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](https://policy.eadtrust.eu)

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

- **Persona física:** En certificados correspondientes a personas físicas la identificación del signatario estará formada por su nombre y apellidos, más su número de identificación de los admitidos en la norma EN 319 412-1.
- **Persona física - representante persona jurídica:** Determina la relación de representación legal o de apoderado general entre la persona física (titular del certificado/Sujeto/Firmante) y una persona jurídica o entidad sin personalidad jurídica.
- **Persona física - empleado público:** Es una persona física representante de un organismo público o un empleado público adscrito a un organismo público.
- **Persona Jurídica:** En certificados correspondientes a personas jurídicas, esta identificación se realizará por medio de su denominación o razón social, y su identificación fiscal u otro número de identificación de los admitidos en la norma EN 319 412-1. En los certificados orientados a PSD2 se considerarán los contenidos exigidos por su normativa. Los certificados de sello de órgano son un caso particular de este tipo de certificados y tienen un perfil propio.
- **Certificados para sitio web:** El dato principal es el nombre de dominio o dominios y también podrán utilizarse nombres que identifiquen subdominios mediante una referencia genérica (wildcard). Es necesario acreditar la relación con el dominio, con la organización o con datos extendidos de la organización (domain validation, organization validation, extended validation). En los certificados orientados a PSD2 se considerarán los contenidos exigidos por su normativa. Los certificados de sede electrónica son un caso particular de certificados “organization validated” (nivel de aseguramiento sustancia/medio) y “extended validation” (nivel de aseguramiento alto) y tienen un perfil propio.

---

#### 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.

---

#### 4.1.3 Anonimidad o pseudonimidad de los titulares de certificados

---

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

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

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

EADTrust se compromete a 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.

---

#### 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 **Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks**

- **X.509** - ISO/IEC 9594-8<sup>15</sup>
- X.520 -ISO/IEC 9594-6<sup>16</sup>

---

#### 4.1.6 Singularidad de los nombres

---

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

---

### 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 a instancias de 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 clave de descifrado, que podrán hacer uso de técnicas de comunicación de doble factor de

---

<sup>15</sup><http://www.itu.int/rec/T-REC-X.509-201610-I>

<sup>16</sup><http://www.itu.int/rec/T-REC-X.520-201610-I>

autenticación (por ejemplo, un mensaje de correo electrónico o un SMS) o un secreto compartido determinado en el momento de completar la solicitud de certificado.

Cuando se genera el par de claves por el solicitante:

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

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

---

#### 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 física empleado público, de sello de órgano, de persona jurídica, de sede electrónica 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). Cuando las entidades no sean sociedades se utilizarán de referencia los poderes notariales aportados y publicaciones de nombramientos en los boletines oficiales.

En el caso de certificados 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<sup>17</sup> 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 comprobar los datos de Dominios Completamente Cualificados dejando constancia de las acciones de comprobación en sus registros y logs.

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

---

<sup>17</sup>RFC 6844: DNS Certification Authority Authorization (CAA) Resource Record

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

Los registros identificados que se consultarán se señalan en el **Anexo II** de la política específica de emisión de certificados QSEAL y QWAC para entidad PSD2.

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

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

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

---

#### 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 mediante personación del titular del certificado.

---

### 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 empleado público, de Persona Jurídica o de sitio web.
- Por el titular, por compromiso de sus claves o por cualquier otra razón que lo requiera.
- Por la Autoridad Competente en los casos previstos en la normativa PSD2.

Para solicitar la revocación se requiere la personación física del solicitante de la revocación en una Entidad de Registro, o bien que el solicitante haga uso del servicio de revocación remota proporcionado al efecto, que podrá requerir la aportación de información específica para ello.

La Autoridad 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.



## 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

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

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

La cita con la RA se podrá llevar a cabo mediante personación en sus instalaciones, o mediante verificación de identidad a distancia (identificación remota) por videoconferencia verificada y alternativamente por *Firma Electrónica Cualificada* (aseguramiento sustancial o alto) En el caso en el que se utiliza una firma electrónica cualificada como parte de una solicitud de certificado; conforme a los requisitos definidos en la Política específica definida por EADTrust al efecto.

Actualmente se encuentran disponibles las siguientes variantes del servicio de verificación de identidad ante la RA:

Tipo de Servicio	Modalidad Presencial	Modalidad a distancia
Emisión de Certificado de persona física	X	X
Emisión de Certificado de persona jurídica	X	X
Emisión de Certificado de servidor web	-	X
Emisión de certificados QWAC y QSEAL entidad PSD2	-	X
Servicio de revocación de certificados	X	X

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

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

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

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

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

---

### 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 transmitidos 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 sello de órgano.
- las personas jurídicas propietarias de un sitio web o sede electrónica que requieran el uso de comunicaciones cifradas en servidores web o la sede de forma que se confirme la identidad del dominio.

---

### 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 y revocación 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, y revocación
- Notificar a EADTrust sobre las solicitudes de revocación de certificados con la debida diligencia y de una manera rápida y confiable.
- Permitir a EADTrust el acceso a sus archivos de procedimiento y registros de auditoría para desempeñar sus funciones y mantener la información necesaria.
- Informar a EADTrust sobre las solicitudes de emisión, revocación y cualquier otro aspecto relacionado con los certificados emitidos por EADTrust.
- Validar, con la debida diligencia, las circunstancias de revocación que puedan afectar a la validez del certificado.
- Cumplir con los procedimientos establecidos por EADTrust y con la legislación vigente en esta materia, en sus operaciones de gestión relacionadas con la emisión, 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 y se ha agendado la cita conforme indica el apartado 5.1 de esta DPC, el operador de la RA procederá a iniciar el proceso de identificación y validación de identidad declarada.

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

### 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)<sup>18</sup>. Para una referencia respecto a los términos utilizados, se recomienda acceder al Glosario<sup>19</sup>.

Características difractivas:

- Hologramas
- Identigramas
- Estructuras cinemáticas (Kinegramas)

Técnicas de personalización:

- Imagen láser cambiante
- Tipografía

Material:

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

Impresión de seguridad:

- Microimpresión

<sup>18</sup><http://www.consilium.europa.eu/prado/es/prado-start-page.html>

<sup>19</sup><https://www.consilium.europa.eu/prado/ES/prado-glossary/prado-glossary.pdf>

- 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.

Para los certificados de representante de persona jurídica, de empleado público, de sello de entidad, de sello de órgano, de sede electrónica y otros relacionados con personas jurídicas o entidades sin personalidad jurídica, la RA verificará, además: la vigencia del documento de representación o nombramiento aportado, la vigencia de la persona jurídica respecto de la cual el solicitante acredita vinculación.

En los certificados web (organization validation y extended validation) se realizan estas mismas comprobaciones. Para los certificados web (domain web) se verificará que el Solicitante tiene la propiedad del dominio.

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, la suficiencia de poderes de representación o del nombramiento como funcionario público.

Si la información no es correcta, la RA denegará la solicitud y se pondrá en contacto con el solicitante para explicar la razón. Si la información es correcta, la RA solicitará la aprobación de la emisión del certificado. Una vez verificado por el segundo nivel de aprobación, la CA de EADTrust emitirá el certificado correspondiente.

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

En el proceso de expedición de certificados web (extended validation, organization validation, domain validation, PSD2 QWAC, sede electrónica), además, se aplica un tercer control para la comprobación de que el dominio esté bajo el control exclusivo del solicitante del certificado.

---

### 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. Una vez hechas las comprobaciones de identidad del suscriptor, el tiempo de emisión del certificado 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 QSCD se entregan en un token criptográfico, en una tarjeta inteligente o en HSM. Cuando no es un certificado QSCD, EADTrust podrá entregar el certificado en un soporte de software USB, o enviarlo por email, adjuntando el certificado en un archivo .zip.

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

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

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

- La Autoridad de Registro autentica la validez de la documentación presentada por el solicitante, y audita la generación de la solicitud de certificado en HSM y la solicitud de certificado con formato PKCS#10. También podrá admitirse un informe de auditoría de un especialista certificando que la solicitud se ha generado en un HSM.
- Tras la autenticación, la Autoridad de Registro solicita el certificado de EADTrust, aportando el fichero en formato PKCS#10.

- Después de comprobar que la solicitud procede de una Autoridad de Registro autorizada, EADTrust emite el certificado según los procedimientos establecidos y lo envía a la Autoridad de Registro
- Después de que la Autoridad de Registro haya comprobado que la solicitud proviene de EADTrust, esta descarga el certificado y lo pone a disposición del solicitante que deberá insertarlos en el dispositivo criptográfico en el que se generó la solicitud.
- Si EADTrust decide no emitir el certificado (incluso cuando los procedimientos de autenticación sean correctos), se notificarán al solicitante los motivos de la decisión.

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

- Junto con el formulario de solicitud, el solicitante genera un par de claves en su propio ordenador, y hace llegar a EADTrust la solicitud de certificado con formato PKCS#10. 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 aunque no sea el dispositivo en el que se generó la solicitud.
- Por una vía diferente a la de la entrega del fichero PKCS#12 se hace llegar al solicitante la clave que permite el descifrado e instalación del fichero PKCS#12.
- EADTrust elimina la clave privada y el fichero PKCS#12 tras su remisión al solicitante.

---

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

---

Cuando el suscriptor coincide con el titular de las claves, EADTrust realiza la notificación de la emisión en el mismo acto de firma del contrato de condiciones generales y particulares del servicio. Además, se entrega el dispositivo que almacena el certificado.

Cuando el suscriptor del certificado no es la misma persona que el titular de las claves (en certificados de representante de persona jurídica, funcionario público y otros relacionados con persona jurídica); EADTrust firma el contrato y entrega el dispositivo al titular de las claves y; adicionalmente envía una notificación certificada de la entrega al suscriptor.

Los certificados web (domain validation) en lo que no se requiere personación ante la RA, se procederá a remitir el contrato de condiciones generales y particulares del servicio al solicitante y este lo devolverá firmado electrónicamente.

---

## 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 determinado de 10 días desde la entrega del certificado para asegurarse de que funciona correctamente y, si es necesario, devolverlo a la Autoridad de Registro.

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

---

### 5.4.1 Conducta que constituye la aceptación del certificado

---

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

---

### 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”<sup>20</sup>

---

## 5.5 Par de claves y uso del certificado

---

---

### 5.5.1 Clave privada del titular y uso del certificado

---

El titular que tiene la custodia de la clave privada:

- Garantizará el uso correcto y el mantenimiento de los soportes de almacenamiento del certificado.

---

<sup>20</sup><https://www.certificate-transparency.org/>

- Facilitará a EADTrust y a sus entidades de registro información completa y adecuada, conforme a los requerimientos de esta DPC (CPS) y de las políticas específicas, en especial en lo relativo al procedimiento de registro.
- Hará uso adecuado del certificado y, en particular, cumplirá con las limitaciones de uso del mismo.
- Salvaguardará diligentemente la clave privada (sea cual sea su soporte, e incluso si se trata de una copia de respaldo) y la clave o código PIN que permite su activación para evitar el uso no autorizado
- Notificará a EADTrust, y a cualquier otra persona que el titular piense que pueda confiar en el certificado, sin demora razonable, si se produce alguna de las siguientes situaciones:
  - La clave privada del titular se ha perdido, ha sido robada o se ha visto potencialmente comprometida.
  - El control sobre la clave privada del titular se ha perdido debido a que los datos de activación se han visto comprometidos (por ejemplo, código PIN del dispositivo criptográfico) o debido a otras razones.
  - Inexactitud o cambios en el contenido del certificado, según lo notificado o sospechado por el titular, solicitando la revocación del certificado cuando tales cambios constituyan una causa de revocación.
- Dejará de usar la clave privada al final del período de validez del certificado.
- Se abstendrá de supervisar, interferir o realizar un proceso de ingeniería inversa de la implementación técnica de los servicios de certificación sin la previa aprobación por escrito de la Autoridad de Certificación.
- Se abstendrá de comprometer intencionadamente la seguridad de los servicios de certificación.
- Se abstendrá de utilizar las claves privadas correspondientes a las claves públicas incluidas en los certificados con el fin de firmar un certificado como si desempeñara la función de una Autoridad de Certificación.
- Los titulares de certificados cualificados que generen firmas digitales utilizando la clave privada correspondiente a la clave pública incluida en el certificado deben asumir que tales firmas electrónicas son equivalentes a firmas manuscritas, siempre que se utilice un dispositivo criptográfico (dispositivo cualificado de creación de firma electrónica), según las disposiciones del Reglamento eIDAS.
- Los titulares de certificados cualificados que generen sellos digitales utilizando la clave privada correspondiente a la clave pública incluida en el certificado deben asumir que tales sellos digitales gozan de presunción de integridad de los datos y de la corrección del origen de los datos a los que el sello electrónico cualificado esté vinculado, siempre que se utilice un dispositivo criptográfico (dispositivo cualificado de creación de sello electrónico), según las disposiciones del Reglamento eIDAS.
- Abonar las tarifas por los servicios de certificación y sellado de tiempo solicitados en los términos y condiciones previstos por la CA, cuando el titular coincide con el suscriptor
- Autorizar a la CA a que, a través de la RA, utilice los datos personales aportados por el titular para validar, comprobar y autenticar la identidad declarada por este.
- Solicitar la revocación del Certificado cuando se cumpla alguno de los supuestos previstos en las políticas y prácticas específicas y en la legislación vigente para los diferentes status del ciclo de vida de los certificados
- Comprender y aceptar los términos y condiciones de uso del certificado, y cualquier modificación que se realice a estos
- No comprometer intencionadamente 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, o revocación de los certificados emitidos, utilizando la información sobre el estado del certificado, disponible en el servicio OCSP.
- Comprobar todos los certificados en la jerarquía de certificados antes de confiar en una firma digital o en cualquiera de los certificados de la jerarquía. En relación con los certificados cualificados, comprobar que la autoridad de certificación raíz de EADTrust en cuya jerarquía se encuentra el certificado, está incluida en la lista TSL correspondiente.<sup>21</sup>
- 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

---

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

---

<sup>21</sup> 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>

---

#### 5.6.1 Circunstancias para la renovación del certificado

---

No Aplica.

---

#### 5.6.2 Quién puede solicitar la renovación

---

No Aplica.

---

#### 5.6.3 Procesamiento de solicitudes de renovación de certificados

---

No Aplica.

---

#### 5.6.4 Notificación de una nueva emisión de certificado al suscriptor

---

No Aplica.

---

#### 5.6.5 Conducta que constituye la aceptación de un certificado de renovación

---

No Aplica.

---

#### 5.6.6 Publicación del certificado de renovación por la CA

---

No Aplica.

---

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

---

No Aplica.

---

### 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

---

No Aplica.

---

#### 5.7.2 Quién puede solicitar la modificación del certificado

---

No Aplica.

---

#### 5.7.3 Procesamiento de las solicitudes de modificación del certificado

---

No Aplica.

---

#### 5.7.4 Notificación de la emisión de un nuevo certificado al suscriptor

---

No Aplica.

---

#### 5.7.5 Conducta que constituye la aceptación de un certificado modificado

---

No Aplica.

---

#### 5.7.6 Publicación del certificado modificado por la CA

---

No Aplica.

---

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

---

No Aplica.

---

### 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 de certificados. 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 jurídica.
- Los datos de creación de firma del firmante o del prestador de servicios de certificación han sido comprometidos o si el firmante o un tercero han utilizado los datos de forma incorrecta.
- Cuando se haya emitido una orden legal o administrativa a tal efecto.
- Que una Autoridad Competente indique la necesidad de revocar un certificado PSD2.
- La muerte del firmante o la extinción de la persona jurídica titular del certificado de sello, la incapacidad total o parcial imprevisible del firmante o de la persona jurídica representada por el firmante, la terminación de la representación, la disolución de la persona jurídica representada, el cambio en las circunstancias de la custodia o uso de los datos de creación de firma o de sello incluidos en los certificados expedidos a una persona jurídica.

- El caso de que EADTrust termine su actividad, excepto en los casos en que el firmante haya dado su consentimiento para que los servicios de gestión de certificados electrónicos sean transferidos a otro prestador de servicios de certificación.
- Cambio en los datos suministrados para obtener el certificado o modificación de las circunstancias verificadas para la emisión del certificado.
- Que haya perdido la clave privada asociada al certificado, que haya sido robada o no sea útil debido a daños en el soporte del certificado, o cuando se haya cambiado a otro soporte no previsto en la política de certificación.
- Una de las partes incumple sus obligaciones, como, por ejemplo, el pago.
- Se detecta un error en el procedimiento de emisión del certificado, ya sea porque uno de los requisitos previos no se ha cumplido o debido a problemas técnicos durante el proceso de emisión del certificado.
- Existe una amenaza potencial para la seguridad de los sistemas y para la fiabilidad de los certificados emitidos por EADTrust por razones distintas del compromiso de los datos de creación de firmas.
- Fallo técnico en la emisión o distribución de certificados o de la documentación asociada.
- Si EADTrust recibe una solicitud para la emisión del certificado y ya existe un certificado válido de la misma clase y unicidad, el certificado válido será revocado a petición del solicitante.

---

### 5.8.2 Quién puede solicitar la revocación

---

La revocación de un certificado podrá solicitarse por

- El titular del certificado.
- El Solicitante o Suscriptor cuando no coincide con el Titular.
- La RA o la CA.
- En el caso de los certificados para PSD2, los organismos supervisores (Autoridades Competentes).

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

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

---

### 5.8.3 Procedimiento para la solicitud de revocación

---

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

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

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

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

- En línea, en la dirección [www.eadtrust.eu](http://www.eadtrust.eu) o por correo electrónico con solicitud firmada electrónicamente utilizando un certificado cualificado. También será válida la solicitud de revocación que referencie un código designado para ese uso.
- 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 organismos supervisores (Autoridades Competentes) pueden solicitar la revocación mediante el uso de una dirección de e-mail designada para ello, sin perjuicio de las comprobaciones adicionales que realice EADTrust para verificar la legitimidad de la solicitud. La demora máxima entre la recepción de una solicitud de revocación de certificado y la decisión de cambiar su información de estado para que esté disponible para todas las partes que confían es siempre menor de 24 horas, y usualmente menor de 10 minutos.

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

#### 5.8.4 Período de gracia para comprobar certificados revocados

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

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

En la relación de firmas electrónicas, este período podrá ser, desde el momento en que se realiza la firma o el sellado de tiempo, como mínimo, el tiempo máximo permitido para el refresco completo de las CRLs (CertificateRevocationLists) o el tiempo máximo de actualización del estado del certificado en el servicio OCSP (Online Certificate Status Protocol). Esta definición tendrá en cuenta también la posibilidad de que estos tiempos varíen según el Prestador de Servicios de Certificación. El período de gracia recomendado es de 24 horas.

En caso de que sea de aplicación una política de firma concreta, es responsabilidad del tercero que confía en los certificados expedidos por EADTrust la comprobación de que la Política de Firma aplicable es compatible con la Política de Certificación de EADTrust. Tres de las posibles políticas a aplicar, en España, son la de factura electrónica<sup>22</sup>, la de la Administración General del Estado<sup>23</sup> y la de la Administración de Justicia<sup>24</sup>.

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

<sup>22</sup> <https://www.facturae.gob.es/formato/Paginas/politicas-firma-electronica.aspx>

<sup>23</sup> <https://www.boe.es/boe/dias/2016/11/03/pdfs/BOE-A-2016-10146.pdf>

<sup>24</sup> [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](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)

---

### 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, generándose una nueva CRL y en la base de datos de la plataforma de gestión que consulta 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 o la lista de revocación de certificados (CRL).

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

---

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

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

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

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

---

### 5.8.8 Actualización de las CRLs

---

El tiempo que transcurre tras la finalización de la comunicación que da noticias de las razones de la revocación, hasta que la información está disponible en la base de datos desde la que se ofrece el servicio OCSP y desde la que se genera la lista CRL se establece en un máximo de 10 minutos.

---

### 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)<sup>25</sup>.

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.

---

<sup>25</sup> 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<sup>26</sup> y OVH<sup>27</sup>

---

### 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 posible circular en el edificio sin estar identificado y acompañado por un empleado.
  - El personal que no está en la lista de acceso de EADTrust y que puede estar trabajando en el sitio está debidamente supervisado.
- El acceso a las instalaciones que acogen los servidores implica la videograbación de la actividad y requiere identificación biométrica y control dual de los accesos.
- Se lleva a cabo el registro de los accesos a las instalaciones que acogen los servidores. Se cuenta con medidas adicionales de limitación de accesos al edificio en las oficinas de EADTrust.
- Las RAs cumplen con los criterios de seguridad necesarios definidos en el documento de securitización del sitio de registro.

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

---

### 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.

---

<sup>26</sup> Aspectos de cumplimiento de Amazon: <https://aws.amazon.com/es/compliance/>

<sup>27</sup> 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. Sus instalaciones se encuentran en un emplazamiento geográficamente elevado.

---

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

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

---

### 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)<sup>28</sup> 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.

---

<sup>28</sup><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.
- Procedimiento de gestión de incidencias

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

---

### 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 procedimiento de gestión de incidentes de seguridad diseñado tomando en consideración las directrices técnicas definidas por la European Union Agency For Network And Information Security ENISA en el documento; *“Article 19 Incident reporting. (Incident reporting framework for eIDAS Article 19).”*<sup>29</sup>

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

---

### 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.

---

<sup>29</sup> <https://www.enisa.europa.eu/publications/article19-incident-reporting-framework>

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 CA a través de la red.
- Intentos de accesos no autorizados al sistema de archivos.
- Acceso físico a los registros de auditoría.
- Cambios en la configuración y mantenimiento del sistema.
- Registros de las aplicaciones de la CA.
- Encendido y apagado de la aplicación de la CA.
- Cambios en los detalles de la CA y/o sus claves.
- Cambios en la creación de políticas de certificados.
- Generación de claves propias.
- Registros de peticiones de generación y revocación de certificados.
- Registros de generación y revocación de certificados.
- Eventos relacionados con el ciclo de vida del módulo criptográfico, como recepción, preparación, uso y desinstalación de este.

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

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

---

#### 6.4.2 Frecuencia de procesamiento del registro

---

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

---

#### 6.4.3 Periodo de retención del registro de auditoría

---

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

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

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

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

---

#### 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.

---

#### 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

---

No hay previsión específica sobre cambio de claves.

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

---

#### 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. Al respecto EADTrust ha tomado en consideración las directrices técnicas definidas por la European Union Agency for Network and Information Security (ENISA), en particular las siguientes: *“Guidelines on Termination of Qualified Trust Services”*<sup>30</sup>

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 supervisión 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

---

<sup>30</sup> <https://www.enisa.europa.eu/publications/tsp-termination>

dejará sin efecto. La notificación a dicho organismo se realizará con al menos dos (2) meses de antelación, en documento firmado manuscrito o electrónicamente. Además, se remitirá a dicho organismo la información relativa a los certificados cuya vigencia haya sido extinguida para que éste se haga cargo de su custodia a los efectos pertinentes. La última CRL generada contendrá los certificados revocados y no caducados. Siempre que sea posible, se gestionarán las CRLs en el proceso de terminación de manera que no queden certificados vigentes al generar la última CRL.

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 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.

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 RAs 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 Servicios de Confianza Digital en sus jerarquías de certificación emplean software y dispositivos específicos para la protección de claves privadas.

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

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

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

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

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

#### 7.1.2 Entrega de la clave privada al suscriptor/titular de la clave

---

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

- Certificados emitidos en un token criptográfico o en una tarjeta criptográfica: las claves privadas para la autenticación y la firma se entregan en un dispositivo criptográfico.



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

---

### 7.1.3 Entrega de la clave pública al emisor del certificado

---

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

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

---

### 7.1.4 Entrega de la clave pública de la CA a los terceros que confían

---

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

---

### 7.1.5 Tamaños de clave

---

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

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

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

---

### 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)<sup>31</sup>

---

### 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.

---

<sup>31</sup><https://github.com/crocs-muni/roca>

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

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

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

## 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 Common Criteria EAL4+ o posteriores.

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

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

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

EADTrust monitoriza que los dispositivos utilizados mantengan la certificación. Entre otras referencias se utiliza la siguiente: “Compilation of: Member States' notifications on: Designated Bodies under Article 30(2) and 39(2) of Regulation 910/2014 and Certified Qualified Signature Creation Devices under Article 31(1)-(2), and Certified Qualified Seal Creation Devices under Article 39(3) of Regulation 910/2014, and information from Member States on: Secure Signature Creation Devices benefiting from the transitional measure set in article 51(1) of Regulation 910/2014”.<sup>32</sup>

<sup>32</sup> <https://ec.europa.eu/futurium/en/system/files/ged/eidas-art.31-list-2019-08-01.pdf>

---

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

---

### 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 al módulo criptográfico de la CAs subordinadas 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 certificados una vez caducada.

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

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

---

### 7.2.6 Transmisión de la clave privada a módulo criptográfico

---

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

---

### 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.<sup>33</sup>

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

---

<sup>33</sup><https://cabforum.org/baseline-requirements-documents/>

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 al menos control dual para el acceso y gestión de los dispositivos criptográficos (tokens criptográficos o tarjetas).

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

---

#### 7.2.9 Método de desactivación de una clave privada

---

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

---

#### 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.

---

#### 7.2.11 Calificación del módulo criptográfico

---

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

---

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

---

### 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 de activación (PIN o PUK) junto al dispositivo criptográfico o compartirlo con otras personas.
- Cambiar el PIN antes de usarlo.

---

### 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 cifrados 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 RAs y CAs.
- El servicio de consulta de revocaciones está disponible 24 horas al día, 7 días a la semana.
- Control de acceso
  - Las identificaciones de usuario son únicas y se utilizan de tal manera que sus acciones quedan registradas y les son atribuibles.
  - Los usos permitidos se asignan con el fin de proporcionar a los usuarios el perfil más restrictivo que permita hacer su trabajo.
  - Los identificadores de usuario dejan de ser válidos cuando los usuarios cambian de trabajo o salen de la organización.
  - 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

---

Existe un repositorio para el control de versiones de software.

Los sistemas de producción se revisan periódicamente para comprobar que las actualizaciones de seguridad publicadas por los desarrolladores están correctamente aplicadas. En particular: sistema operativo, bases de datos y aplicaciones críticas.

Los desarrollos propios se verifican antes de su paso a producción.

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

- Existen prácticas de coordinación para actualizar las bibliotecas del software (incluidos los parches) en la producción. La autorización se concede sólo después de asegurarse de que funciona correctamente.
- El sistema de pruebas se mantiene separado del sistema de producción para asegurarse de que funciona correctamente antes de pasar a producción.
- Existe un registro de dependencias para garantizar que una actualización no inhabilita una función de seguridad requerida de modo que se pueda controlar el nivel de versión adecuado.
- Se conservan las versiones anteriores del software propio.
- El software adquirido se mantiene al nivel soportado por el proveedor, salvo que existan dependencias identificadas que requieran una versión anterior.

---

### 7.6.2 Controles de gestión de seguridad

---

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

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

---

### 7.6.3 Controles de seguridad del ciclo de vida

---

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

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

---

## 7.7 Controles de seguridad de red

---

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

Los firewalls se revisan cuando sea preciso actualizar las reglas de filtrado.

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

Los usuarios 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.<sup>34</sup>

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.
- 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.

<sup>34</sup> [https://administracionelectronica.gob.es/pae\\_Home/dam/jcr:474ae40a-fe06-45fa-aa8f-113049e9c889/2016\\_Perfiles\\_de\\_certificados\\_1-ed.pdf](https://administracionelectronica.gob.es/pae_Home/dam/jcr:474ae40a-fe06-45fa-aa8f-113049e9c889/2016_Perfiles_de_certificados_1-ed.pdf)



## 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
<b>version</b>		3
<b>serialNumber</b>		Número positivo único
<b>signature</b>		Sha256WithRSAEncryption o sha512WithRSAEncryption o ecdsa-with-SHA256 o ecdsa-with-SHA384
<b>issuer</b>		Igual que el campo Subject
<b>validity</b>		32 años
<b>subject</b>		
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
<b>subjectPublicKeyInfo</b>		RSA 2048, 4096 ó 8192 bits ECDSA 256 bits (prime256v1) ó 384 bits (secpr384r1)
<b>Extensiones</b>		
<b>subjectKeyIdentifier</b>		Derivada del resultado de aplicar el hash a la clave pública del sujeto
<b>subjectAltName</b>		rfc822 Name ca@eadtrust.eu URI: <a href="http://www.eadtrust.eu">http://www.eadtrust.eu</a> URI: <a href="http://ca.eadtrust.eu">http://ca.eadtrust.eu</a> URI: <a href="http://policy.eadtrust.eu">http://policy.eadtrust.eu</a>
<b>basicConstraint</b>	<b>Crítica</b>	CA:true
<b>keyUsage</b>	<b>Crítica</b>	Certificate signing, CRL signing

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

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

### 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
<b>subject</b>		
Country		País (ISO 3166-1 alpha 2 code)
Organization Name		Nombre completo de la organización
Common Name		Nombre de la CA
subjectPublicKeyInfo		RSA 4096 ó 8192 bits ECDSA 256 bits (prime256v1) ó 384 bits (secpr384r1)
<b>Extensiones</b>		
subjectKeyIdentifier		Derivada del resultado de aplicar el hash a la clave pública del sujeto
basicConstraint	<b>Crítica</b>	CA:true
keyUsage	<b>Crítica</b>	Certificate signing, CRL signing

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

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

### 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
<b>subject</b>		
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
<b>Extensiones</b>		
subjectKeyIdentifier		Derivada del resultado de aplicar el hash a la clave pública del sujeto
subjectAltName		rfc822 Name ca@eadtrust.eu

		URI: <a href="http://www.eadtrust.eu">http://www.eadtrust.eu</a> URI: <a href="http://ca.eadtrust.eu">http://ca.eadtrust.eu</a> URI: <a href="http://policy.eadtrust.eu">http://policy.eadtrust.eu</a>
<b>basicConstraint</b>	<b>Crítica</b>	CA:true
<b>keyUsage</b>	<b>Crítica</b>	Certificate signing, CRL signing

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

- RSA 2048 y SHA 256

### 8.3.4 Perfil de certificado de subCA para emisión de certificados cualificados

Campo	Crítico	Contenido
<b>version</b>		3
<b>serialNumber</b>		Número positivo único
<b>signature</b>		Sha256WithRSAEncryption o sha512WithRSAEncryption o ecdsa-with-SHA256 o ecdsa-with-SHA384
<b>issuer</b>		Igual al campo Subject del certificado de la CA emisora
<b>validity</b>		16 años
<b>subject</b>		
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)
<b>subjectPublicKeyInfo</b>		RSA 2048, 4096 ó 8192 bits ECDSA 256 bits (prime256v1) ó 384 bits (secpr384r1)
<b>Extensiones</b>		
<b>authorityKeyIdentifier</b>		Derivada del resultado de aplicar el hash a la Clave pública de la AC emisora
<b>basicConstraints</b>	<b>Crítica</b>	CA=true, pathlen=0
<b>subjectKeyIdentifier</b>		Derivada del resultado de aplicar el hash a la clave pública del sujeto
<b>issuerAltName</b>		Igual al campo Subject Alternative Names de la CA Emisora
<b>subjectAltName</b>		rfc822 Name ca@eadtrust.eu URI: <a href="http://www.eadtrust.eu">http://www.eadtrust.eu</a> URI: <a href="http://ca.eadtrust.eu">http://ca.eadtrust.eu</a> URI: <a href="http://policy.eadtrust.eu">http://policy.eadtrust.eu</a>
<b>certificatePolicies</b>		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.1.401
cpsURI		<a href="http://policy.eadtrust.eu/">http://policy.eadtrust.eu/</a>
userNotice		Subordinate Certificate Authority. European Agency of Digital Trust, S.L.
policyIdentifier		2.5.29.32.0 (AnyPolicy)
<b>cRLDistributionPoints</b>		
distributionPoint		<a href="http://crl.eadtrust.eu/eadtrust-root-&lt;algoritmo&gt;&lt;longitud clave&gt;eadq&lt;año&gt;.crl">http://crl.eadtrust.eu/eadtrust-root-&lt;algoritmo&gt;&lt;longitud clave&gt;eadq&lt;año&gt;.crl</a>
<b>authorityInfoAccess</b>		
calssuers		<a href="http://ca.eadtrust.eu/eadtrust-root-&lt;algoritmo&gt;&lt;longitud clave&gt;eadq&lt;año&gt;.crt">http://ca.eadtrust.eu/eadtrust-root-&lt;algoritmo&gt;&lt;longitud clave&gt;eadq&lt;año&gt;.crt</a>
ocsp		<a href="http://ocsp.eadtrust.eu">http://ocsp.eadtrust.eu</a>
<b>keyUsage</b>	<b>Crítica</b>	Digital Signature, Certificate signing, CRL signing

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

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

### 8.3.5 Perfil de certificado de subCA para emisión de certificados web y PSD2

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

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

- RSA 4096 y SHA 256 (Extended validation que incluye los certificados de sede electrónica de nivel alto y PSD2)
- RSA 4096 y SHA 256 (Domain validation y Organization validation, que incluye los certificados de sede electrónica de nivel medio/sustancial)
- RSA 8192 y SHA 512 (Extended validation y PSD2)
- RSA 8192 y SHA 512 (Domain validation y Organization validation)
- ECC 256 y SHA 256 (Extended validation y PSD2)
- ECC 256 y SHA 256 (Domain validation y Organization validation)
- ECC 384 y SHA 384 (Extended validation y PSD2)
- ECC 384 y SHA 384 (Domain validation y Organization validation)

### 8.3.6 Perfil de certificado de subCA para emisión de certificados no cualificados

Campo	Crítico	Contenido
<b>version</b>		3
<b>serialNumber</b>		Número positivo único
<b>signature</b>		Sha256WithRSAEncryption
<b>issuer</b>		Igual al campo Subject del certificado de la CA emisora
<b>validity</b>		16 años
<b>subject</b>		
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
<b>subjectPublicKeyInfo</b>		RSA 2048 bits
<b>Extensiones</b>		
<b>authorityKeyIdentifier</b>		Derivada del resultado de aplicar el hash a la Clave pública de la AC emisora
<b>basicConstraints</b>	<b>Crítica</b>	CA=true, pathlen=0
<b>subjectKeyIdentifier</b>		Derivada del resultado de aplicar el hash a la clave pública del sujeto
<b>issuerAltName</b>		Igual al campo Subject Alternative Names de la CA Emisora
<b>subjectAltName</b>		rfc822 Name ca@eadtrust.eu URI: <a href="http://www.eadtrust.eu">http://www.eadtrust.eu</a> URI: <a href="http://ca.eadtrust.eu">http://ca.eadtrust.eu</a> URI: <a href="http://policy.eadtrust.eu">http://policy.eadtrust.eu</a>
<b>certificatePolicies</b>		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.1.3161
cpsURI		<a href="http://policy.eadtrust.eu/">http://policy.eadtrust.eu/</a>
userNotice		Subordinate Certificate Authority. European Agency of Digital Trust, S.L.
policyIdentifier		2.5.29.32.0 (AnyPolicy)
<b>cRLDistributionPoints</b>		
distributionPoint		<a href="http://crl.eadtrust.eu/eadtrust-root-&lt;algoritmo&gt;&lt;longitud clave&gt;eadnq&lt;año&gt;.crl">http://crl.eadtrust.eu/eadtrust-root-&lt;algoritmo&gt;&lt;longitud clave&gt;eadnq&lt;año&gt;.crl</a>
<b>authorityInfoAccess</b>		
caIssuers		<a href="http://ca.eadtrust.eu/eadtrust-root-&lt;algoritmo&gt;&lt;longitud clave&gt;eadnq&lt;año&gt;.crt">http://ca.eadtrust.eu/eadtrust-root-&lt;algoritmo&gt;&lt;longitud clave&gt;eadnq&lt;año&gt;.crt</a>
ocsp		<a href="http://ocsp.eadtrust.eu">http://ocsp.eadtrust.eu</a>
<b>keyUsage</b>	<b>Crítica</b>	Digital Signature, Certificate signing, CRL signing

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

- RSA 2048 y SHA 256

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

## 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
<b>Versión</b>		3
<b>serialNumber</b>		Número positivo único
<b>Signature</b>		Sha256WithRSAEncryption ó ecdsa-with-SHA256 ó ecdsa-with-SHA384
<b>Issuer</b>		Igual al campo Subject del certificado de la CA emisora
<b>validity</b>		4 años
<b>subject</b>		
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
<b>subjectPublicKeyInfo</b>		RSA mínimo 2048 bits, ECDSA 256 bits (prime256v1) ó 384 bits (secpr384r1)
<b>Extensiones</b>		
<b>issuerAltName</b>		Igual al campo Subject Alternative Name de la CA Emisora
<b>subjectAltName</b>		email:ca@eadtrust.eu URI:http://www.eadtrust.eu URI:http://ca.eadtrust.eu URI:http://policy.eadtrust.eu
<b>extendedKeyUsage</b>		timeStamping
<b>subjectKeyIdentifier</b>		Derivada del resultado de aplicar el hash a la clave pública del sujeto
<b>authorityKeyIdentifier</b>		Derivada del resultado de aplicar el hash a la Clave pública de la AC emisora
<b>privateKeyUsagePeriod</b>		Indica la fecha y la hora más tempranas en las que la clave privada podría usarse para firmar. notBefore / notAfter
<b>certificatePolicies*</b>		
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-I)
userNotice		European Telecommunications Standards Institute. eIDAS European Regulation Compliant
<b>cRLDistributionPoints</b>		http://crl.eadtrust.eu/eadtrust-subca- <algoritmo><tamañoclave>eadlp<Año>.crl
<b>authorityInfoAccess</b>		

Campo	Crítico	Contenido
calssuers		http://ca.eadtrust.eu/ eadtrust-subca- <algoritmo><tamañoclave>eadlp<Año>.crt
ocsp		http://ocsp.eadtrust.eu
<b>qcStatements **</b>		
QcCompliance		Presente
QcType		id-etsi-qct-eseal
qcStatement-2		0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)
QcRetentionPeriod		15 años
<b>keyUsage</b>	<b>Crítica</b>	digitalSignature
<p>* En caso de que la clave privada del certificado se encuentre en un <b>dispositivo cualificado de creación de sello</b> 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</p> <p>** En caso de que la clave privada del certificado se encuentre en un <b>dispositivo cualificado de creación de sello</b> se añade el campo QSCD</p>		

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

#### 8.4.2 Perfil de certificado no cualificado de persona jurídica para sello de tiempo cualificado y no cualificado

Campo	Crítico	Contenido
<b>Versión</b>		3
<b>serialNumber</b>		Número positivo único
<b>Signature</b>		Sha256WithRSAEncryption ó ecdsa-with-SHA256 ó ecdsa-with-SHA384
<b>Issuer</b>		Igual al campo Subject del certificado de la CA emisora
<b>validity</b>		4 años
<b>subject</b>		
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
<b>subjectPublicKeyInfo</b>		RSA mínimo 2048 bits ECDSA 256 bits (prime256v1) ó 384 bits (secpr384r1)
<b>Extensiones</b>		
<b>issuerAltName</b>		Igual al campo Subject Alternative Names de la CA Emisora
<b>subjectAltName</b>		email:ca@eadtrust.eu URI:http://www.eadtrust.eu URI:http://ca.eadtrust.eu URI:http://policy.eadtrust.eu
<b>extendedKeyUsage</b>		timeStamping
<b>subjectKeyIdentifier</b>		Derivada del resultado de aplicar el hash a la clave pública del sujeto
<b>authorityKeyIdentifier</b>		Derivada del resultado de aplicar el hash a la Clave pública de la AC emisora
<b>certificatePolicies</b>		

Campo	Crítico	Contenido
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.
<b>cRLDistributionPoints</b>		http://crl.eadtrust.eu/eadtrust-subca- <algoritmo><tamañoclave>eadnq<Año>.crl
<b>authorityInfoAccess</b>		
caIssuers		http://ca.eadtrust.eu/ <algoritmo><tamañoclave>eadnq<Año>.crt
ocsp		http://ocsp.eadtrust.eu
<b>keyUsage</b>	<b>Crítica</b>	digitalSignature

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

#### 8.4.3 Perfil de certificado cualificado de persona física

Campo	Crítico	Contenido
<b>version</b>		3
<b>serialNumber</b>		Número positivo único
<b>signature</b>		Sha256WithRSAEncryption o ecdsa-with-SHA256 o ecdsa-with-SHA384
<b>issuer</b>		Igual al campo Subject del certificado de la CA emisora
<b>validity</b>		4 años
<b>subject</b>		
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
<b>subjectPublicKeyInfo</b>		RSA mínimo 2048 bits ECDSA 256 bits (prime256v1) ó 384 bits (secpr384r1)
<b>Extensiones</b>		
<b>authorityKeyIdentifier</b>		Derivada del resultado de aplicar el hash a la Clave pública de la AC emisora
<b>subjectKeyIdentifier</b>		Derivada del resultado de aplicar el hash a la clave pública del sujeto
<b>issuerAltName</b>		Igual al campo Subject Alternative Names de la CA Emisora
<b>subjectAltName</b>		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
<b>certificatePolicies*</b>		
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)



<b>qcStatements**</b>		
QcCompliance		Presente
QcType		id-etsi-qct-esign
QcRetentionPeriod		15 años
qcStatement-2		0.4.0.194121.1.1 (id-etsi-qcs-SemanticsId-Natural)
<b>cRLDistributionPoints</b>		
distributionPoint		http://crl.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadnp<Año>.crl
<b>authorityInfoAccess</b>		
calssuers		http://ca.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadnp<Año>.crt
ocsp		http://ocsp.eadtrust.eu
<b>extendedKeyUsage</b>		clientAuth, emailProtection
<b>keyUsage</b>	<b>Crítica</b>	digitalSignature, nonRepudiation, keyEncipherment
<p>* En caso de que la clave privada del certificado se encuentre en un <b>dispositivo cualificado de creación de firma</b> 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</p> <p>** En caso de que la clave privada del certificado se encuentre en un <b>dispositivo cualificado de creación de firma</b> se añade el campo QSCD</p>		

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

#### 8.4.4 Perfil de certificado cualificado de representante de persona jurídica

Campo	Crítico	Contenido
<b>version</b>		3
<b>serialNumber</b>		Número positivo único
<b>signature</b>		Sha256WithRSAEncryption o ecdsa-with-SHA256 o ecdsa-with-SHA384
<b>issuer</b>		Igual al campo Subject del certificado de la CA emisora
<b>validity</b>		4 años
<b>subject</b>		
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
<b>subjectPublicKeyInfo</b>		RSA mínimo 2048 bits ó ECDSA 256 bits (prime256v1) ó 384 bits (secpr384r1)
<b>Extensiones</b>		
<b>authorityKeyIdentifier</b>		Derivada del resultado de aplicar el hash a la Clave pública de la AC emisora
<b>subjectKeyIdentifier</b>		Derivada del resultado de aplicar el hash a la clave pública del sujeto
<b>issuerAltName</b>		Igual al campo Subject Alternative Names de la CA Emisora

Campo	Crítico	Contenido
<b>subjectAltName</b>		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
<b>certificatePolicies*</b>		
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)
<b>qcStatements**</b>		
QcCompliance		Presente
QcType		id-etsi-qct-esign
QcRetentionPeriod		15 años
qcStatement-2		0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)
<b>cRLDistributionPoints</b>		
distributionPoint		http://crl.eadtrust.eu/eadtrust-subca- <algoritmo><tamañoclave>eadnp<Año>.crl
<b>authorityInfoAccess</b>		
caIssuers		http://ca.eadtrust.eu/eadtrust-subca- <algoritmo><tamañoclave>eadnp<Año>.crt
ocsp		http://ocsp.eadtrust.eu
<b>extendedKeyUsage</b>		clientAuth, emailProtection
<b>keyUsage</b>	<b>Crítica</b>	digitalSignature, nonRepudiation, keyEncipherment
<p>* En caso de que la clave privada del certificado se encuentre en un <b>dispositivo cualificado de creación de firma</b> 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</p> <p>** En caso de que la clave privada del certificado se encuentre en un <b>dispositivo cualificado de creación de firma</b> se añade el campo QSCD</p>		

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

#### 8.4.5 Perfil de certificado cualificado de web “domain validated” (QWAC)

Campos/Extensiones	Crítico	Contenido
<b>Versión</b>		3
<b>serialNumber</b>		Unique non-sequential positive number of minimum length 64 bits
<b>Signature</b>		Sha256WithRSAEncryption ó ecdsa-with-SHA256 ó ecdsa-with-SHA384
<b>Issuer</b>		Same as the Subject field of the issuing CA certificate
<b>Validity</b>		2 años

Campos/Extensiones	Crítico	Contenido
<b>Subject</b>		
OrganizationalUnit		Type of web certificate
<b>subjectPublicKeyInfo</b>		RSA 2048 bits minimum or ECDSA 256 bits (prime256v1) or 384 bits (secpr384r1)
<b>Extensions</b>		
<b>subjectAltName</b>		
dnsName		DNS name(s)
<b>extendedKeyUsage</b>		serverAuth, clientAuth
<b>subjectKeyIdentifier</b>		Derived from the result of applying the hash to the public key of the subject
<b>authorityKeyIdentifier</b>		Derived from the result of applying the hash to the Public key of the issuing CA
<b>certificatePolicies</b>		
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)
<b>cRLDistributionPoints</b>		http://crl.eadtrust.eu/eadtrust-subca- <algoritmo><tamañoclave>eaddvov<Año>.crl
<b>authorityInfoAccess</b>		
caIssuers		http://ca.eadtrust.eu/eadtrust-subca- <algoritmo><tamañoclave>eaddvov<Año>.crt
Ocsp		http://ocsp.eadtrust.eu
<b>basicConstraint</b>	Crítica	CA false
<b>qcStatements</b>		
QcRetentionPeriod		15 years
QcCompliance		Present
QcType		id-etsi-qct-web
<b>keyUsage</b>	Crítica	digitalSignature, keyEncipherment
<b>CT RFC6962</b>		Certificate Transparency

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

#### 8.4.6 Perfil de certificado cualificado de web “organization validated” (QWAC)

Campos/Extensiones	Crítico	Contenido
<b>version</b>		3
<b>serialNumber</b>		Unique non-sequential positive number of minimum length 64 bits
<b>signature</b>		Sha256WithRSAEncryption or ecdsa-with-SHA256 or ecdsa-with-SHA384
<b>issuer</b>		Same as the Subject field of the issuing CA certificate
<b>validity</b>		2 años
<b>subject</b>		
OrganizationalUnit		Type of web certificate
OrganizationName		Organization Name
LocalityName		Locality Name
StateOrProvinceName		State or province name

Campos/Extensiones	Crítico	Contenido
CountryName		CountryName
subjectPublicKeyInfo		RSA 2048 bits minimum or ECDSA 256 bits (prime256v1) or 384 bits (secpr384r1)
<b>Extensions</b>		
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

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

#### 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

Campos/Extensiones	Crítico	Contenido
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
<b>subjectPublicKeyInfo</b>		RSA 2048 bits minimum or ECDSA 256 bits (prime256v1) or 384 bits (secpr384r1)
<b>Extensions</b>		
<b>subjectAltName</b>		
dnsName		DNS name(s)
<b>extendedKeyUsage</b>		serverAuth, clientAuth
<b>subjectKeyIdentifier</b>		Derived from the result of applying the hash to the public key of the subject
<b>authorityKeyIdentifier</b>		Derived from the result of applying the hash to the Public key of the issuing CA
<b>certificatePolicies</b>		
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)
<b>cRLDistributionPoints</b>		http://crl.eadtrust.eu/eadtrust-subca- <algoritmo><tamañoclave>eadevpsd2<Año>.crl
<b>authorityInfoAccess</b>		
caIssuers		http://ca.eadtrust.eu/eadtrust-subca- <algoritmo><tamañoclave>eadevpsd2<Año>.crt
ocsp		http://ocsp.eadtrust.eu
<b>basicConstraint</b>	Crítica	CA false
<b>qcStatements</b>		
QcCompliance		Present
QcType		id-etsi-qct-web
QcRetentiodPeriod		15
<b>keyUsage</b>	Crítica	digitalSignature, keyEncipherment
<b>CT RFC6962</b>		Certificate Transparency

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

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

Campos/Extensiones	Crítico	Contenido
<b>Versión</b>		3
<b>serialNumber</b>		Número positivo único
<b>signature</b>		Sha256WithRSAEncryption ó ecDSA-with-SHA256 ó ecDSA-with-SHA384
<b>Issuer</b>		Igual que el subject de la CA C O OU OI CN
<b>Validity</b>		4 años

Campos/Extensiones	Crítico	Contenido
<b>Subject</b>		
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
<b>subjectPublicKeyInfo</b>		RSA 2048 bits
<b>extensions</b>		
<b>subjectAltName</b>		
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 suscriptor
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
<b>extendedKeyUsage</b>		clientAuth, emailProtection
<b>subjectKeyIdentifier</b>		Derivado de aplicar el hash a la clave del suscriptor
<b>authorityKeyIdentifier</b>		Derivado de aplicar el hash a la clave del emisor
<b>certificatePolicies*</b>		
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
<b>cRLDistributionPoints</b>		http://crl.eadtrust.eu/eadtrust-subca- <algoritmo><tamañoclave>eadnp<Año>.crl
<b>authorityInfoAccess</b>		
calssuers		http://ca.eadtrust.eu/eadtrust-subca- <algoritmo><tamañoclave>eadnp<Año>.crt
ocsp		http://ocsp.eadtrust.eu
<b>qcStatements**</b>		
QcCompliance		Present
QcType		id-etsi-qct-esign

Campos/Extensiones	Crítico	Contenido
QcRetentiodPeriod		15
qcStatement-2		0.4.0.194121.1.1 (id-etsi-qcs-SemanticsId-Natural)
<b>keyUsage</b>	Crítica	digitalSignature, keyEncipherment,contentcommitment
<p>* En caso de que la clave privada del certificado se encuentre en un <b>dispositivo cualificado de creación de firma</b> 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</p> <p>** En caso de que la clave privada del certificado se encuentre en un <b>dispositivo cualificado de creación de firma</b> se añade el campo QSCD</p>		

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 Público (LRJ) y al Reglamento (UE) 910/2014.

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

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

Campos/Extensiones	Crítico	Contenido
<b>Versión</b>		3
<b>serialNumber</b>		Número positivo único
<b>signature</b>		Sha256WithRSAEncryption
<b>Issuer</b>		Igual que el subject de la CA C O OU OI CN
<b>Validity</b>		4 años
<b>Subject</b>		
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
<b>subjectPublicKeyInfo</b>		RSA 2048
<b>extensions</b>		
<b>subjectAltName</b>		
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

Campos/Extensiones	Crítico	Contenido
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
<b>subjectKeyIdentifier</b>		Derivado de aplicar el hash a la clave del suscriptor
<b>authorityKeyIdentifier</b>		Derivado de aplicar el hash a la clave del emisor
<b>certificatePolicies*</b>		
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
<b>cRLDistributionPoints</b>		http://crl.eadtrust.eu/eadtrust-subca- <algoritmo><tamañoclave>eadnp<Año>.crl
<b>authorityInfoAccess</b>		
caIssuers		http://ca.eadtrust.eu/eadtrust-subca- <algoritmo><tamañoclave>eadnp<Año>.crt
ocsp		http://ocsp.eadtrust.eu
<b>qcStatements**</b>		
QcCompliance		Present
QcType		id-etsi-qct-esign
QcRetentiodPeriod		15
QcSSCD		Presente
qcStatement-2		0.4.0.194121.1.1 (id-etsi-qcs-SemanticsId-Natural)
<b>keyUsage</b>	Crítica	contentCommitment

Contempla el uso de dispositivo cualificado de creación de firma.

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

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

Campos/Extensiones	Crítico	Contenido
<b>Versión</b>		3
<b>serialNumber</b>		Número positivo único
<b>signature</b>		Sha256WithRSAEncryption
<b>Issuer</b>		Igual que el subject de la CA C O OU OI CN
<b>Validity</b>		4 años
<b>Subject</b>		
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



Campos/Extensiones	Crítico	Contenido
CountryName		CountryName
subjectPublicKeyInfo		RSA 2048
<b>extensions</b>		
subjectAltName		
rfc822Name	Opcional	Email del responsable
directoryName		
2.16.724.1.3.5.4.1.1		CERTIFICADO CUALIFICADO DE FIRMA ELECTRONICA DE EMPLEADO PUBLICO CON SEUDONIMO, DE NIVEL ALTO
2.16.724.1.3.5.4.1.2		Entidad suscriptora
2.16.724.1.3.5.4.1.3		NIF suscriptora
2.16.724.1.3.5.4.1.9	Opcional	Correo electrónico de contacto
2.16.724.1.3.5.4.1.10	Opcional	Unidad
2.16.724.1.3.5.4.1.11	Opcional	Puesto
2.16.724.1.3.5.4.1.12		Seudónimo
subjectKeyIdentifier		Derivado de aplicar el hash a la clave del suscriptor
authorityKeyIdentifier		Derivado de aplicar el hash a la clave del emisor
certificatePolicies*		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.1.41225
cpsURI		http://policy.eadtrust.eu
userNotice		European Agency of Digital Trust, S.L. Certificado cualificado de empleado público con seudónimo nivel alto
policyIdentifier		0.4.0.194112.1.2 (ETSI QCP-n-qscd)
policyIdentifier		2.16.724.1.3.5.4.1
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
<b>qcStatements**</b>		
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.

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

8.4.11 Perfil de certificado cualificado de web PSD2 (QWAC)

Campos/Extensiones	Crítico	Contenido
<b>version</b>		3
<b>serialNumber</b>		Unique non-sequential positive number of minimum length 64 bits
<b>signature</b>		Sha256WithRSAEncryption or ecdsa-with-SHA256 or ecdsa-with-SHA384
<b>issuer</b>		Same as the Subject field of the issuing CA certificate
<b>validity</b>		2 años
<b>subject</b>		
OrganizationIdentifier		ETSI EN 319 412-1 and CA/B Forum format
OrganizationalUnit		Type of web certificate
OrganizationName		Organization Name
LocalityName		Locality Name
StateOrProvinceName		State or province name
CountryName		CountryName
businessCategory		Private Organization, Government Entity, Business Entity or Non-Commercial Entity
jurisdictionCountryName		Country of Jurisdiction of Incorporation or Registration Field
jurisdictionStOrProvName		State or Province of Jurisdiction of Incorporation or Registration Field
jurisdictionLocalityName		Locality of Jurisdiction of Incorporation or Registration Field
serialNumber		Registration Number
<b>subjectPublicKeyInfo</b>		RSA 2048 bits minimum or ECDSA 256 bits (prime256v1) or 384 bits (secpr384r1)
<b>extensions</b>		
<b>subjectAltName</b>		
dnsName		DNS name(s)
<b>extendedKeyUsage</b>		serverAuth, clientAuth
<b>subjectKeyIdentifier</b>		Derived from the result of applying the hash to the public key of the subject
<b>authorityKeyIdentifier</b>		Derived from the result of applying the hash to the Public key of the issuing CA
<b>certificatePolicies</b>		
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
<b>basicConstraint</b>	Crítica	CA false
<b>qcStatements</b>		
QcCompliance		Present

Campos/Extensiones	Crítico	Contenido
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
<b>keyUsage</b>	Crítica	digitalSignature, keyEncipherment
<b>CT RFC6962</b>		Certificate Transparency
<b>cabfOrganizationIdentifier</b>		Effective January 31, 2020, if the subject:organizationIdentifier field is present, this field MUST be present

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

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

#### 8.4.12 Perfil de certificado cualificado de sello electrónico para persona jurídica

Campos/Extensiones	Crítico	Contenido
<b>version</b>		3
<b>serialNumber</b>		Número positivo único
<b>signature</b>		Sha256WithRSAEncryption ó ecdsa-with-SHA256 ó ecdsa-with-SHA384
<b>issuer</b>		Igual al campo Subject del certificado de la CA emisora
<b>validity</b>		4 años
<b>subject</b>		
serialNumber	Opcional	DNI/NIE en formato ETSI EN 412-1
Surname	Opcional	Apellidos
Givenname	Opcional	Nombre
CommonName		Nombre común
organizationIdentifier		<3 caracteres de tipo de identidad><país>- <identificador>. Ejemplo: VATES-B12312312
Organization Name		Nombre registrado completo
Country		País
OrganizationalUnit		Certificado de Sello de Entidad
<b>subjectPublicKeyInfo</b>		RSA 2048 mínimo ECDSA 256 bits (prime256v1) ó 384 bits (secpr384r1)
<b>extensions</b>		
<b>issuerAltName</b>		Igual al campo SubjectAlternativeNames de la CA Emisora
<b>extendedKeyUsage</b>		clientAuth, emailProtection
<b>subjectKeyIdentifier</b>		Derivada del resultado de aplicar el hash a la clave pública del sujeto
<b>authorityKeyIdentifier</b>		Derivada del resultado de aplicar el hash a la Clave pública de la AC emisora
<b>certificatePolicies</b>		
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.

Campos/Extensiones	Crítico	Contenido
policyIdentifier		0.4.0.194112.1.1 (OID ETSI QCP-I)
userNotice		European Telecommunications Standards Institute. eIDAS European Regulation Compliant
<b>cRLDistributionPoints</b>		http://crl.eadtrust.eu/eadtrust-subca- <algoritmo><tamañoclave>eadlp<Año>.crl
<b>authorityInfoAccess</b>		
caIssuers		http://ca.eadtrust.eu/eadtrust-subca- <algoritmo><tamañoclave>eadlp<Año>.crt
ocsp		http://ocsp.eadtrust.eu
<b>basicConstraint</b>	Crítica	CA false
<b>qcStatements</b>		
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
<p>* En caso de que la clave privada del certificado se encuentre en un <b>dispositivo cualificado de creación de sello</b> 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</p> <p>** En caso de que la clave privada del certificado se encuentre en un <b>dispositivo cualificado de creación de sello</b> se añade el campo QSCD</p>		

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

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

Campos/Extensiones	Crítico	Contenido
<b>version</b>		3
<b>serialNumber</b>		Número positivo único
<b>signature</b>		Sha256WithRSAEncryption ó ecdsa-with-SHA256 ó ecdsa-with-SHA384
<b>issuer</b>		Igual al campo Subject del certificado de la CA emisora
<b>validity</b>		4 años
<b>subject</b>		
serialNumber	Opcional	DNI/NIE en formato ETSI EN 412-1
Surname	Opcional	Apellidos
Givenname	Opcional	Nombre
CommonName		Nombre común
organizationIdentifier		<3 caracteres de tipo de identidad><país>- <identificador>. Ejemplo: VATES-B12312312
Organization Name		Nombre registrado completo
Country		País
OrganizationalUnit		Certificado de Sello de Entidad
<b>subjectPublicKeyInfo</b>		RSA mínimo 2048 bits ECDSA 256 bits (prime256v1) ó 384 bits (secpr384r1)
<b>extensions</b>		
<b>issuerAltName</b>		Igual al campo SubjectAlternativeNames de la CA Emisora

Campos/Extensiones	Crítico	Contenido
<b>extendedKeyUsage</b>		clientAuth, emailProtection
<b>subjectKeyIdentifier</b>		Derivada del resultado de aplicar el hash a la clave pública del sujeto
<b>authorityKeyIdentifier</b>		Derivada del resultado de aplicar el hash a la Clave pública de la AC emisora
<b>certificatePolicies*</b>		
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-I)
userNotice		European Telecommunications Standards Institute. eIDAS European Regulation Compliant
<b>cRLDistributionPoints</b>		http://crl.eadtrust.eu/eadtrust-subca- <algoritmo><tamañoclave>eadlp<Año>.crl
<b>authorityInfoAccess</b>		
caIssuers		http://ca.eadtrust.eu/eadtrust-subca- <algoritmo><tamañoclave>eadlp<Año>.crt
ocsp		http://ocsp.eadtrust.eu
<b>basicConstraint</b>	Crítica	CA false
<b>qcStatements**</b>		
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
<p>* En caso de que la clave privada del certificado se encuentre en un <b>dispositivo cualificado de creación de sello</b> 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</p> <p>** En caso de que la clave privada del certificado se encuentre en un <b>dispositivo cualificado de creación de sello</b> se añade el campo QSCD</p>		

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

#### 8.4.14 Perfil de certificado cualificado de sede electrónica administrativa "Organization Validated" (QWAC) con nivel de aseguramiento medio/sustancial

Campos/Extensiones	Crítico	Contenido
<b>version</b>		3
<b>serialNumber</b>		integer positivo, no mayor 20 octetos *
<b>signature</b>		SHA-2 con RSA.
<b>issuer</b>		Mismo Subject que el del certificado emisor. Country Common Name Organization
<b>validity</b>		372 días (maximun 397 days)
<b>subject</b>		

Campos/Extensiones	Crítico	Contenido
OrganizationalUnit		OU= "SEDE ELECTRONICA"
OrganizationalUnit		El nombre descriptivo de la sede. OU= p. ej: PUNTO DE ACCESO GENERAL
OrganizationName		Denominación (nombre "oficial" de la organización) del suscriptor de servicios de certificación (custodio del certificado)
Common Name		Denominación de nombre de dominio (DNS) donde residirá el certificado. CN= p. ej: administracion.gob.es
LocalityName		Ciudad
StateOrProvinceName		State or province name
CountryName		Estado cuya ley rige el nombre, que será ES ("España") por tratarse de entidades públicas.
serialNumber		El NIF de la entidad responsable. SerialNumber = p. ej: S2833002. Size [RFC 5280] 64
Organization Identifier		Identificador de la organización. Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad) OrganizationIdentifier p. ej: VATES-S2833002.
<b>subjectPublicKeyInfo</b>		RSA 2048 bits minimum
<b>Extensions</b>		
<b>subjectAltName</b>		
dnsName		DNS name(s)
<b>extendedKeyUsage</b>		serverAuth
<b>subjectKeyIdentifier</b>		Identificador de la clave pública del suscriptor o poseedor de claves (derivada de utilizar la función de Hash sobre la clave pública del sujeto). Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.
<b>authorityKeyIdentifier</b>		Medio para identificar la clave pública correspondiente a la clave privada utilizada para firmar un certificado, por ejemplo, en los casos en que el emisor tiene múltiples claves de firma.
<b>certificatePolicies</b>		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.0.41245
cpsURI		http://policy.eadtrust.eu
userNotice		Ej: "Certificado cualificado de sede electrónica, nivel medio/sustancial. Consulte las condiciones de uso en " + URL de la DPC o, en su caso, documento legal de tercero
policyIdentifier		0.4.0.194112.1.4 (ETSI QCP-w)
policyIdentifier		2.23.140.1.2.2 (CAB/FORUM OV)
policyIdentifier		2.16.724.1.3.5.5.2
<b>cRLDistributionPoints</b>		http://crl.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eaddvov<Año>.crl
<b>authorityInfoAccess</b>		
calssuers		http://ca.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eaddvov<Año>.crt
ocsp		http://ocsp.eadtrust.eu
<b>basicConstraint</b>	Crítica	CA false
<b>qcStatements</b>		
QcCompliance		Indicación de certificado cualificado
QcType		id-etsi-qct-web

Campos/Extensiones	Crítico	Contenido
QcRetentiodPeriod		Integer:=15 ([ETSI EN 319 412-5] describe el periodo de conservación de toda la información relevante para el uso de un certificado, tras la caducidad de este)
QcPDS		Lugar donde se encuentra la declaración PDS
semnaticsId-Legal		Para indicar semántica de persona jurídica definida por la EN 319 412-1
keyUsage	Crítica	digitalSignature, keyEncipherment
CT RFC6962		Certificate Transparency (cuando estemos en CA/B Forum)

Los certificados OV pueden ser multidominio y se pueden emitir con calificadores de subdominio de tipo “wildcard” (\*).

#### 8.4.15 Perfil de certificado cualificado de sede electrónica administrativa “Extended Validation” (QWAC) con nivel de aseguramiento Alto

Campos/Extensiones	Crítico	Contenido
version		3
serialNumber		integer positivo, no mayor 20 octetos
signature		SHA-2 con RSA.
issuer		Mismo Subject que el del certificado emisor. Campos Country Common Name Organization
validity		372 días (maximun 397 days)
subject		
OrganizationalUnit		OU= “SEDE ELECTRONICA”
OrganizationalUnit		El nombre descriptivo de la sede. OU= p. ej: PUNTO DE ACCESO GENERAL
businessCategory		businessCategory = “Government Entity”
jurisdictionCountryName		jurisdictionCountryName= “ES”
jurisdictionStOrProvName		State or Province of Jurisdiction of Incorporation or Registration Field
jurisdictionLocalityName		Locality of Jurisdiction of Incorporation or Registration Field
OrganizationName		Denominación (nombre “oficial” de la organización) del suscriptor de servicios de certificación (custodio del certificado)
Common Name		Denominación de nombre de dominio (DNS) donde residirá el certificado. CN= p. ej: administracion.gob.es
LocalityName		Ciudad
StateOrProvinceName		State or province name
CountryName		Estado cuya ley rige el nombre, que será ES (“España”) por tratarse de entidades públicas.
serialNumber		El NIF de la entidad responsable. SerialNumber = p. ej: S2833002. Size [RFC 5280] 64

Campos/Extensiones	Crítico	Contenido
Organization Identifier		Identificador de la organización. Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad) OrganizationIdentifier p. ej: VATES-S2833002.
subjectPublicKeyInfo		RSA 2048 bits
<b>Extensions</b>		
subjectAltName		
dnsName		DNS name(s)
extendedKeyUsage		serverAuth
subjectKeyIdentifier		Identificador de la clave pública del suscriptor o poseedor de claves (derivada de utilizar la función de Hash sobre la clave pública del sujeto). Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.
authorityKeyIdentifier		Medio para identificar la clave pública correspondiente a la clave privada utilizada para firmar un certificado, por ejemplo en los casos en que el emisor tiene múltiples claves de firma.
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.0.41246
cpsURI		http://policy.eadtrust.eu
userNotice		P. ej: "Certificado cualificado de sede electrónica, nivel alto. Consulte las condiciones de uso en " + URL de la DPC o, en su caso, documento legal de tercero
policyIdentifier		0.4.0.194112.1.4 (ETSI QCP-w)
policyIdentifier		2.23.140.1.1 (CAB/FORUM EV)
policyIdentifier		2.16.724.1.3.5.5.1
cRLDistributionPoints		http://crl.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadevpsd2<Año>.crl
authorityInfoAccess		
calssuers		http://ca.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadevpsd2<Año>.crt
ocsp		http://ocsp.eadtrust.eu
basicConstraint	Crítica	CA false
qcStatements		
QcCompliance		Indicación de certificado cualificado
QcType		id-etsi-qct-web
QcRetentiodPeriod		Integer:=15 ([ETSI EN 319 412-5] describe el periodo de conservación de toda la información relevante para el uso de un certificado, tras la caducidad de este) OID 0.4.0.1862.1.3
QcPDS		Lugar donde se encuentra la declaración PDS
semanticsId-Legal		Para indicar semántica de persona jurídica definida por la EN 319 412-1
keyUsage	Crítica	digitalSignature, keyEncipherment
CT RFC6962		Certificate Transparency (cuando estemos en CA/B Forum)
cabfOrganizationIdentifier		(OID: 2.23.140.3.1) If the subject:organizationIdentifier is present, this field MUST be present.

Los certificados EV pueden ser multidominio pero NO se pueden emitir con calificadores de subdominio de tipo "wildcard" (\*).



8.4.16 Perfil de certificado cualificado de sello de órgano Nivel Medio/Sustancial

Campos/Extensiones	Crítico	Contenido
<b>version</b>		3
<b>serialNumber</b>		Número positivo único (menor de 20 octetos)
<b>signature</b>		Sha256WithRSAEncryption
<b>issuer</b>		Igual al campo Subject del certificado de la CA emisora Country Organization Organizational Unit Organization Identifier Common Name
<b>validity</b>		5 años (o menos)
<b>subject</b>		
serialNumber	Opcional	Número único de identificación de la entidad, aplicable de acuerdo con la legislación del país. En España, NIF.  SerialNumber = p. ej: S2833002. Número secuencial único asignado por el prestador (Printable String ) Size [RFC 5280] 64
Surname	Opcional	Primer y segundo apellido, de acuerdo con documento de identidad (DNI/Pasaporte), así como su DNI (Ver Criterios de Composición del campo CN para un empleado público).  Primer apellido, espacio en blanco, segundo apellido del responsable del certificado (titular del órgano) de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 80 p. ej: "DE LA CAMARA ESPAÑOL - DNI 00000000G"
Givenname	Opcional	Nombre de pila, de acuerdo con documento de identidad (DNI/Pasaporte)  Nombre de pila del responsable del certificado (titular del órgano) de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40  p. ej: "JUAN ANTONIO"
CommonName		Denominación de sistema o aplicación de proceso automático.  CN= p. ej: "PLATAFORMA DE VALIDACION Y FIRMA ELECTRONICA. @FIRMA. Nombre descriptivo del sistema automático. Asegurando que dicho nombre tenga sentido y no dé lugar a ambigüedades.
organizationIdentifier		Identificador de la organización distinto del nombre Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)

Campos/Extensiones	Crítico	Contenido
Organization Name		Denominación (nombre "oficial" de la organización) del creador del sello.
Country		Estado cuya ley rige el nombre, que será "España" por tratarse de entidades públicas.
OrganizationalUnit		SELLO ELECTRONICO
OrganizationalUnit		Denominación oficial de la unidad p. ej: SUBDIRECCION DE EXPLOTACION
OrganizationalUnit		Código DIR3 de la unidad p. ej: E04976701
<b>subjectPublicKeyInfo</b>		RSA 2048 mínimo
<b>extensions</b>		
<b>issuerAltName</b>		Igual al campo SubjectAlternativeNames de la CA Emisora
<b>Subject Alternate Names</b>		
Rfc822Name		Correo electrónico de contacto de la entidad suscriptora del sello. P. ej: soporte.afirma5@minhap.es
Directory Name		<p>Tipo de certificado Tipo= SELLO ELECTRONICO DE NIVEL MEDIO (String UTF8) Size = 31 2.16.724.1.3.5.6.2.1</p> <p><b>Nombre de la entidad suscriptora</b> Entidad Suscriptora = p. ej: MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS (String UTF8) Size = 80 OID: 2.16.724.1.3.5.6.2.2</p> <p><b>NIF entidad suscriptora</b> NIF suscriptora = NIF entidad suscriptora, p. ej: S2833002 (String UTF8) Size = 9 OID: 2.16.724.1.3.5.6.2.3</p> <p><b>DNI/NIE del responsable (titular del órgano)</b> DNI/NIE responsable= p. ej: 00000000G (String UTF8) Size = 9 OID: 2.16.724.1.3.5.6.2.4</p> <p><b>Denominación de sistema o componente</b> Nombre descriptivo del sistema de sellado automático, asegurando que dicho nombre tenga sentido y no dé lugar a ambigüedades. Denominación sistema = p. ej: "PLATAFORMA DE VALIDACION Y FIRMA ELECTRONICA. @FIRMA". (String UTF8) Size = 128 OID: 2.16.724.1.3.5.6.2.5</p> <p><b>Nombre de pila (titular del órgano)</b> N = Nombre de pila del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte.</p>

Campos/Extensiones	Crítico	Contenido
		<p>(String UTF8) Size 40            OID: 2.16.724.1.3.5.6.2.6            Ej: "JUAN ANTONIO"  <b>Primer apellido (titular del órgano)</b>            SN1 = Primer apellido del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte.            (String UTF8) Size 40            OID: 2.16.724.1.3.5.6.2.7 Ej: "DE LA CAMARA"  <b>Segundo apellido (titular del órgano)</b>            SN2 = Segundo apellido del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte.            (String UTF8) Size 40            En caso de no existir el segundo apellido, se dejará en blanco (sin ningún carácter).            OID: 2.16.724.1.3.5.6.2.8 Ej: "ESPAÑOL"  <b>Correo electrónico</b>            Correo electrónico de la persona responsable del sello, p. ej: juanantonio.delacamara.espanol@mpr.es (String) Size [RFC 5280] 255            OID: 2.16.724.1.3.5.6.2.9</p>
<b>extendedKeyUsage</b>		clientAuth, emailProtection
<b>subjectKeyIdentifier</b>		Derivada del resultado de aplicar el hash a la clave pública del sujeto
<b>authorityKeyIdentifier</b>		Derivada del resultado de aplicar el hash a la Clave pública de la AC emisora
<b>certificatePolicies</b>		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.0.41233
cpsURI		http://policy.eadtrust.eu
userNotice		Ej: "Certificado cualificado de sello electrónico de Administración, órgano o entidad de derecho público, nivel Medio/Sustancial. Consulte las condiciones de uso en " + URL de la DPC o, en su caso, documento legal de tercero.
policyIdentifier		0.4.0.194112.1.1 (OID ETSI QCP-I)
userNotice		European Telecommunications Standards Institute. eIDAS European Regulation Compliant
policyIdentifier		2.16.724.1.3.5.6.2
<b>cRLDistributionPoints</b>		http://crl.eadtrust.eu/eadtrust-subca- <algoritmo><tamañoclave>eadlp<Año>.crl
<b>authorityInfoAccess</b>		

Campos/Extensiones	Crítico	Contenido
calssuers		http://ca.eadtrust.eu/eadtrust-subca- <algoritmo><tamañoclave>eadlp<Año>.crt
ocsp		http://ocsp.eadtrust.eu
<b>basicConstraint</b>	Crítica	CA false
<b>qcStatements</b>		
QcCompliance		Presente
QcType		id-etsi-qct-eseal
QcRetentiodPeriod		Integer:=15 ([ETSI EN 319 412-5] describe el periodo de conservación de toda la información relevante para el uso de un certificado, tras la caducidad de este) OID 0.4.0.1862.1.3
qcStatement-2		0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)
QcPDS		
<b>keyUsage</b>	Crítica	digitalSignature, nonRepudiation, keyEncipherment

#### 8.4.17 Perfil de certificado cualificado de sello de órgano Nivel Alto

Campos/Extensiones	Crítico	Contenido
<b>version</b>		3
<b>serialNumber</b>		Número positivo único (menor de 20 octetos)
<b>signature</b>		Sha256WithRSA Encryption.
<b>issuer</b>		Igual al campo Subject del certificado de la CA emisora Country Organization Organizational Unit Organization Identifier Common Name
<b>validity</b>		5 años (o menos)
<b>subject</b>		
serialNumber	Opcional	Número único de identificación de la entidad, aplicable de acuerdo con la legislación del país. En España, NIF.  SerialNumber = p. ej: S2833002. Número secuencial único asignado por el prestador (Printable String) ) Size [RFC 5280] 64

Campos/Extensiones	Crítico	Contenido
Surname	Opcional	<p>Primer y segundo apellido, de acuerdo con documento de identidad (DNI/Pasaporte), así como su DNI (Ver Criterios de Composición del campo CN para un empleado público).</p> <p>Primer apellido, espacio en blanco, segundo apellido del responsable del certificado (titular del órgano) de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 80 p. ej: "DE LA CAMARA ESPAÑOL - DNI 00000000G"</p>
Givenname	Opcional	<p>Nombre de pila, de acuerdo con documento de identidad (DNI/Pasaporte)</p> <p>Nombre de pila del responsable del certificado (titular del órgano) de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40</p> <p>p. ej: "JUAN ANTONIO"</p>
CommonName		<p>Denominación de sistema o aplicación de proceso automático.</p> <p>CN= p. ej: "PLATAFORMA DE VALIDACION Y FIRMA ELECTRONICA. @FIRMA. Nombre descriptivo del sistema automático. Asegurando que dicho nombre tenga sentido y no dé lugar a ambigüedades.</p>
organizationIdentifier		Identificador de la organización distinto del nombre Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)
Organization Name		Denominación (nombre "oficial" de la organización) del creador del sello.
Country		Estado cuya ley rige el nombre, que será "España" por tratarse de entidades públicas.
OrganizationalUnit		SELLO ELECTRONICO
OrganizationalUnit		Denominación oficial de la unidad p. ej: SUBDIRECCION DE EXPLOTACION
OrganizationalUnit		Código DIR3 de la unidad p. ej: E04976701
<b>subjectPublicKeyInfo</b>		RSA 2048 mínimo
<b>extensions</b>		
<b>issuerAltName</b>		Igual al campo SubjectAlternativeNames de la CA Emisora
<b>Subject Alternate Names</b>		
Rfc822Name		Correo electrónico de contacto de la entidad suscriptora del sello. P. ej: soporte.afirma5@minhap.es
Directory Name		<b>Tipo de certificado</b>

Campos/Extensiones	Crítico	Contenido
		<p>Tipo= SELLO ELECTRONICO DE NIVEL ALTO (String UTF8) Size = 31 2.16.724.1.3.5.6.1.1</p> <p><b>Nombre de la entidad suscriptora</b> Entidad Suscriptora = p. ej: MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS (String UTF8) Size = 80 OID: 2.16.724.1.3.5.6.1.2</p> <p><b>NIF entidad suscriptora</b> NIF suscriptora = NIF entidad suscriptora, p. ej: S2833002 (String UTF8) Size = 9 OID: 2.16.724.1.3.5.6.1.3</p> <p><b>DNI/NIE del responsable (titular del órgano)</b> DNI/NIE responsable= p. ej: 00000000G (String UTF8) Size = 9 OID: 2.16.724.1.3.5.6.1.4</p> <p><b>Denominación de sistema o componente</b> Nombre descriptivo del sistema de sellado automático, asegurando que dicho nombre tenga sentido y no dé lugar a ambigüedades. Denominación sistema = p. ej: "PLATAFORMA DE VALIDACION Y FIRMA ELECTRONICA. @FIRMA". (String UTF8) Size = 128 OID: 2.16.724.1.3.5.6.1.5</p> <p><b>Nombre de pila (titular del órgano)</b> N = Nombre de pila del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 OID: 2.16.724.1.3.5.6.1.6 Ej: "JUAN ANTONIO"</p> <p><b>Primer apellido (titular del órgano)</b> SN1 = Primer apellido del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 OID: 2.16.724.1.3.5.6.1.7 Ej: "DE LA CAMARA"</p> <p><b>Segundo apellido (titular del órgano)</b> SN2 = Segundo apellido del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 En caso de no existir el segundo apellido, se dejará en blanco (sin ningún carácter). OID: 2.16.724.1.3.5.6.1.8 Ej: "ESPAÑOL"</p> <p><b>Correo electrónico</b> Correo electrónico de la persona responsable del sello, p. ej: juanantonio.delacamara.espanol@mpr.es (String) Size [RFC 5280] 255 OID: 2.16.724.1.3.5.6.1.9</p>
<b>extendedKeyUsage</b>		clientAuth, emailProtection
<b>subjectKeyIdentifier</b>		Derivada del resultado de aplicar el hash a la clave pública del sujeto

Campos/Extensiones	Crítico	Contenido
<b>authorityKeyIdentifier</b>		Derivada del resultado de aplicar el hash a la Clave pública de la AC emisora
<b>certificatePolicies</b>		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.1.41233
cpsURI		http://policy.eadtrust.eu
userNotice		Ej: "Certificado cualificado de sello electrónico de Administración, órgano o entidad de derecho público, nivel alto. Consulte las condiciones de uso en " + URL de la DPC o, en su caso, documento legal de tercero
policyIdentifier		0.4.0.194112.1.3 (OID ETSI QCP-I-qscd)
userNotice		European Telecommunications Standards Institute. eIDAS European Regulation Compliant
policyIdentifier		2.16.724.1.3.5.6.1
<b>cRLDistributionPoints</b>		http://crl.eadtrust.eu/eadtrust-subca- <algoritmo><tamañoclave>eadlp<Año>.crl
<b>authorityInfoAccess</b>		
caIssuers		http://ca.eadtrust.eu/eadtrust-subca- <algoritmo><tamañoclave>eadlp<Año>.crt
ocsp		http://ocsp.eadtrust.eu
<b>basicConstraint</b>	Crítica	CA false
<b>qcStatements</b>		
QcCompliance		Indicación de certificado cualificado
QcType		id-etsi-qct-eseal
QcRetentiodPeriod		Integer:=15 ([ETSI EN 319 412-5] describe el periodo de conservación de toda la información relevante para el uso de un certificado, tras la caducidad de este) OID 0.4.0.1862.1.3
qcStatement-2		0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)
QcSSCD		
QcPDS		
<b>keyUsage</b>	Crítica	digitalSignature, nonRepudiation, keyEncipherment

## 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
<b>version</b>		3
<b>serialNumber</b>		Número positivo único
<b>signature</b>		Sha256WithRSAEncryption
<b>issuer</b>		Igual al campo Subject del certificado de la CA emisora
<b>validity</b>		1 año
<b>Subject</b>		
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
<b>subjectPublicKeyInfo</b>		RSA 1024 ó 2048 bits
<b>Extensiones</b>		
<b>authorityKeyIdentifier</b>		Derivada del resultado de aplicar el hash a la Clave pública de la AC emisora
<b>subjectKeyIdentifier</b>		Derivada del resultado de aplicar el hash a la clave pública del sujeto
<b>issuerAltName</b>		Igual al campo Subject Alternative Names de la CA Emisora
<b>subjectAltName</b>		email: ca@eadtrust.eu URI: http://www.eadtrust.eu URI: http://ca.eadtrust.eu URI: http://policy.eadtrust.eu
<b>certificatePolicies</b>		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.0.6960
cpsURI		<a href="http://policy.eadtrust.eu/cps">http://policy.eadtrust.eu/cps</a>
userNotice		European Agency of Digital Trust, S.L. OCSP Certificate
<b>OCSP No Check</b>		
<b>Basic Constraints</b>		CA false
<b>extendedKeyUsage</b>		OCSP Stamping
<b>keyUsage</b>	<b>Crítica</b>	digitalSignature

Este tipo de certificados se expiden para servidores OCSP externos. El servidor OCSP interno firma las respuestas OCSP con el certificado de la CA subordinada correspondiente.



## 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
<b>ISO 20000-1:2011</b>	10242586 / 10242587
<b>ISO 27001:2013</b>	10242584 / 10242585
<b>ISO 9001:2015</b>	10242588 / 10242589

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.

EADTrust ha diseñado una política específica de sellado de tiempo en la que se ofrece información detallada del servicio, por lo que se recomienda su lectura.

#### 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<sup>35</sup>.

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.

<sup>35</sup>RFC 5905 - Network Time Protocol Version 4: Protocol and Algorithms Specification

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:

- 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
- test de timestamp no cualificado 1.3.6.1.4.1.501.2.2.2
- test de timestamp cualificado 1.3.6.1.4.1.501.2.2.3

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

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

## 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<sup>36</sup>.

#### 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 entregan. Pueden acudir personalmente o través de un mandatario o apoderado. 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. Servicio 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 Reglamento 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.

---

<sup>36</sup> <https://www.boe.es/buscar/act.php?id=BOE-A-2010-10544>

### 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.

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

#### 11.1.1 Tarifas de emisión de certificados

---

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

#### 11.1.2 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.

### 11.2 Consideraciones de protección de datos de carácter personal

---

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

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

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

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

Los siguientes datos son considerados información privada:

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

- Cualquier otra información que pudiera identificarse como “Información privada”.

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

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

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

---

### 11.2.1 Consentimiento para usar datos de carácter personal

---

EADTrust S.L informa que los datos personales a los que tenga acceso en el marco de la prestación de sus servicios serán incorporados al registro de actividades de tratamiento del que es Responsable. EADTrust fundamenta el tratamiento de datos fundamentalmente en: el interés legítimo que tiene en responder solicitudes de información sobre sus servicios, la ejecución de un contrato o en el consentimiento expreso del titular del dato. Los titulares de datos pueden retirar ese consentimiento en cualquier momento.

Los datos recabados son los mínimos necesarios para la prestación de los servicios y se conservan por los períodos que establece la Ley. No se ceden a terceros, salvo obligación legal; ni se realizan perfiles o se toman decisiones automatizadas en base a estos datos.

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

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



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

### 11.2.2 Comunicación a terceros de datos de carácter personal

Los datos de carácter personal solo podrán ser comunicados a terceros, siempre que el titular del derecho lo consienta expresamente o por obligación legal de EADTrust.

### 11.3 Garantías de la CA

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

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

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

Las garantías del certificado incluyen:

1. **Derecho a usar el nombre de dominio o la dirección IP:** que, en el momento de la emisión, la CA (i) implementó un procedimiento para verificar que el Solicitante tenía derecho a usar o tenía control del Nombre/s Dominio/s y dirección/es IP que figuran en el campo Asunto del certificado y la extensión subjectAltName (o, solo en el caso de los Nombres de Dominio, se delegó tal derecho o control por alguien que tenía tal derecho para usar o controlar); (ii) siguió el procedimiento al emitir el Certificado; y (iii) con precisión describió el procedimiento en la Política de Certificación de CA y / o la Declaración de Práctica de Certificación;
2. **Autorización para el Certificado:** Que, en el momento de la emisión, la CA (i) implementó un procedimiento para verificar que el Sujeto autorizó la emisión del Certificado y que el representante del solicitante está autorizado a solicitar el Certificado en nombre del Sujeto; (ii) siguió el procedimiento al emitir el Certificado; y (iii) describió con precisión el procedimiento en la Política de Certificación de CA y / o la Declaración de Práctica de Certificación;
3. **Exactitud de la información:** que, en el momento de la emisión, la CA (i) implementó un procedimiento para verificar la exactitud de toda la información contenida en el Certificado (con la excepción del atributo subject: organizationalUnitName); (ii) siguió el procedimiento al emitir el Certificado; y (iii) describió con precisión el procedimiento en la Política de certificación de CA y / o la Declaración de práctica de certificación;
4. **Sin información engañosa:** que, al momento de la emisión, la CA (i) implementó un procedimiento para reducir la probabilidad de que la información contenida en el atributo del Certificado subject: organizationalUnitName es engañosa; (ii) siguió el procedimiento cuando

emitió el Certificado; y (iii) describió con precisión el procedimiento en la Política de certificación de CA y / o la Declaración de práctica de certificación;

5. **Identidad del solicitante:** que, si el Certificado contiene información de identidad del sujeto, la CA (i) implementó un procedimiento para verificar la identidad del Solicitante de acuerdo con las Secciones 3.2 y 11,2; (ii) siguió el procedimiento al emitir el Certificado; y (iii) describió con precisión el procedimiento en la Política de certificación de CA y / o la Declaración de práctica de certificación;
6. **Acuerdo del suscriptor:** que, si la CA y el suscriptor no están afiliados, el suscriptor y la CA son partes de un acuerdo de suscriptor legalmente válido y exigible que cumple estos requisitos, o, si la CA y el suscriptor son la misma entidad o están afiliados, el representante del solicitante reconoció los Términos de Uso;
7. **Estado:** que la CA mantiene un repositorio de acceso público 24 x 7 con información actual con respecto al estado (válido o revocado) de todos los Certificados no expirados; y
8. **Revocación:** que la CA revocará el Certificado por cualquiera de los motivos especificados en estos Requerimientos.

La 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.

#### 11.4 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 certificados/s solicitado/s (y cualquier dispositivo o datos de activación asociados, por ejemplo, contraseña o token)
3. **Aceptación del Certificado:** Obligación y garantía de que el Suscriptor revisará y verificará la exactitud del contenido del Certificado;
4. **Uso del Certificado:** Obligación y garantía de instalar el Certificado solo en servidores a los que se pueda acceder mediante el `subjectAltName` 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.

## 11.5 Responsabilidad contractual y extracontractual

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

### 11.5.1 Limitación de responsabilidad

EADTrust no asumirá responsabilidad alguna por los daños derivados o relacionados con la no ejecución o la ejecución defectuosa de las obligaciones del titular de un certificado.

EADTrust no será responsable de la utilización incorrecta de los Certificados ni de las claves, ni de cualquier daño indirecto que pueda resultar de la utilización de los Certificados.

EADTrust no será responsable de los daños que puedan derivarse de aquellas operaciones en que se hayan incumplido las limitaciones de uso del Certificado.

EADTrust no asumirá responsabilidad alguna por la no ejecución o el retraso en la ejecución de cualquiera de las obligaciones contenidas en esta DPC si tal falta de ejecución o retraso fuera consecuencia de un

supuesto de fuerza mayor, caso fortuito o, en general, cualquier circunstancia en la que no se pueda tener un control directo.

EADTrust no será responsable del contenido de aquellos documentos firmados electrónicamente por los titulares de certificados.

EADTrust no garantiza los algoritmos criptográficos ni responderá de los daños causados por ataques exitosos externos a los algoritmos criptográficos usados, si guardó la diligencia debida de acuerdo al estado actual de la técnica, y procedió conforme a lo dispuesto en esta DPC y en la normativa de aplicación.

---

### 11.5.2 Responsabilidades

---

EADTrust responderá en el caso de incumplimiento de sus obligaciones según se indica en el Reglamento (UE) 910/2014 del Parlamento europeo y del Consejo, de 23 de julio de 2014, y en la normativa reguladora de los servicios electrónicos de confianza, así como en la presente DPC.

EADTrust responderá por los daños y perjuicios que causen al firmante o terceros de buena fe cuando incumpla las obligaciones que impone el Reglamento (UE) 910/2014 del Parlamento europeo y del Consejo, de 23 de julio de 2014 y la próxima Ley reguladora de determinados aspectos de los servicios electrónicos de confianza.

La responsabilidad del prestador de servicios de confianza regulada en la ley será exigible conforme a las normas generales sobre la culpa contractual o extracontractual, según proceda, si bien corresponderá al prestador de servicios de confianza demostrar que actuó con la diligencia profesional que le es exigible siendo responsable de los perjuicios causados de forma deliberada o por negligencia a cualquier persona física o jurídica en razón del incumplimiento de las obligaciones establecidas en el Reglamento 910/2014.

Se presumirá la intencionalidad o la negligencia de un prestador cualificado de servicios de confianza salvo cuando el prestador cualificado de servicios de confianza demuestre que los perjuicios a que se refiere el párrafo primero del artículo 13 del Reglamento 910/2014 se produjeron sin intención ni negligencia por su parte.

Cuando EADTrust, como prestador cualificado de servicios de confianza, informe debidamente a los suscriptores con antelación sobre las limitaciones de la utilización de los servicios que presta y estas limitaciones sean reconocibles para un tercero, el prestador de servicios de confianza no será responsable de los perjuicios producidos por una utilización de los servicios que vaya más allá de las limitaciones indicadas.

De manera particular, EADTrust como prestador de servicios de confianza responderá de los perjuicios que se causen al firmante o a terceros de buena fe por la falta o el retraso en la inclusión en el servicio de consulta sobre la vigencia de los certificados electrónicos.

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

---

### 11.5.3 Entidad de registro

---

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

---

### 11.5.4 Responsabilidades del titular de los certificados

---

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

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

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**)<sup>37</sup>

Un certificado (en el sentido de instrumento que contempla la gestión de una clave privada) es un documento personal e intransferible emitido por EADTrust. Su titular está obligado a su custodia y la del código PIN o clave que habilita su uso, y es responsable de la conservación del mismo. No puede cederlos a otras personas.

---

## 11.6 Exención de responsabilidades de EADTrust

---

EADTrust no asume ninguna responsabilidad por perjuicios ocasionados en las siguientes circunstancias:

- En caso de guerra, catástrofes naturales o cualquier otro supuesto de caso fortuito o de fuerza mayor: alteraciones de orden público, huelga en los transportes, corte de suministro eléctrico y/o telefónico, virus informáticos, deficiencias en los servicios de telecomunicaciones o el compromiso de las claves asimétricas derivado de un riesgo tecnológico imprevisible.
- Ocasionados durante el periodo comprendido entre la solicitud de un certificado y su entrega al usuario.
- Ocasionados durante el periodo comprendido entre la revocación de un certificado y el momento de publicación de la siguiente CRL.
- Ocasionados por el uso de certificados que exceda los límites establecidos por los mismos y esta DPC.
- Ocasionado por el uso indebido o fraudulento de los certificados o CRLs emitidos por la infraestructura de Certificación de EADTrust.
- Ocasionados por el mal uso de la información contenida en el certificado.

---

<sup>37</sup>La norma RFC 6961 “TheTransportLayer Security (TLS) - MultipleCertificate Status RequestExtension” contempla múltiples respuestas, en el establecimiento de sesiones TLS, lo que permite validar los certificados de las CAs intermedias de la cadena de confianza.

- 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.

---

#### 11.6.1 Perjuicios derivados del uso de servicios y certificados

---

A excepción de lo establecido por las disposiciones de la presente DPC, y lo determinado por Ley, EADTrust no asume ningún otro compromiso ni brinda ninguna otra garantía, así como tampoco asume ninguna otra responsabilidad ante titulares de certificados o terceros que confían en los certificados.

---

#### 11.6.2 Seguro de responsabilidad civil

---

EADTrust cuenta con un Seguro de Responsabilidad Civil adecuado a sus actividades, según lo dispuesto en la normativa reguladora de los servicios electrónicos de confianza.

---

### 11.7 Enmiendas y cambios

---

---

#### 11.7.1 Procedimiento para realizar cambios

---

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

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

Las versiones actualizadas de la Declaración de Prácticas de Servicios Electrónicos de Confianza junto con la relación de modificaciones realizadas pueden ser consultadas en la dirección [www.eadtrust.eu](http://www.eadtrust.eu) y más concretamente en [www.policy.eadtrust.eu](http://www.policy.eadtrust.eu)

EADTrust podrá 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.

---

#### 11.7.2 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 Órgano Nacional de Supervisión
- Publicación 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 integren 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.

---

### 11.7.3 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 cambiará su OID.

---

### 11.8 Quejas. Reclamaciones y jurisdicción

---

En caso de una queja del usuario o de un tercero interesado, este podrá dirigir su queja al mail: [info@eadtrust.eu](mailto: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, 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](mailto:info@eadtrust.eu), indicando en el asunto que se trata de un recurso de apelación. También podrá emplearse la vía del correo postal.

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

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



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



## 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.<sup>38</sup>
- 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.<sup>39</sup>
- 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.<sup>40</sup>
- 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.<sup>41</sup>
- 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.<sup>42</sup>
- 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) 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.<sup>43</sup>
- 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.<sup>44</sup>
- 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,

<sup>38</sup><http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679>

<sup>39</sup><http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32014R0910&from=EN>

<sup>40</sup>[http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:JOL\\_2015\\_053\\_R\\_0006&from=EN](http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:JOL_2015_053_R_0006&from=EN)

<sup>41</sup>[http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:JOL\\_2015\\_128\\_R\\_0006&from=EN](http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:JOL_2015_128_R_0006&from=EN)

<sup>42</sup>[http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:JOL\\_2015\\_235\\_R\\_0001&qid=1441792087678&from=ES](http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:JOL_2015_235_R_0001&qid=1441792087678&from=ES)

<sup>43</sup>[http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:JOL\\_2015\\_235\\_R\\_0002&qid=1441792087678&from=ES](http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:JOL_2015_235_R_0002&qid=1441792087678&from=ES)

<sup>44</sup>[http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:JOL\\_2015\\_235\\_R\\_0006&qid=1441792087678&from=ES](http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:JOL_2015_235_R_0006&qid=1441792087678&from=ES)  
[Enlaces-Legislacion](#)

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].<sup>45</sup>

- 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.<sup>46</sup>
- 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.<sup>47</sup>

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.

En relación con la verificación de la identidad a distancia mediante videoconferencia:

- Real Decreto-ley 11/2020, de 31 de marzo, por el que se adoptan medidas urgentes complementarias en el ámbito social y económico para hacer frente al COVID-19
- Ley 10/2010, de 28 de abril, de prevención de blanqueo de capitales y de la financiación del terrorismo
- Real Decreto 304/2014, de 5 de mayo, por el que se aprueba el Reglamento de la Ley 10/2010, de 28 de abril, de prevención de blanqueo de capitales y de la financiación del terrorismo.
- Autorización SEPBLAC de 1 de marzo de 2016.

## 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.
- 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.

<sup>45</sup><http://www.boe.es/doue/2015/289/L00018-00025.pdf>

<sup>46</sup><http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016D0650&from=EN>

<sup>47</sup><https://www.boe.es/buscar/doc.php?id=BOE-A-2015-8048>

- Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (entrada en vigor: 2 de octubre de 2016).
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (entrada en vigor: 2 de octubre de 2016).
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de Derechos Digitales.
- Real Decreto-Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.

## 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<sup>48</sup> de EADTrust. En este enfoque, los servicios que se desarrollan por EADTrust enfatizan la gestión de identidades (eld) 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 el arco PEN 501

#### # 1.3.6.1.4.1.501 Spritel base OID

##### 13.2.2.1 Tabla de asignación de OID para el arco 2 (Policy)

<u>OID</u>	<u>Asignación</u>
2.0	Test
2.1	Certificate
2.2	Timestamping
2.3	Identity Management
2.4	Electronic delivery
<b>2.1.0</b>	<b>Non qualified Certificate</b>
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 Cert; key generated by USR
2.1.0.5	QSCD-based Cert; 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)
<b>2.1.1</b>	<b>Qualified Certificate</b>
2.1.1.0	non-QSCD QC; key generated by TSP
2.1.1.1	QSCD-based QC; key generated by TSP

<sup>48</sup> Secure Platform for Registered Identities and Trusted Electronic Ledger

<b>OID</b>	<b>Asignación</b>
2.1.1.1.2	non-QSCD server-based; key generated by TSP
2.1.1.1.3	QSCD server-based; key generated by TSP
2.1.1.1.4	non-QSCD QC; key generated by USR
2.1.1.1.5	QSCD-based QC; key generated by USR
2.1.1.1.6	non-QSCD server-based; key generated by USR
2.1.1.1.7	QSCD server-based; key generated by USR (non-available/reserved)
<b>2.2</b>	<b>Timestamping</b>
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

#### 13.2.3 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-creation devices. 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-semanticId-Natural -> **Natural person semantics** (para certificados de persona física – firma electrónica).
- 0.4.0.194121.1.2 -> id-etsi-qcs-SemanticId-Legal -> **Legal person semantics** (para certificados de persona jurídica – sello electrónico).
- 0.4.0.194112.1.0-> QCP-n->qcp-natural: certificate policy for European Union (EU) qualified certificates issued to natural persons.
- 0.4.0.194112.1.1-> QCP-l->qcp-legal: certificate policy for European Union (EU) qualified certificates issued to 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 public key 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.

#### 13.2.4 OID definidos en normas españolas de administración pública

Para los certificados de empleado público, de sello de órgano, de sede electrónica administrativa y para los de persona jurídica y representante, la Administración Española ha definido unos perfiles<sup>49</sup> 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.

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).

<sup>49</sup><https://administracionelectronica.gob.es/ctt/politicafirma/descargas>

- 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 Certificate 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 (Root CA y Sub-CA)

#### 13.3.1 EADTrust ECC 256 Root CA For Qualified Web DV/OV Cert 2019

```
-----BEGIN CERTIFICATE-----
MIICQDCCAeagAwIBAgIIUgcyMxmBF3kwCgYIKoZIzj0EAwIwYmVhbnRlbnR1eSBBBgNVBAMM
OkVBRFRydXN0IEVDQyAyNTYgUm9vdCBDQSBGbz3IgUXVhbGlnaWVkaWVlYiBEVi9P
ViBDZXJ0IDIwMTkxLzAtBgNVBAoMJKV1cm9wZWZuIEFnZW5jeSBvZiBEaWdpdGFs
IFRydXN0LCBTLkxwMQswCQYDVQGEwJFuzAeFw0xOTA2MDYxMTM1NTJaFw00MzA1
MzExMTM1NTJJaMIgDMUMwQQYDVQDDDPFQURUcnVzdCBFQ0MgMjU2IFJvb3QgQ0Eg
Rm9yIFF1YWxpZm1lZCBXZWlgaRfYvT1YgQ2VydCAyMDE5MS8wLQYDVQQKDCZFdXJv
cGVhbiBBZ2V1Y3kqb2YgRGlnaXRhbCBUcnVzdCwgUy5MLjELMAkGA1UEBhMCRVMw
WTATBgqhkJOPQIBBggqhkJOPQMBBwNCAASmsvUbofnnKs3E/Ax/DsRZeCTWd/se
MrM/afOWgFWh30mNWFmhNEZvT6sICq42qRM35y/avbTZRdrf9bxu6v+po0IwQDAP
BgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBBjAdBgNVHQ4EFgQUvCvHW+Nq
2n3RqEatR97jRcDD/bIwCgYIKoZIzj0EAwIDSAAwRQIgecIKoOw2jGf3xLbnBLXd
NCv1E5yqXefogNF10FlStkECIQc+5T1Tj1Ql4BKUk4QFehy4B96aDIH5WoVV+Fbu
dcOIFA==
-----END CERTIFICATE-----
```

#### 13.3.2 EADTrust ECC 256 Root CA For Qualified Web EV/PSD2 Cert 2019

```
-----BEGIN CERTIFICATE-----
MIICRDCCAeaggAwIBAgIIImMDVYeTMkgwCgYIKoZIzj0EAwIwYUxRTBDBgNVBAMM
PEVBRFRydXN0IEVDQyAyNTYgUm9vdCBDQSBGbz3IgUXVhbGlnaWVkaWVlYiBFVi9Q
U0QyIENlcnQgMjAxOTEvMCA0GA1UECgwmRXVyb3BlYW4gQWdlbmN5IG9mIERpZ210
YWwgVHJ1c3QsIFMuTC4xZCZAJBgNVBAYTAkVTMB4XDTE5MDYwNjE5eXNDkyNFoXDTQz
MDUzMTExNDkyNFowYUxRTBDBgNVBAMMPEVBRFRydXN0IEVDQyAyNTYgUm9vdCBD
QSBGbz3IgUXVhbGlnaWVkaWVlYiBFVi9QU0QyIENlcnQgMjAxOTEvMCA0GA1UECgwm
RXVyb3BlYW4gQWdlbmN5IG9mIERpZ210YWwgVHJ1c3QsIFMuTC4xZCZAJBgNVBAYT
AkVTMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAE0EISu3kfw9Uasnh4Y7vNtkWG
UvCkCAA45lWFPbvIH668463fRfObNL9jCuRryOAj5ws2/XnVx03P/iEBhCvsNKNC
MEAwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFNN3
zVrao5Nci0pMZdKaDAHVMt8TMAoGCCqGSM49BAMCA0gAMEUCIQDxOmhZS7u3F1KC
tGQDCDs0rzvaw9mO03YP/Y0GSi2JQAIgdwgCgMc42H3u2Apo7uubqUIIY+Ebo3MT
```



9wwf4X0aTRg=  
-----END CERTIFICATE-----

---

### 13.3.3 EADTrust ECC 256 Root CA For Qualified Certificates 2019

---

-----BEGIN CERTIFICATE-----  
MIIC2TCCAn+gAwIBAgIIIVIg0cUCCeFAwCgYIKoZIzj0EAwIwZSsxQTA/BgNVBAMM  
OEVBFRydXN0IEVDQyAyNTYgUm9vdCBDQSBG3IgwUXVhbG1maWVkiENlcnRpZmlj  
YXRlc3YyMDE5MS8wLQYDVQQKDCZFdXJvcGVhbiBBZ2VuY3kgb2YgRGlnaXRhbCBU  
cnVzdCwgUy5MLjELMAkGA1UEBhMCRVMxGDAwBgNVBGE1ZBVEVTLUI4NTYyNjI0  
MDAgFw0xOTA2MDYxMTIzMTFaGA8yMDUxMDUyOTExMjMxMVowZSsxQTA/BgNVBAMM  
OEVBFRydXN0IEVDQyAyNTYgUm9vdCBDQSBG3IgwUXVhbG1maWVkiENlcnRpZmlj  
YXRlc3YyMDE5MS8wLQYDVQQKDCZFdXJvcGVhbiBBZ2VuY3kgb2YgRGlnaXRhbCBU  
cnVzdCwgUy5MLjELMAkGA1UEBhMCRVMxGDAwBgNVBGE1ZBVEVTLUI4NTYyNjI0  
MDBZMBMGBYqGSM49AgEGCCqGSM49AwEHA0IABCmRZ006jBfLIwYCHIDiBAMTbiue  
EHu7uBeWlfSEFE1OSrHSAYShQgX9Z5BxGxNIXblTlrjdmRYTvgYzDzy1s3yJgagw  
gaUwDwYDVR0TAQH/BAUwAwEB/zA0BgNVHQ8BAf8EBAMCAQYwYwYDVR0RBFwwWoeO  
Y2FAZWFkdHJlc3QuZXZGFmh0dHA6Ly93d3cuZWZkdHJlc3QuZXZGFWh0dHA6Ly9j  
YS5lYWw0cnVzdC5ldYYZaHR0cDovL3BvbG1jeS5lYWw0cnVzdC5ldTAdBgNVHQ4E  
FgQUAWeahMSZxoHtPFgEdK8ko9deQQ0wCgYIKoZIzj0EAwIDSAAwRQIGDt6bdlhA  
NUyIgwUbwq7b7DsQ8/aGGpr3n96x4fwZdLUCIQCEPIqtElTsfjc0kc8fW5/LVZ+  
ZTomWaLy4q7/TaBxkA==  
-----END CERTIFICATE-----

---

### 13.3.4 EADTrust ECC 384 Root CA For Qualified Web DV/OV Cert 2019

---

-----BEGIN CERTIFICATE-----  
MIICfjCCAgOgAwIBAgIIQkhkc3QlBBIwCgYIKoZIzj0EAwMwgYMxQzBBBgNVBAMM  
OkVBRFRydXN0IEVDQyAzODQgUm9vdCBDQSBG3IgwUXVhbG1maWVkiFdlYiBEVi9P  
ViBDZXJ0IDIdIwMTkxLzAtBgNVBAoMJKv1cm9wZWZuIEFnZW5jeSBvZiBEaWdpdGFs  
IFRydXN0LCBTLkwuMQswCQYDVQQGEWJFUzAeFw0xOTA2MDYxMTM1NTVaFw00MzA1  
MzExMTM1NTVAMIGDMUMwQQYDVQQDDDFURUcnVzdCBFQ0MgMzg0IFJvb3QgQ0Eg  
Rm9yIFFlYWxpZm1lZCBXZWlgrFYvt1YgQ2VydCAyMDE5MS8wLQYDVQQKDCZFdXJv  
cGVhbiBBZ2VuY3kgb2YgRGlnaXRhbCBUcnVzdCwgUy5MLjELMAkGA1UEBhMCRVMw  
djAQBgcqhkJOPQIBBgUrgQQAIGNiAAS7oySQYb7uQT6YONuFW8H+DKiMY3K5eaRE  
IRYQiYdfvM52nDrMGI3ne422tQXthT3LNaWK+JYvPiO5S+0tkJnPMVN/FcS2YmOx  
ad9E5LUI9yCX+6IglT8c7rTM/SjEE2ujQjBAMA8GA1UdEwEB/wQFMAMBAf8wDgYD  
VR0PAQH/BAQDAgEGMB0GA1UdDgQWBQc1NgSlE1/161Dcbsusroz0sD0RjAKBggq  
hkjOPQDAwNpADBMAjEAU/UWR15XlmtGSSmGBkNw4u5i/pXvdDW9pn8dGw4RBie  
wb75uu50eH0xxrdv8pInAjEAix9xKDwCNClzYZDGLMFvldSG3PlsJqgJ6pB9kOwV  
Ono9W0VX13P+QB9G4ixZ4j0B  
-----END CERTIFICATE-----

---

### 13.3.5 EADTrust ECC 384 Root CA For Qualified Web EV/PSD2 Cert 2019

---

-----BEGIN CERTIFICATE-----

```
MIICgTCCAgigAwIBAgIJAJBWAHV3mAKHMAoGCCqGSM49BAMDMIGFMUuwQwYDVQQD  
DDxFQURUcnVzdCBFQ0MgMzg0IFJvb3QgQ0EgRm9yIFFlYWxpZml1ZCBXZWIGRVYv  
UFNEMiBDZXJ0IDIwMTkxLzAtBgNVBAoMJkV1cm9wZWFuIEFnZW5jeSBvZiBEaWdp  
dGFsIFRydXN0LCBTLkwwMQswCQYDVQQGEwJFUzAeFw0xOTA2MDYxMTQ5MjZaFw00  
MzA1MzExMTQ5MjZaMIGFMUuwQwYDVQQDDEdDxFQURUcnVzdCBFQ0MgMzg0IFJvb3Qg  
Q0EgRm9yIFFlYWxpZml1ZCBXZWIGRVYvUFNEMiBDZXJ0IDIwMTkxLzAtBgNVBAoM  
JkV1cm9wZWFuIEFnZW5jeSBvZiBEaWdpdGFsIFRydXN0LCBTLkwwMQswCQYDVQQG  
EwJFUzB2MBAGByqGSM49AgEGBSuBBAAiA2IABJwJZC1Pg5KoeHhGqUtuv8o8DUYD  
+FuNm4szFz+stoo6Bn8IQjBQaRdj+BXP008keggIoKjeKUfaOGebcot2BLirNhYo  
u5xbN6fsVCoerHfAFz5/pOev4FQRh/m4pHaicaNCMEAwDwYDVR0TAQH/BAUwAwEB  
/zA0BgNVHQ8BAf8EBAMCAQYwHQYDVR0OBByEFOrpUOSzk0k/BQQ1pfBHVx+XhEZ  
MAoGCCqGSM49BAMDA2cAMGQCMBBxKbl4mBx9pWki6DLVPCSloHBSSM7kdPpXUwQY  
v9kCEBnkt5kF8ZFYGbinSSkKDQIwa7qPHhRyKSDD2X1hCQKtauv5FT3ufStwDOQP  
33uSJ7F8aprXuUd2t0bFdIvWKRWz  
-----END CERTIFICATE-----
```

---

### 13.3.6 EADTrust ECC 384 Root CA For Qualified Certificates 2019

---

```
-----BEGIN CERTIFICATE-----  
MIIDFzCCApYgAwIBAgIIJ5cWUAlhiIgwCgYIKoZIzj0EAwMwgZsxQTA/BgNVBAMM  
OEVBFRydXN0IEVDQyAzODQgUm9vdCBDQSBG3IgwUXVhbGlmaWVkiENlcnRpZmlj  
YXRlc3YyMDE5MS8wLQYDVQQKDCZFdXJvcGVhbiBBZ2VvY3kgb2YgRGlnaXRhbCBU  
cnVzdCwgUy5MLjELMAkGA1UEBhMCRVMxGDAWBgNVBGEMD1ZBVEVTLUI4NTYyNjI0  
MDAgFw0xOTA2MDYxMTIzMTVaGA8yMDUxMDUyOTExMjMxNVowZSsxQTA/BgNVBAMM  
OEVBFRydXN0IEVDQyAzODQgUm9vdCBDQSBG3IgwUXVhbGlmaWVkiENlcnRpZmlj  
YXRlc3YyMDE5MS8wLQYDVQQKDCZFdXJvcGVhbiBBZ2VvY3kgb2YgRGlnaXRhbCBU  
cnVzdCwgUy5MLjELMAkGA1UEBhMCRVMxGDAWBgNVBGEMD1ZBVEVTLUI4NTYyNjI0  
MDB2MBAGByqGSM49AgEGBSuBBAAiA2IABJpUpFLZZZkWHv7hxNgamqv9q1L4uZZc  
/TFfnrnJEBoXssZyad/kLD+906Watn5F8e5PhwufanG6wTMD4SEuPH9vC8xmb1+m  
aKUtEJBGF9p16q1RdM8Sg+9oHlulZz73jaOBqDCBpTAPBgNVHRMBAf8EBTADAQH/  
MA4GA1UdDwEB/wQEAwIBBjBjBgNVHREEXDBagQ5jYUBlYWR0cnVzdC5ldYYWahr0  
cDovL3d3dy5lYWR0cnVzdC5ldYYVaHR0cDovL2NhLmVhZHRydXN0LmV1hhlodHRw  
Oi8vcG9saWN5LmVhZHRydXN0LmV1M0GA1UdDgQWBRR4FP3u0QlgXHWnZ24mSIHk  
6sSSATAKBggqhkjOPQQDAwNpADBMAjEApEqkKNMGW8neYsXLzPy2XytMX9Jf7oxN  
Z7I1oonC4XXl0cDVsw5u4KP02+CO0/trAJEA29yWuzRywABtXZlVisrvsSJAHFvC  
E/WD7KUyKb4inlL9R7ssEt6VrzpYdqDLyiqn  
-----END CERTIFICATE-----
```

---

### 13.3.7 EADTrust RSA 2048 Root CA For Non-Qualified Certificates 2019

---

```
-----BEGIN CERTIFICATE-----  
MIIEbzCCAlegAwIBAgIIUWVJVGfYGTAWDQYJKoZIhvcNAQELBQAwwAaxrjBEBGnV  
BAMMPUVBRFRydXN0IFJFTQSAyMDQ4IFJvb3QgQ0EgRm9yIE5vbi1RdWFSaWZpZWQg  
Q2VydGlmaWVhdGVzIDIwMTkxLzAtBgNVBAoMJkV1cm9wZWFuIEFnZW5jeSBvZiBE  
aWdpdGFsIFRydXN0LCBTLkwwMQswCQYDVQQGEwJFUzAeFw0xOTA2MDYxMTQ5MjZaFw00  
MzA1MzExMTQ5MjZaMIGFMUuwQwYDVQQDDEdDxFQURUcnVzdCBFQ0MgMzg0IFJvb3Qg  
Q0EgRm9yIFFlYWxpZml1ZCBXZWIGRVYvUFNEMiBDZXJ0IDIwMTkxLzAtBgNVBAoM  
JkV1cm9wZWFuIEFnZW5jeSBvZiBEaWdpdGFsIFRydXN0LCBTLkwwMQswCQYDVQQG  
EwJFUzB2MBAGByqGSM49AgEGBSuBBAAiA2IABJwJZC1Pg5KoeHhGqUtuv8o8DUYD  
+FuNm4szFz+stoo6Bn8IQjBQaRdj+BXP008keggIoKjeKUfaOGebcot2BLirNhYo  
u5xbN6fsVCoerHfAFz5/pOev4FQRh/m4pHaicaNCMEAwDwYDVR0TAQH/BAUwAwEB  
/zA0BgNVHQ8BAf8EBAMCAQYwHQYDVR0OBByEFOrpUOSzk0k/BQQ1pfBHVx+XhEZ  
MAoGCCqGSM49BAMDA2cAMGQCMBBxKbl4mBx9pWki6DLVPCSloHBSSM7kdPpXUwQY  
v9kCEBnkt5kF8ZFYGbinSSkKDQIwa7qPHhRyKSDD2X1hCQKtauv5FT3ufStwDOQP  
33uSJ7F8aprXuUd2t0bFdIvWKRWz  
-----END CERTIFICATE-----
```

```
QVRFUy1CODU2MjYyNDAwggEiMA0GCSqGS1b3DQEBAQUAA4IBDwAwggEKAoIBAQC2
6Guzxu4fwaJwcrUUvfbHKJewhuRrvicFNohy5x2cTgu8/X5R9Etb+KlOJl5JGkW8
i/05VFebp4Fq1c99Ia3GAzSbJXSw6yo0Yj5qBR6L81WHCMflpYlZqB7IL6iPfYfj
nR8ukVxsmeAAVsP2+7y/KnjoIdhQC7SL7XQ522kYZ1bNZSXFpStH+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
AiqNzAGhDnHEayPTFH1fdyMKwLH5JzX1R0D/lfEk0UWYS1cgF0xPLzRP/OZHDiMY
3S9Jiuzy9bJNUfEbOy9vzfN/kKwgAiz+Yq7nI+LY6XALriqwI83Puv05yEBXPmGD
BaVwUIbSLz/WqfWkFiZ97zK+KmAzwkoyAHVKgFy44OWCPRVjJm/8QY/9bDFspUX1
h/li6Lb9ARdsTIHLuHMT3TdTqTdJy/iAeTyy+6DfgTV5g1k=
-----END CERTIFICATE-----
```

### 13.3.8 EADTrust RSA 2048 Root CA For Qualified Certificates 2019

```
-----BEGIN CERTIFICATE-----
MIIEZzCCA0+gAwIBAgIIU2BoCBlIgyQwDQYJKoZIhvcNAQELBQAwgZwxQjBBAgNV
BAMMOUVBRFRydXN0IFJTSAAyMDQ0IFJvb3QgQ0EgRm9yIFF1YWxpZml1ZCBkZXJ0
aWZpY2F0ZXMGmJAxOTEvMC0GAlUECgwmRXVyY3B1YW4gQWdlbmN5IG9mIERpZ210
YWwgVHJ1c3QsIFMuTC4xCzAJBgNVBAYTAkVTMRgwFgYDVQRhDA9WQVRFUy1CODU2
MjYyNDAwIBcNMtKwNjA2MTA1NjE4WhgPMjA1MTA1MjkxMDU2MThaMIGCMUIwQAYD
VQDDDDlFQURUcnVzdCBSU0EgMjA0OCBSb290IENBIEZvcjBRdWFSaWZpZWQgQ2Vy
dGlmawNhdGVzIDlwMTkxLzAtBgNVBAoMJKV1cm9wZWZuIEFnZW5jeSBvZiBEaWdp
dGFsIFRydXN0LCBTLkxwMQswCQYDVQGEwJFuzEYMBYGA1UEYQwPVkFURVmtQjg1
NjI2MjQwMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAXH50WSvmyaP2
TqEN/WI6VtuYjI5TjHaotSjgUGz72z0Z1da7liX082iF/JGcvIovMbb0ayUNULz1
ezKkoTxCvPzNobvNFRxPtkySAS5BVtxoD/0xZlgMwsyse892rEl/FIOiUucPzc2
HxWB10dDAhxhYlWcBAecs jYA0czh98s2uln1WPAinFBcr0wmWD3P5qfz8TCzpk4r
4NstZFeg+ScdYbXLzcCGGU33V+8yEsMzppUyztRbtJrwpD/k/yumIXtStbWXup+d
Snbi5JiUhcTn3hXipjypIu3VFRBFzXY8Be6IVjpr24GG7tDVHyhbvJONGCK5CjD
umhFVOMS9QIDAQABO4GoMIG1MA8GA1UdEwEB/wQFMAMBAf8wDgYDVR0PAQH/BAQD
AgEGMGMA1UdeQRcMFqBDmNhQGVhZHRydXN0LmV1hhZodHRwOi8vd3d3LmVhZHRy
dXN0LmV1hhVodHRwOi8vY2EuZWfkdHJ1c3QuZXWGGWh0dHA6Ly9wb2xpY3kuZWfkdHJ1c3QuZXUwHQYDVR0OBBYEFB/Ua7BjhgwLCYxCbjPdeh0UMSuZMA0GCSqGS1b3
DQEBCwUAA4IBAQC/7aPGae9raByQdwTQCrfJZB8NCyKxWP847BGznHFh83k9hH4D
gQay13qnFRF7cxhv7DZ9p7u0Rrn89HQGEDp9zzlu3+PBa5rhh4ftZmAk5qL/0Wws
0IYZjwfuns+AnfUZdroLtWsVqpN0sgzrR73Rks00h2L1/Xm+1blPB8bcJcu0siaT
5BW6yb+sD/Whal5lZVayNcSX6vF5g0Ooxjeojk2e1offACMAhpy5iTWW1jtcjpf3
R4F62ITsOdTtWzshdu7Bi4bHHwbSoLDlxLZmgmiZBg8In1EA0qb5zCR5Cdsy4w+6
Vi9PBz6ImVmgJmvsv+ojGjHpv0vCdU9ML/1j
-----END CERTIFICATE-----
```

13.3.9 EADTrust RSA 4096 Root CA For Qualified Web DV/OV Cert 2019

```
-----BEGIN CERTIFICATE-----
MIIFzjCCA7agAwIBAgIIaUgRCwiBiBUwDQYJKoZIhvcNAQELBQAwwYQxRD8CBgNV
BAMMO0VBRFRydXN0IFJ0QSA0MDk2IFJvbn3QgQ0EgRm9yIFF1YWxpZmllZCBBZWIg
RFYvTlYgQ2VydCAyMDE5MS8wLQYDVQKDCZFdXJvcGVhbiBBZ2VuY3kgb2YgRGl
aXRhbCBUCnVzdCwgUy5MLjELMAkGA1UEBhMCFRVwHhcNMTkxMzA2MTEyMzUyLj
NDMwNTMxMTEyMzUyLjNDMwNTMxMTEyMzUyLjNDMwNTMxMTEyMzUyLjNDMwNTMx
MTEyMzUyLjNDMwNTMxMTEyMzUyLjNDMwNTMxMTEyMzUyLjNDMwNTMxMTEyMzUy
dCBDQSBGb3IgUXVhbGlmaWVkiFdlYiBEVi9PViBDZXXJ0IDIWMTkxLzAtBgNVBAoM
JkV1cm9wZWVUeUFnZW5jeSBvZiBEaWdpdGFsIFRydXN0LzCBTLkwmQSwCQYDVQ
EwJFUzCCAiiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgCggIBALwsCMbnfiu95vK8
pyDOIGJAJegch7EURLP979Fxtyz47Tb5GSLO81tGW6ncwTFYtQKh6UMSiL0+tW44
QM9DLYWu3kSvAQPxiImFKQIkkZPxnOQ7X35EGWdQ5R/Z10aX7x0kwu9hGS+FwBQ
tTPHWR7t7GpNbmFu/qggL3tbTDZRQHP1EgpQWkND4CGLXS452CXpymNg36/NMKU
3kL0DCoWno02SUMtbehIwCwPZknWNFbGdXE3AZVUFDHRk8JXRQug+G5Ma7gMQ+Dy
TG6vWM0UVSlRpEmUXvD6EJ6te3g9+L5uSUkJ5HNlUAK4nCzi560/ek6b5ga+Tuit
MtlCN+exp+vnXTy4eXDjwrfNUS4dc0pzn3nVR7uuJ/vrWPDHqjdZiWb2pMQ9qy
rcG1hmz2lHQWPx+MeTwtfDniDYeFYsOvv2bBEakeTGq5qRdx32vNseKabhC4qsJL
HP20700hiqwJkPaolS/8JdhwIvsOr0ao8EY/vx3A37S3ixPzIz+J6PfuOwx3Taqrl
K3zmHXamu7l2NFaPygxecU7LbVu6xwxs0HT8Ch2bvjLTLW2pc112XxdrQ1lbm83jT
qAlMcGNGKjH7Yma7sI+T5ToUyF1Lb6xLnFkMW15Fmz1sDKdWUvAYt4oLkgQi4Erp
TgtYSpWFUtTqVDRYp2HS1PsvBEkVAgMBAAGjQjBAMA8GA1UdEwEB/wQFMAMBAF8w
DgYDVR0PAQH/BAQDAgEGMB0GA1UdDgQWBBS2xXmeFhyF2VI dyxzSiMUysya8NRzAN
BqkqhkiG9w0BAQsFAAOCAgEAAdajcm8hyZIMZXHdzFbmSGm8KtjzT7wPNytf79ajU
QBA1vT3X9EnlEVROZfHAecbn4qLHvp3oZ9MQzUP/QRqZsJKNzBzkHiNCDAB5GLdj
cx5GBD23YuEPhxgt0uWf0xCBH9SGQiSMS+KBD2XTbwOPOWQ2fdJ7VnI/lorVks17
Hkk+SD9rycRyPJu4nnl3pqsHqsBGtdLKCyluw0x0bvVGHdGEf0nSdmzSHJMn/rpb
ka9EoMIV3IiirkC2coXSmkyasyhmI3EiMwYyTnI08262cF1sIwftH7VAW+p2H1tj
h8kZZT7bm9HyMfNGCUXWKR+QeAVZl/Wgi+luxuxsqigiLOiWTG2jPriuIlu0ujDG
TbtQnc1Reig0ImTmfy844e+7uGJVzQHl649YU1+OZS8S1mLgNB8fC416qj70xmLs
t/kTU4zj6PrwqaNkSiI8446A4TsC789SXqK6pEqs9GvJvPZS/mESNytjyIwZbVup
nqGDqbmQNhrVos++aQEtEnWkLw4mHGwqJBiw7xWVCNEv4R/vhywFLjaruSThwRi
O2siulXBgAmP7yHu3Nh/Np8h9HvQyE6/tVEvecex04xOLCY5H3Rs6l2nxfxxEbyM
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-----
MIIF0zCCA7ugAwIBAgIIAJSCBgEgJCdbMA0GCSqGSIb3DQEBCwUAMIGGMUYwRAYD
VQDDDD1FQURUCnVzdCBSU0EgNDA5NiBSb290IENBIEZvciBRdWFSaWZpZWQgV2Vi
IEVWl1BTRDIgQ2VydCAyMDE5MS8wLQYDVQKDCZFdXJvcGVhbiBBZ2VuY3kgb2Yg
RGlnaXRhbCBUCnVzdCwgUy5MLjELMAkGA1UEBhMCFRVwHhcNMTkxMzA2MTEyMzUy
LjNDMwNTMxMTEyMzUyLjNDMwNTMxMTEyMzUyLjNDMwNTMxMTEyMzUyLjNDMwNTMx
MTEyMzUyLjNDMwNTMxMTEyMzUyLjNDMwNTMxMTEyMzUyLjNDMwNTMxMTEyMzUy
Um9vdCBDQSBGb3IgUXVhbGlmaWVkiFdlYiBFVi9QU0QyIENlcnQgMjAxOTEvMC0G
A1UECgwmbXVyb3BlYW4gQWdlbmN5IG9mIERPZ2l0YWwgVHJlcnQsIFMuTC4xCzAJ
BgNVBAYTAkVUaWJicjANBgkqhkiG9w0BAQEFAAOCAg8AMIICcGKCAGEAqd1bZClu
b8Oc7Ehs6nPuqjmVkuNbFWXNPiBtPg74gNGtO1GpKcz2C2b46Numxn1zjL7HVTfv
ovd1MvVpq9erz1PTV+KeeuNHXeXmWbleQNT2uCPLnlnf1hPIs2QL8/66WtueLTQ0
```

EjygIbLEgAAGEniFwch0GTNHPWoIOmTOfXnurpvXYI1w0f2vM3p5LeRD/wVD6v3D  
I0on20/JcXltdsGbucKxRa65mzkGfc7ARrMKer0gJDEFaLigvd+CFbcqpxB/kk2u  
6qxA/IhsIYZ3vly+EaVXhm0h05WMvC2XeW+lxguavsw2n+ru0Hl jcnBJh9Np0WKe  
3Tr4RU+ZDvOodrfUM9B84P/FPhvpTYqHwmdjm3lVdl3qMI5fyasTBeFJKWojybch  
mEFrwFP+VTy5fCh5j9mt682PonMbgxxQGX9Uqy0qzo0x62fSiXzPAoTRJdd6RfY7  
fNm64gndW09Rn9j4LLuGoyf16yFsfv5SutiJMK9j1tsaVc0Y4x9ec7QA+58cLMM  
yZWfTEoJ8fZv6CUycBv4WldTzza/HP9FTDjQmbHqdBw0bsSyzN37M6dgdR5+TQ1A  
Lf6VocYEMct8YDZ8nHe2waBYix4fKlKi//nnpJTtPp07v1Ptp13zpOd/sOep2bus  
IWg3FcODltY0jQw5533Yf/i/QcMz/Y6ApHcCAwEAAaNCMEAwDwYDVR0TAQH/BAUw  
AwEB/zAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFLLQeKNTqqmAPEAR0y3eUaUwR  
h+JEMA0GCSqGSIB3DQEBcWUAA4ICAQBcWYyYcusmGs jmtaZU9Y6w8FHPQ9yJUNWg  
9gKykaYKcEPv/AJf6tINI1nh7si22kGYS5PpVx6wcNdnUjOmFzpwErAQIzdb6kkg  
5LDe19xAD2fsgMb/zV0Xa6ZcEJyimp74uaXCdGFHqUwhFyusS9HSWhnSURiO1zzk  
cZ1AgyKllm8e/RndiY8gvD+TXUDkVGFimtF26zCUtgaO1Fzul+mi/ShfJfrSnpGx  
qn2zoCCpImefkRpz/7YseQDcnJ7sYAPxveM+b0C6vk5VH9B5bkSWdLZ+dSjLgp1p  
HAAGTLyn4GXt8JYSp0CNz jeqBMJVAGCXPqmGloDFIg+IecLZdTZRtdaIr3pnD0jB  
hrZ/WyxuFFlCXsNgTfcqZK2LS2yY5drfNu+zyTgg4XtAzkq0Wbn2JNCjxihz16no  
EldaenDtCNqFofXFK8gItFTwxHBh18H7dkQmyiZe4qvWT8qvU08VzJfAuQ7aEALC  
lmGJR4wGo7h/QL0iMV9MiiTlBkDK9M3cboH9UV8uEHFVVM5NkDhFhXwDBo5s85Ix  
bIKkfZBvoesJ2yveTElWGztSED3JzCsIU7GH01JdW9MMjJFGrY2/s35/+KLSosgn  
WlKAJX8Lg61JQER4PNWh5bUEl1gN3HYd75bLdEXlwb1MEbuoHfhi7CtsjrHf7G+v  
lhVDgRGPCA==  
-----END CERTIFICATE-----

### 13.3.11 EADTrust RSA 4096 Root CA For Qualified Certificates 2019

-----BEGIN CERTIFICATE-----  
MIIGZzCCBE+gAwIBAgIIIIQ1JZjUjzJIwDQYJKoZIhvcNAQELBQAwZwQjBABgNV  
BAMMOUVRFRydXN0IFJTSQA0MDk2IFJvb3QgQ0EgRm9yIFFlYWxpZmllZCBZDZl0  
aWZpY2F0ZXMGmJAxOTEvMCA0GAlUECgwmRXVyb3B1YW4gQWdlbmN5IG9mIERpZ2l0  
YWwgVHJlc3QsIFMuTC4xZCzAJBgNVBAYTAKVTMRgwFgYDVQRhDA9WQVRFUy1CODU2  
MjYyNDawIBcNMtkwnJA2MTA1NjMzWWhgPMjA1MTA1MjMzMDU2MzNaMIGCMUIwQAYD  
VQOQDDdlFQURUcnVzdCBSU0EgNDA5NiBsB290IENBIEZvcjBRdWFSaWZpZWQgQ2Vy  
dGlmawNhdGVzIDIwMTkxLzAtBgNVBAoMJKV1cm9wZWZuIEFnZW5jeSBvZiBEaWdp  
dGFsIFRydXN0LCBTLkwuMQswCQYDVQGEwJFuzEYMBYGA1UEYQwPVkFURVmtQjg1  
NjI2MjQwMIIICjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAQYfy0Vrc8SK  
L6Saw5s1UQ4CztHwWDmyHKp5otL/7Ldp6i1R6CDW/Nd2E4Pfd5HCms5tql6c6qk  
npNheWlHrMOWCxoJagcuDfa3ISmEpLtnNqvOlJTF2sBevzRNhFSdrEEsGJ4W6Or  
7diR495e5DlnifF3LI/vPIk8RLEPGMnp74fcrPM2ML28Nx9VvhvzhsYsiGFNZKgw  
e3nqueAUC3TIUi/d8js+VS4Bty1BlzFD3VrstQ14NACTQN11DQB9TN07XyOyP7A8  
f+GWNs7LCy01Y01pk8X/jcz4RkBXAYETy6QNr/ome+abmSs7Nu7JVa6TCy1cXQgC  
B5InQD18V077wFvH0WidkLJvN5MqO2MyVkzVzFk8q3CeVcWj8c8f0wYtptU3SNiN  
QyVkah1AFyaMt4spancQjTY/eQ1jf5wjtQdnC48AJtgp46bbt0HAYEMgx6JWpkJ  
7GRr5REL+rqrTFZNPWqs1+nrcXS3NeZSgrtWKxDAA3w9t+aC/19HrwAAAXH8MnB5  
Ym8+0z50YEMTI9GNS4lbkDZe5DvkwYldxIawBhdXGWTfifG1Puz5TGr0k4h85ko9  
EusOCs2Ix8CGL3Y5dSdKWMPkAerVRuclwG0eLP+wCKf5jPo2RFjC6qcUIqGFJsS8  
U15iJmYGkqpxRvq9EpKkmduhIeahOIkCAwEAAaOBqDCBpTAPBgNVHRMBAf8EBTAD  
AQH/MA4GA1UdDwEB/wQEAwIBBjBjBgNVHREEXDBagQ5jYUB1YWR0cnVzdC5ldYYW  
aHR0cDovL3d3dy51YWR0cnVzdC5ldYYVaHR0cDovL2NhLmVhZHRydXN0LmV1hhlo  
dHRwOi8vcG9saWN5LmVhZHRydXN0LmV1MB0GA1UdDgQWBBTjwja0RwPADxeyY7BQ  
E+UUsQxZ9DANBgkqhkiG9w0BAQsFAAOCAgEAgMlFhhM2dRMxE8v14Rkq7X1MI0t9

```
t0DwJnxGZZLZaAX+FgzggHNWygWUbSeGZDrYQP/ulrWWffsGvCmd7WioRHhHzLs8
N9tr5cToapCElfoh7L++Cx8yVRP9dkoAgKeCAfDsg3uLcLlnn+32NFXD3sFkhBMY
8FbP1MOFNFYFQ0pMm9rbsLMR27qyCPyBt1kLjJX1y1RJVmp9Q9Isc9LOpcG7rSf
T41IH/NOa2RdfZXL0yuYGVHyPnREvGamI17OGXVWvirmpfWKvdMPi1Z12mEktOLn
paXBbrAHHjtGgB3wT8ujTo8TkV0nEWrlrpuqjd+mo8Nd2OqGk5Rya8yQ93OFuMT+
fHbdCEs0M7xy7DNeoAEuQIFVmc2FpeYhmc6ZSPzFCjey/8ojWz7+zLRqlnmjIcwr
m7cLDgKmNoNOWy5HM0XEAZtzn57sgE7LLQICWSdZGpi7OE8K+hWqzV0L5v36hOm
cr9udcjcW9u83VuusPp/OuKLyRXiqRobYOZbpM/1wQI1G8csuaq118R3BWxDeUR6
SiGZVfx8xTlxCGIbG2udvuBrExntPIhFdWi7VjiIOQkI7lvYwLprCvhbRYD9Sm1R
19kIyD3eE2esLEPto0bLu3AETQtcadOQZqsQG+qLmzZfU3KTRzvbaHTAK4Y5qE+U
CmHHuZU44qXdGEI=
-----END CERTIFICATE-----
```

### 13.3.12 EADTrust RSA 8192 Root CA For Qualified Web DV/OV Cert 2019

```
-----BEGIN CERTIFICATE-----
MIIEJzJCCBbagAwIBAgIINpRQh3QHYYJYwDQYJKoZIhvcNAQENBQAwYQxRDBCBgNV
BAMMO0VBRFRydXN0IFJFTQSA4MTkyIFJvb3QgQ0EgRm9yIFF1YWxpZml1ZCBXZWIG
RFYvT1YgQ2VydCAyMDE5MS8wLQYDVQQKDCZlZDZlZDZlZDZlZDZlZDZlZDZlZDZl
aXRhbCBUcnVzdCwgUy5MLjELMAkGA1UEBhMCFRFRFRFRFRFRFRFRFRFRFRFRFRFR
NDMwNTMxMTEyODI0WjCBDFEMEIgA1UEAw7RUFVHJ1c3QgU1NBIDgxOTIgaU9v
dCBDQSBG3I9UXVhbGlmaWVkaWV1eSBEVi9PViBDZlZlZlZlZlZlZlZlZlZlZlZl
JkV1cm9wZWV1eSBEVi9PViBDZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZl
EwJFUzCCBCIwDQYJKoZIhvcNAQEBBQADggQPADCCBAoCggQBAN0LprZCZ8+5dEQ1
RYCdFq91cpjmUkuf3sECKJKk53nnXxbDQhup/gS9I8K0FQrs0iWouxSksDLr9gdh
bWp00fOGDKbMb3Wfktq2qlhce/HNqYHP9HrrqHEXg4V/wXuHGVC1edWk2pR08js
PrcZZf/IjdavwRp57AnmFjIyhm1ypiEqHBieHHgeDdEn2i43CSd710t7dXCnhmlr
wUhtgI18umIeMdAPy4cEhVTL8IWjzAkhbcUoC6ZGYS7WaXYeCflxD4tcZUv0/o6k
RLT24bZRKxrUwygL8JmravQaDSDZ9biGnZ9PkfQOK/0N6V31mSxdAJ0zykeXWCPT
IvxoNn9ewfCKehfUhrfSY/DK7nL3oDkuT3zHTywymasa6oE7HYqOqAoXzKPAcDal
xiW7At8A5+Tsh1jPaOzZfIGEAgm7VqnDnpjXttn+WII7rf8RM932UESqkpCrmw1
H/u/V5cj4uFuGk4UHVJJKJKEQ49vI2n00i2LsJsm16tY+OPCEXZFkcJZxWE7rc10G
UXkd9OyYCIc8ZKOQ6/lt5mMMm5Xxx6qudMAppLsB/ZFhqNB4kFvgvWWDk9MyvosJ
mp5KpsjKqjhCHucng33KYGFAZQJtz7Irv4pHDTyAJxEyCNQGRiAmq9YX8d1DTxgc
Qqx0IG5Gq4zNHe7PzR/ihARNR+1CATbC+VbKNTRbkvxpkiPOGU5EU2lda/Sb/2q
RHZwJkcID0t3rPlgxuB/Alwo+Ynxe/lftGw91Ba3fbt+wweHvYhvS9jpcR70Svs3
9TiwHE+0aDHPvJwHnpXq2TrfYY8pFp9fJ8REACPF0s18xRFmS4BbEQd95v6B+3Ik
t54GghcnDBr9Q0fYSWJPBqCuaAFWDN0pWD9UobVAUXzaTMEr7zjInYyLXHb9mXGf
ADOWEbisvmhEINKx9GxalrhZ68Icy6rC1b8h9ON8DnoGja7AeLP+zMAJSjvombP1
1VvxFoS7b4zNok02Lcsa2250TcAXIBeK2oECPutiJFfn8MUp/XmbT0fwOeqFZ38q
QX3BDRAbXCOGs3vhMXHqiP1+Z3h59jHfjwUj0gPEuybG8JLg0qdNtqVTGc5rjL3
Gbv66GK4eJoVKKPh14/TquV8up8TwpPr8MErrCD7SmuHvhZL0rYzszJcBhimvGkRY
xIixukKuIXqJgRmqAfj4Ss5psUlmrIOlGf/iekI62g0aGyvCe2XPpLtu4n/JK2V
zAVjyciwY0Ysc9uR8tFChkyQjpp3KSqDGV7Jf08Tpnkibwx0zA3dLPSeotlW8vrK
NVdrkis3eSnqCJLICbCrBfKl7AmBSOm5gcQ8SHZClzm7d7XsuSXJTv3CSdEcKc
PwEo/8CAwEAaANCMEAwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYw
HQYDVR0OBBYEFJ7tDEGBam/6Zgn6fH+MSGMINn0AMA0GCSqGSIB3DQEEDQUAA4IE
AQCSbcQ7Y0FPXewl5+HKKSE4wl9Gx1fznLKBzXaqqj8sNfS+FM7snBlMXbrUUNWQ
kt8r82B4N1Zu7g5jZhjTN6jey9BxA41yHtBhOA6M6tG5ITEWIq+Oa3L1PhCuvfty
kz0CsAg/g3j3RTB4k9az6Jnuivihwlygoi4GcV7JZiUOHk9+DyFSLiuvBuOmXstl
PVg6I5H4R3vBcIL44THdAkfLTXORXs7Db3aqQmG/tyMxwalkrBLS3mJnPRUzr1p4
```

```
6MZ9bHtJp7Q0gFGYA/KtR3H5GFbXgqQnaBUPEwWbRBHTD+HtiY9zcJ/h9CeC/Tt+
q9J9s6x2MeBWLpZ+nn4UEj5E+WWfNOt1TXzty1EdjoqY9CgddoneE3UpHV8Lp40w
ewE+pNx6SH7QsunxKokasdEkENyD6BmNdlm2g8PbSb/eSJcAKVvs8mhrKM6Ube40
rO361KNrShEwQhG82eSbInHwGlmF/LWr6PdIm33AsKac28wluoA6b8jv7Zu637R1
lgiwSJRugcceYrH7CTQAiVGKEfovBSGGOOMtY/UHY8GWbgKlufGqpSBZOyofQwVI
CQh6HEakHHXWtSOrJdQqPpAF8eMgDjK07ggF9ZHdeZBgLWf3fx3+A+JLODxE5q30
DvcMJ5tp5MG37vRnozWeyP2xRj9jJKqpAvD3hu7zwjv4T2hlJO415L88ck9963Ni
mRWpu+uh+0HB3o2+xaWAsQeqYevSiWC69NHA47TPeph2aSEzSgggSH6st088QqcY
3zscUQj+kYI05y/TF49fxQPp+6EiChmMPZa6qZf1OCWADMRjRVXxLXIIXhByEOGK
qg831boLmiH8LU/FpC48hqslPAn0T1tL/TDTGkUhgW7816D/y9sCu08Ee9I3ijJG
MurQiS89DCRYKbsbJ+pG7KD+nu2acYh/bt73XS0pet9eGCnwLNCaAwCFOpDBKzzI
e8/avbtEYFoNXi/X1KkmLpys9Sx/o9B5m8xEVKSm6jQVABele/uIiR1bkt4PFvZv
VBzDN6Sq29Exln3mdUpFvqh9e7tC+kgE5z9T9QEyTdsdUstfFnXbkQQ0Y1LALzKv
C6did9gA2pOKHr7cNGSdbpY2xKg8WSBR+CsmZNT4aadA5jOqC1SmfMae6Ei6PhFT
TPsUQfW7Ug+0OmRJRn35I4hk46nr+6N6cAD9sodVbojLYUmh1NwyARoHJd99RaWJ
NM710461tdQM5KNjp85b9Yq3iB1ZnqmR5nWwxHdfGDnxdM3iyszITu9Ey0vx9BSD
jI5h3cZCZc2WUZrbyG6d16n1mXdV4ANo0zTzE6NNQef6JRfAzXzpFep5PT80a4je
2VSvVuVhT5VEYQbgkNhkIFh/
-----END CERTIFICATE-----
```

13.3.13 EADTrust RSA 8192 Root CA For Qualified Web EV/PSD2 Cert 2019

```
-----BEGIN CERTIFICATE-----
MIIEJ0jCCBbqgAwIBAgIIIBpeYBykiiEMwDQYJKoZIhvcNAQENBQAwgYYxRjBEBgNV
BAMMPUVBRFRydXN0IFJTTQSA4MTkyIFJvb3QgQ0EgRm9yIFF1YWxpZml1ZSBXZWlG
RVYvUFRNEMiBDZXJ0IDIwMTkxLzAtBgNVBAOMJkV1cm9wZWZuIEFmZW5jeSBvZiBE
aWdpdGFsIFRydXN0LCBTLkwuMQswCQYDVQQGEWJFUzAeFw0xOTA2MDYxMTQzMzda
Fw00MzA1MzExMTQzMzdaMIGMUUYwRAYDVQQDDE1FQUURUcnVzdCBSU0EgODE5MiBS
b290IENBIEZvcBRdWfSaWZpZWQgV2ViIEVWV1BTRDIgQ2VydCAyMDE5MS8wLQYD
VQQKDCZFdXJvcGVhbiBBZ2VuY3kgb2YgRGlNaXRhbCBUcnVzdCwgUy5MLjELMAkG
A1UEBhMCRVMwggQiMA0GCSqGSIb3DQEBAQUAA4IEDwAwggQKAoIEAQDnFBGJSZQF
iCvbIU5x8/ssEZE0hb0WoksmQcGdJsGpEY3FHIbqkg9J/CMAqKpbHemtrQoalRU+
5a7iTMH+dYyoiKyUYgoZ1wxWYjXD88U1XW06Jhk3wkqEe0Ps8rHoTcSWlXqHvEte
QYW/jaO+3vAFFBYAFGzmC4bYnGksxRO+4uKdPzpteXNVdV06GA/WnX341VXnQNAD
dK4Xxhmf6Ztkoj0ev+U0lRlv6WekBL5MjpesV8xehYkTtoitiPdAVpScOJ6gDzy
2ELhKrewz6u/Htf9G1cRusbYXvL09U01OQ/z6WnaSOre9VDZunZlSZxlnPatCj7
g4Wo7/8TsbRRlRMyh6M/ZMFODvb54V6e0lEGPNBZF0HMKnrk15459/2P0qWh7VK+
LeXAbQif0QVib1B7Lxkcf4c/yFro6lge/vdTHHn5/oV9NpWfdwdzcgfQg7MoZGi7
llfz9gvm4lGeAlV0Z+3lt6nrSDidWxsknWoEioxE0fmfGiFBdTUWmwTGEla4nd/V
DLf4Rh7LZBeMvqiu/PSVlet7TtSLJt4ZFpC75k9FX3I6zjoZQRJSnKXXtpRaoyv1
hfEzCboAKZYyvSz5PmWicB2xuX4yOkUqqEHgg5qmA8GQVtZABVDkmCBG0ghdrZJy
DjsPsd1hZXvSbSFVTFCZbLHnUeU+mtf1Ed3HDGq/HL5xSFRNfex3aYgerOpjCrS2
2Bcqb3c06LVnappJ8BTY8sBV0dLEHFANLsHGP/NtWW1nZ9Mw6m5Dc/LNmSwvHWa9
PGxyJAWxYOL331QIzh/+GnSWDA5vHgfolluHRtr06euBQGDLaKZo7vTpQKrnIdOf
111nc4K2sJVM1ch7MRup+dppwb2mvASClHmXQtGwS2cuJxAeCCCN2paJ1wEU00ed
BxKkPmI6zu38zJU053A2GvB/pVPZlnyfoAS+/ywtayOD/zRK8oTl0lytzDeb6K7V
LZsQtAqtKhOTZobSLSIYNYdsIAAjnMsleQwWEcyb9lHDlJgn+wsLV8MHfTCnSvAb
YgT3MbZLHqhz4Q1CvjJu7fl68cdnXGDhvkqwx1C3zqoWKlyTvtFEV+OTVBZVZ/J
Asg+SqbMaBhUVTEuVfHc3ATLKwNouh9cJgtVf6n96H59TXmUpgEvWtcZd9SNH+N1
TapoXnJcBWYobl0GYCk2H93WCJ14rGfuZczwzBdiHGjE9GilvVzBPb9+wX+IX4o
pQ/mwTWCEXe1RaQz6xocmMeaic7JDbGA2xcvHOeZZkhTuFoQPmfDrkl88q2A4cLq
d1vLc0BSyjj9Nw5MGHShMJifzK6gfWCaRsZ9+XKyF9+/eNu7sZ1ivL/wXhiiYN0C
-----END CERTIFICATE-----
```





J+3Y3qfJJPJg+G0wwNMztV9TSC4n4J58ac82do0GcccWdGoyr/yEnlte9jJ/NQ61P  
FKo/499m3UbfrwmBHeKI f hXW3LA0VHmkapfxTPGQSwTDewjwqolHwPG1skCa3SII  
i0xwUcXqK5/5ZPFnYV9TrxOUOv+y+UfOk6U2wE4cXnEllykrdOKFV4DuL5yplbTM  
bJ+MlUI3cy693DdVjyF5V5VoJzZW2vFFA+N4pG9mkyICiULewUjMNoFcxwCHjkDl  
VBUYZIH25MA9o7HS1dsGA4InNtIl5Lt0aR8xR6alx/Vgu7i26mQ+t/9mlBxEyDED  
6WN9kjne/i jEmdv5gJwAu0pPUHsDclI+2YGtSKJD3ZWWk/RiwAmgVkrdicK50Ii  
Xk67Ypj25JBXLfj5OfAnFJawNmCc jCv/BdQBMDmlPxMnyXmUZpf8Vua5mvncdcPT  
zi2WTtDvq4kpvQwkXBuWySLQWv1f1PY6HZIYwqWEJXQptlM4DuhpgJyM+g1hqsDn  
UyoXjbb2nQIDAQABO4GoMIG1MA8GA1UdEwEB/wQFMAMBAf8wDgYDVR0PAQH/BAQD  
AgEGMGMA1UdEQRCMFqBDMNhQGVhZHRydXN0LmV1hhZodHRwOi8vd3d3LmVhZHRy  
dXN0LmV1hhVodHRwOi8vY2EuZWFKdHJlc3QuZXZlZG90dHA6Ly9wb2xpY3kuZWFK  
dHJlc3QuZXUwHQYDVR0OBByEFAbmc9lROUCn0VeMnN/H7dB53ffLMA0GCSqGSIB3  
DQEBDQUAA4IEAQCq6yOyzhD3p8j+R8cMwqtd2sJepky1JGcz7pN0o50TtP2zSZL/  
+ZNS7cI30cg97Ywc8JE7yRA+ppcLss25N1UlRUL8t1JTG0Xbf9fIovjlljU3ha0z  
RhzdtfGz5cdH0LS2rU6r893tX/yjW4KUyYI24XUrt0OZpcfKrtuZnSa2YHhmW009  
KYrVqpIpnVU4P92Gr91H9Ro9IW6kg29/zpgjVr8SrNqkmaxhDEFuzLVphKbf+RZx  
PzYZ7p5kobYSLNpzzgnhPkylc5ytkxTpQBxa79OZp7bwIEoRqYNfucTqIhY77wWL  
7YUc2gq9HQM5FFaCUSb2Ik3HlgujBvk4euccvgrRrOJXi9j2DL5ICHTdG7Gw6F+xG  
MrThkzevQoG4HHIvB/tQwQDHATEuTghzD2cFavIhnX0A97plPMEPlUwV7edJMum6  
b/NaNRFJCIWhs9x6cORAQPfGDDyUwyaWWrQ9VgcS2L+Yk/fs6nkhZdLtZ97F167i  
pv11c3V89Q0x2Iv+9JD5Nm+VqnaI5Z9vgrfYDDR5OMli+EakKBDs7nDySPwd3F4L  
lyuQu99FsBlQCE0k6C3TK8XgATqzwrW205Yic6NcSo3Byz4HMSarFHbK4utP3vI1  
3KKzsImHmpJ/483xSPHxUYT4sD2FtynillSR0JIEyHZuhMGAK5Ix/JnTQNmCx6C  
M//Vq3IJN8ofFBMFCFxn/Kx0p8LZAHIQVsy8ttQBA2jnzlU98VDwS5sBsENCr927  
hSaWw3XlWWUdZwbx0qu6wQskiSlrVm3zyWSeFpv74ibM8VYMwRLiAL65m9nTxMyA  
lfvcWgupv9RQbvrX2GU4KHhJN0vi6yUHOgugaGXvnnsOEl1f49nop7zrA0N9QFoD  
Jf530D9/U4mw0LS0Cli5eWKctCxDYMQxs/RTNog0x0fy0yFNIGOLXBodLtsWZPXw  
sNcvo5H74dJLrbPwi6ZlaYOoEDq78XuP7kx0n7940Qrq7Ks6FGbhrNHYbb7Apm80  
uYKKkw4qjBXlQUNqDd3wc8ug+y1abLZnHnmw+dfGBKJD6M+hr6zDJXqcNz6xCWb  
DzbBnxiiR/2zCP9rbHx1Af2bL2MCrvmwfaKtRHnNWS1vbfmu025p+Vr7yerin5+J  
fyAs2hLJEO/G7Ef3EcMG6sH//z55EJw+zicbExb0OPVsRLZqVv84H/vT4VxVsS8G  
lRDxuEKSy9gg9iESq0a0VMVxk2Fypim6rvxFGAZceEWXy+XUP6G8zkXF3lqjl2/3  
UJpVg+Z96CideS4DGHjVpFW/tu6J1NFK139KS6QFke9wP6g/bzrN+Q60izSCc7v6  
wjup+COimIMePMHiseuA4TKzEZD0U2lhjoiz  
-----END CERTIFICATE-----

13.3.15 EADTrust ECC 256 SubCA For Qualified Web DV/OV Cert 2019

-----BEGIN CERTIFICATE-----  
MIIDnDCCA0GgAwIBAgIIEXWHRlgglDkwCgYIKoZIzj0EAwIwYmVxQzBBBgNVBAMM  
OkVBRFRydXN0IEVDQyAyNTYgUm9vdCBDQSBG3IgwUXVhbG1maWVkiFdlYiBEVi9P  
ViBDZXJ0IDIwMTkxLzAtBgNVBAoMJKV1cm9wZWZuIEFnZW5jeSBvZiBEaWdpdGFs  
IFRydXN0LCBTLkwuMQswCQYDQQGEWJFUzAeFw0xOTA2MDYxMTM1NTJhFw0zMTA2  
MDMxMTM1NTJhMIGBMUEwPwYDQDdHhFQURUcnVzdCBFQ0MgMjU2IFN1YkNBIEZv  
ciBRdWFsaWZpZWQgV2ViIERWl09WIENlcnQgMjAxOTFvMCA1UEcGwmRXVyb3Bl  
YW4gQWdlbmN5IG9mIERpZ2l0YWwvVHJlc3QsIFMuTC4xZCZAJBgNVBAYTAkVMTkVh  
EwYHkoZIzj0CAQYIKoZIzj0DAQcDQgAEQmQp2YJyJACaPj9Mu1FeH2UTDK5U6zrX  
oPr/+1cA0VayagC9JFB02g/xej3X9tv55c9V8iUfw5LA70VoFbNMjaOCAZ0wggGZ  
MEsGA1UdIAREMEIwBgYEVR0gADA4Bg0rBgEEAYN1AgEBAYMRMCCwJQYIKwYBBQUH  
AgEwGWh0dHA6Ly9wb2xpY3kuZWFKdHJlc3QuZXUwEgYDVR0TAQH/BAGwBgEB/wIB  
ADA0BgNVHQ8BAf8EBAMCAYYwHQYDVR0OBByEFOCbqvBLf7ZoiOqft6Av/hWlrJVk

```
MB8GA1UdIwQYMBaAFLwrxlvjatp90ahGrUfe40XAw/2yMEsGA1UdHwREMEIwQKA+
oDyGomh0dHA6Ly9jcmwuZWFKdHJlc3QuZXUvZWFKdHJlc3Qtcm9vdC1lY2MyNTZl
YWRkdm92MjAxOS5jcmwwegYIKwYBBQUHAQEebjBsMEUGCCsGAQUFBzAChj1odHRw
Oi8vY2EuZWFKdHJlc3QuZXUvZWFKdHJlc3Qtcm9vdC1lY2MyNTZlYWRkdm92MjAx
OS5jcnQwIwYIKwYBBQUHMAGGF2h0dHA6Ly9vY3NwLmVhZHRydXN0LmV1MB0GA1Ud
JQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjAKBggqhkjOPQQAQAgNjADBGAiEA+xsp
1y3d0b/kLk+9bqHx1TXznZQSSjYmiBQCpv8kabsCIQCaLjx5plNhyGTWMMRoasNw0
fSAkivbPUopn53pcCu8Cjg==
-----END CERTIFICATE-----
```

### 13.3.16 EADTrust ECC 256 SubCA For Qualified Web EV/PSD2 Cert 2019

```
-----BEGIN CERTIFICATE-----
MIIDpDCCA0mgAwIBAgIIMiJzWEZDQEQwCgYIKoZIzj0EAwIwYUxRTBDBgNVBAMM
PEVBRFRydXN0IEVDQyAyNTYgUm9vdCBDQSBG3IgwUXVhbG1maWVkiFdlYiBFVi9Q
U0QyIENlcnQGMjAxOTEvMC0GA1UECgwmRXVyb3B1YW4gQWdlbmN5IG9mIERpZ2l0
YWwgVHJlc3QsIFMuTC4xZCZAJBgNVBAYTAkVTMB4XDTE5MDYwNjExNDkyNFoXDTMx
MDYwMzExNDkyNFowYm9vZzBBBggrBgNVBAMMOkVBRFRydXN0IEVDQyAyNTYgU3ViQ0Eg
Rm9yIFF1YWxpZm1lZCBXZWlGRVYvUFNEMiBDZXJ0IDlwMTkxLzAtBgNVBAoMJKV1
cm9wZWFuIEFnZW5jeSBvZiBEaWdpdGFsIFRydXN0LCBTLkwwMQswCQYDVQQLGwJF
UzBZMBMGBYqGSM49AgEGCCqGSM49AwEHA0IABCOD0KvinA0yE58PK9jtDhp24ao1
77XI+uENlek+PYZhgdZZeD5TkjDrGIC2UchXhw24U1/plMMbZNVVf4KhBzWjggGh
MIIBnTBLBgNVHSAERDBCMAyGBFUDIAAwOAYNKwYBBAGDdQIBAQGDETAncMCUGCCsG
AQUFBwIBFh1odHRwOi8vcG9saWN5LmVhZHRydXN0LmV1MBIGA1UdEwEB/wQIMAYB
Af8CAQAwDgYDVROPAQH/BAQDAgGMB0GA1UdDgQWBBQJdr5ZrQBosRSSVUEGb7Nm
MDkgczAfBgNVHSMEGDAWgBTTd81a2qOTXIktGTGXSmgwB1Zk/EzBNBgNVHR8ERjBE
MEKqQKA+hjxodHRwOi8vY3J5LmVhZHRydXN0LmV1L2VhZHRydXN0LXJvb3QtZWNj
MjU2ZWFKZXZwZ2QyMjAxOS5jcmwwfAYIKwYBBQUHAQEecDBuMEcGCCsGAQUFBzAC
hjtodHRwOi8vY2EuZWFKdHJlc3QuZXUvZWFKdHJlc3Qtcm9vdC1lY2MyNTZlYWRl
dnBzZDIyMDE5LmNydDAjBggrBgEFBQcwAYYXaHR0cDovL29jc3AuZWFKdHJlc3Qu
ZXUwHQYDVROlBBYwFAYIKwYBBQUHAWEGCCsGAQUFBwMCMAoGCCqGSM49BAMCA0kA
MEYCIQC26I5aeV5Y/bM0ZDI6w43s7lbd86MlqAvrX8yciDv+6AIhAPPNHZRucILM
LzkipHGqvNFIPalAzzB3ryo3TE5Af2Lyy
-----END CERTIFICATE-----
```

### 13.3.17 EADTrust ECC 256 SubCA For Qualified Certificates 2019

```
-----BEGIN CERTIFICATE-----
MIIE5jCCBIugAwIBAgIIBJeJkUGCQIMwCgYIKoZIzj0EAwIwZsXQTA/BgNVBAMM
OEVBRFRydXN0IEVDQyAyNTYgUm9vdCBDQSBG3IgwUXVhbG1maWVkiENlcnRpZm1j
YXRlc3QyMDE5LmNydDAjBggrBgEFBQcwAYYXaHR0cDovL29jc3AuZWFKdHJlc3Qu
ZXUwHQYDVROlBBYwFAYIKwYBBQUHAWEGCCsGAQUFBwMCMAoGCCqGSM49BAMCA0kA
MEYCIQC26I5aeV5Y/bM0ZDI6w43s7lbd86MlqAvrX8yciDv+6AIhAPPNHZRucILM
LzkipHGqvNFIPalAzzB3ryo3TE5Af2Lyy
-----END CERTIFICATE-----
```

Bg0rBgEEAYN1AgEBAYMRMIGAMCUGCCsGAQUFBwIBFh1odHRwOi8vcG9saWN5LmVh  
ZHRydXN0LmV1MfcGCCsGAQUFBwICMEsMSVN1Ym9yZGluYXR1IEN1cnRpZmljYXR1  
IEF1dGhvcml0eS4gRXVyY3BlYW4gQWdlbmN5IG9mIERpZ210YWwgVHJ1c3QsIFMu  
TC4wEgYDVR0TAQH/BAGwBgEB/wIBADA0BgNVHQ8BAf8EBAMCAYYwHQYDVR0OBBYE  
FNNMbDq9Nv5whyOHou49kM/Lm/chMGMGA1UdEgRcMFqBDMNhQGVhZHRydXN0LmV1  
hhZodHRwOi8vd3d3LmVhZHRydXN0LmV1hhVodHRwOi8vY2EuZWZkdHJ1c3QuZXWG  
GWh0dHA6Ly9wb2xpY3kuZWZkdHJ1c3QuZXUwYwYDVR0RBFwwWoEOY2FAZWFkdHJ1  
c3QuZXWGFmh0dHA6Ly93d3cuZWZkdHJ1c3QuZXWGFWh0dHA6Ly9jYS5lYWR0cnVz  
dC5ldYYZaHR0cDovL3BvbG1jeS5lYWR0cnVzdC5ldTAFBgNVHSMEGDAWgBQBZ5qE  
xJnGge08WAR0rySj115BDTBIBGvNVR8EQTA/MD2gO6A5hjdodHRwOi8vY3JsLmVh  
ZHRydXN0LmV1L2VhZHRydXN0LXJvb3QtZWNjMjU2ZWZkdHJ1c3QuZXUwYwYDVR0R  
BQYDVR0BBGswaTBCBggrBgEFBQcwoA0Y2aHR0cDovL2NhLmVhZHRydXN0LmV1L2Vh  
ZHRydXN0LXJvb3QtZWNjMjU2ZWZkdHJ1c3QuZXUwYwYDVR0RBMGCCsGAQUFBzABhhdodHRw  
Oi8vb2Nzc5lYWR0cnVzdC5ldTAKBggqhkjOPQQDAgNJADBGAiEA03kjVg5x0Nx2  
Vl5H86QV1mB0g4miZn1xrt7SQV+8ggUCIQCOjpmf3+3shoTYYNZkUlv0aWfjV//5  
lps4eXGPqoaqaQ==  
-----END CERTIFICATE-----

### 13.3.18 EADTrust ECC 256 SubCA For Qualified Certificates 2019

-----BEGIN CERTIFICATE-----  
MIIE5zCCBI2gAwIBAgIIRXRDCCFQI5gwCgYIKoZIzj0EAwIwZSsxQTA/BgNVBAMM  
OEVBRRFrydXN0IEVDQyAyNTYgUm9vdCBDQSBG3IgwUXVhbG1maWVkiEN1cnRpZmlj  
YXR1cyAyMDE5MS8wLQYDVQKDCZFdxJvcGVhbiBBZ2VuY3kgb2YgRGlNaXRhbCBU  
cnVzdCwgUy5MLjELMAKGA1UEBhMCRVMxGDAWBgNVBGEEMD1ZBVEVTLUI4NTYyNjI0  
MDAeFw0xOTA2MDYxMTIzMTJhFw0zNTA2MDI1MTIzMTJhMIGyMT8wPQYDVR0QDDZ  
FQURUcnVzdCBFQ0MgMjU2IFN1YkNBIeZvc1BRdWFSaWZpZWQgQ2VydG1maWNhdGVz  
IDIwMTkxLzAtBgNVBAoMJKV1cm9wZWZuIEF1c3Q5jeSBvZiBEaWdpdGFsIFRydXN0  
LCBTLkkuwQswCQYDVR0QGEwJFUzEYMBYGA1UEYQwPvkFURVMTQjg1NjI2MjQwMRcw  
FQYDVR0QLDA5OYXR1cmFsIFBlcnNvb3BZMBMGByqGSM49AgEGCCqGSM49AwEHA0IA  
BIvhQDKEvOGURiGfC4WgrptHxeQsvHdo1lcoQtGO/ElyWoYx0vS6mIb9KUEPf5s  
3bvFuNbDyyIF00PM5lF3yOijggKgmIICnDCBqAYDVR0gBIGgMIGdMAYGBFudIAAw  
gZIGDSsGAQQBg3UCAQEBgxEwgYAwJQYIKwYBBQUHAQEWGWh0dHA6Ly9wb2xpY3ku  
ZWZkdHJ1c3QuZXUwVwYIKwYBBQUHAQIwSwxJU3Vib3JkaW5hdGUgQ2VydG1maWNh  
dGUgQXV0aG9yaXR5LiBFdXJvcGVhbiBBZ2VuY3kgb2YgRGlNaXRhbCBUcnVzdCwg  
Uy5MLjASBgNVHRMBAf8ECDAGAQH/AgEAMA4GA1UdDwEB/wQEAwIBhjAdBgNVHQ4E  
FgQUw+LbEe82PGqASysjRo07pznrmQwwYwYDVR0SBBFwwWoEOY2FAZWFkdHJ1c3Qu  
ZXWGFmh0dHA6Ly93d3cuZWZkdHJ1c3QuZXWGFWh0dHA6Ly9jYS5lYWR0cnVzdC5l  
dYYZaHR0cDovL3BvbG1jeS5lYWR0cnVzdC5ldTBjBgNVHREEXDBagQ5jYUBlYWR0  
cnVzdC5ldYYWaHR0cDovL3d3dy5lYWR0cnVzdC5ldYYVaHR0cDovL2NhLmVhZHRy  
dXN0LmV1hh1odHRwOi8vcG9saWN5LmVhZHRydXN0LmV1MB8GA1UdIwQYMBaAFAFn  
moTEmcaB7TxYBHSvJKPXXkENMEgGA1UdHwRBMD8wPaA7oDmGN2h0dHA6Ly9jcmwu  
ZWZkdHJ1c3QuZXUwVwZWFkdHJ1c3Qtcm9vdC1lY2MyNTZlYWRxMjAxOS5jcmwwdWYI  
KwYBBQUHAQEeazBpMEIGCCsGAQUFBzAChjZodHRwOi8vY2EuZWZkdHJ1c3QuZXUw  
ZWZkdHJ1c3Qtcm9vdC1lY2MyNTZlYWRxMjAxOS5jcnQwIwYIKwYBBQUHMAGGF2h0  
dHA6Ly9vY3NwLmVhZHRydXN0LmV1MAoGCCqGSM49BAMCA0gAMEUCIGp+6oK32Jsu  
+fGmgaszbcshvgItZIGHNWQxtX44SN2AiEAjj8rAaWdPjX9KPDsCIjTYNY0UeE3  
heqjNssNsXJzCVY=  
-----END CERTIFICATE-----

13.3.19 EADTrust ECC 384 SubCA For Qualified Web DV/OV Cert 2019

```
-----BEGIN CERTIFICATE-----
MIID1zCCA16gAwIBAgIIUCAycVlJY2gwCgYIKoZIzj0EAwMwgYMxQzBBBgNVBAMM
OkVBRFRydXN0IEVDQyAzODQgUm9vdCBDQSBG3IgwUXVhbG1maWVkiFdlYiBEVi9P
ViBDZXJ0IDIwMTkxLzAtBgNVBAoMJkV1cm9wZWFuIEFnZW5jeSBvZiBEaWdpdGFs
IFRydXN0LCBTLkxwMQswCQYDVQGEwJFUAeFw0xOTA2MDYxMTM1NTVaFw0zMTA2
MDMxMTM1NTVAMIGBMUEwPwYDVQDDdhFQURUcnVzdCBFQ0MgMzg0IFN1YkNBIEZv
ciBRdWFSaWZpZWQgV2ViIERWLO9WIEN1cnQgMjAxOTEvMC0GA1UECgwmRXVyb3Bl
YW4gQWdlbmN5IG9mIERpZ2l0YWwgVHJlc3QsIFMuTC4xCzAJBgNVBAYTAkVMTMhYw
EAYHkoZIzj0CAQYFK4EEACIDYgAE6o4xOzPzH2Ht9WK476vEYj6nkC3GiYomL9YS
Ru0gzdi2oS1m8eZcGEuD7pe0Gd3Y8JL7A1ygrZIUa+TUuftPjB4MfWLz79VcHZCR
xtFzrxRuesh4HN61haPqkk7sFSUxo4IBnTCCAzkSwYDVR0gBEQwQjAGBgRVHSAAM
DgGDSsGAQQBg3UCAQEBAgEwJzAlBggrBgEFBQcCARYZaHR0cDovL3BvbG1jeS5l
YWR0cnVzdC5ldTASBgNVHRMBAf8ECDAGAQH/AgeEAMA4GA1UdDwEB/wQEAWIBhAd
BgNVHQ4EFgQUZj/V6yyw0c/kc+YXwGjFc+pv9kowHwYDVR0jBBGwFoAUHJTYEpRj
f9etQ3G7LrK6M9LA9EYwSwYDVR0fBEQwQjBAoD6gPIY6aHR0cDovL2Nybc5lYWR0
cnVzdC5lds9lYWR0cnVzdC1yb290LWVjYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYz
YzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYz
YzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYz
aHR0cDovL29jc3AuZWFKdHJlc3QuZXUwHQYDVR0lBBYwFAYIKwYBBQUHAWEGCCsG
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-----
MIID3zCCA2agAwIBAgIIIBFEXZXBGYzUwCgYIKoZIzj0EAwMwgYUxRTBDBBgNVBAMM
PEVBRFRydXN0IEVDQyAzODQgUm9vdCBDQSBG3IgwUXVhbG1maWVkiFdlYiBFVi9Q
U0QyIEN1cnQgMjAxOTEvMC0GA1UECgwmRXVyb3BlYW4gQWdlbmN5IG9mIERpZ2l0
YWwgVHJlc3QsIFMuTC4xCzAJBgNVBAYTAkVMTMhYwEAYHkoZIzj0CAQYFK4EEACID
YgAE6o4xOzPzH2Ht9WK476vEYj6nkC3GiYomL9YSRu0gzdi2oS1m8eZcGEuD7pe0G
d3Y8JL7A1ygrZIUa+TUuftPjB4MfWLz79VcHZCRxtFzrxRuesh4HN61haPqkk7sFS
Uxo4IBnTCCAzkSwYDVR0gBEQwQjAGBgRVHSAAMdGDSsGAQQBg3UCAQEBAgEwJzAlB
ggrBgEFBQcCARYZaHR0cDovL3BvbG1jeS5lYWR0cnVzdC5ldTASBgNVHRMBAf8ECD
AGAQH/AgeEAMA4GA1UdDwEB/wQEAWIBhAdBgNVHQ4EFgQUZj/V6yyw0c/kc+YXwGj
Fc+pv9kowHwYDVR0jBBGwFoAUHJTYEpRjf9etQ3G7LrK6M9LA9EYwSwYDVR0fBEQ
wQjBAoD6gPIY6aHR0cDovL2Nybc5lYWR0cnVzdC5lds9lYWR0cnVzdC1yb290LWVj
YzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYz
YzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYzYz
aHR0cDovL29jc3AuZWFKdHJlc3QuZXUwHQYDVR0lBBYwFAYIKwYBBQUHAWEGCCsG
AQUFBwMCMAoGCCqGSM49BAMDA2cAMGQCMFqnk4zWsC5s5l+6abjGtJHRJBkaGeCJ
zs7CXXWBDFEF3Wci9b1zKCjr2IZb8hkLZAIwRDNBSURcXnoz1GgWrmW/dazQkIc+
VTQ7t15/sSrmczCUUmBTjo5llrCWFbMV/HgS
-----END CERTIFICATE-----
```

-----END CERTIFICATE-----

### 13.3.21 EADTrust ECC 384 SubCA For Qualified Certificates 2019

-----BEGIN CERTIFICATE-----

MIIFIjCCBKigAwIBAgIiWCYiWAgiDgEwCgYIKoZiZjOEAwMwgZsxxQTA/BgNVBAMM  
OEVBFRydXN0IEVDQyAzODQgUm9vdCBDQSBG3IqUXVhbGlmaWVkiENlcnRpbWlj  
YXRlcjYyMDE5MS8wLQYDVQKDCZFdxJvcGVhbiBBZ2VuY3kgb2YgRGlnaXRhbCBU  
cnVzdCwgUy5MLjELMAKGA1UEBhMCNVBMGEMD1ZBVEVTLUI4NTYyNjI0MDEx  
MDAeFw0xOTAyMDYxMTIzMZaFw0zNTA2MDIxMTIzMZaMIIGwMT8wPQYDVQDDZ  
FQURUcnVzdCBFQ0MgMzg0IFNlYkNBIEZvcjBRdWFsaWZpZWQgQ2VydGlmaWNhdGVz  
IDIwMTkxLzAtBgNVBAoMJKkVlcm9wZWVudIEFmZW5jeSBvZiBEaWdpdGFsIFRydXN0  
LCBTLkkuMQswCQYDVQGEwJFUzEYMBYGA1UEYQwPvFURVMtQjg1NjI2MjQwMRUw  
EwYDVQQLDAxMZWdhdhCBQZlZm24wZjAQBgcqhkjOPQIBBgUrgQQAIgNiAAT16y8u  
3RP+c73LiVVIx3fsNqxqYmu7Xj2TxDNQhibTh64f+OfQB2HmPcavFeYhdks6LmP  
qt+kgY30W9A43fvVsfjyBBqVDrNnaqJyYkfhEE4q6lNZETLCAZUu6inZDqWajggKg  
MIICnDCBqAYDVR0gBIGgMIGdMAYGBFUDIAAwgZIGDSsGAQQBg3UCAQEBgxEwgYA  
wJQYIKwYBBQUHAgEWWGwh0dHA6Ly9wb2xpcy5kb293ZWVudGQwYUgQXV0aG9yaXR5LiBFdXJvcGVh  
biBBZ2VuY3kgb2YgRGlnaXRhbCBUcnVzdCwgUy5MLjASBgNVHRMBAf8ECDAGAQH/  
AgEAMA4GA1UdDwEB/wQEAwIBhjAdBgNVHQ4EFgQUXBniqx22uD1FEpGSG4wUcdjo  
9fYwYwYDVR0SBFwWwoEOY2FAZWFkdHJ1c3QuZXWGFmh0dHA6Ly93d3cuZXWkdHJ1  
c3QuZXWGFw0dHA6Ly9jYS5lYWR0cnVzdC5ldYYZaHR0cDovL3BvbGljeS5lYWR0  
cnVzdC5ldTBjBgNVHREEXDBagQ5jYUB1YWR0cnVzdC5ldYYWahr0cDovL3d3dy5l  
YWR0cnVzdC5ldYYvaHR0cDovL2NhLmVhZHRydXN0LmV1hhlodHRwOi8vcG9saWN5  
LmVhZHRydXN0LmV1MB8GA1UdIwQYMBaAFHGU/e7RCWBCdadnbiZigeTqxJIBMEgG  
A1UdHwRBMD8wPaA7oDmGN2h0dHA6Ly9jcmwuZXWkdHJ1c3QuZXUvZWVkdHJ1c3Qt  
cm9vdC1lY2MzODRlYWRxMjAxOS5jcmwudWYIKwYBBQUHAQEEdzBpMEIGCCSQAUF  
BzAChjZodHRwOi8vY2EuZXWkdHJ1c3QuZXUvZWVkdHJ1c3Qtcm9vdC1lY2MzODRl  
YWRxMjAxOS5jcnQwIwYIKwYBBQUHMAGGF2h0dHA6Ly9vY3NwLmVhZHRydXN0LmV1  
MAoGCCqGSM49BAMDA2gAMGUCCMqQC9ggUfSfkl5l0hpQPBevyklwcm1FLTws08r5g  
KccXtsVJ6W3ZlQnCGCsfYzyF8wIxAIHxWbeFz94DJo4mv53RLthhFkLdLMnPtdeC  
6FFHuJFMZwtSJDfZotTF2D/y7gLUbQ==

-----END CERTIFICATE-----

### 13.3.22 EADTrust ECC 384 SubCA For Qualified Certificates 2019

-----BEGIN CERTIFICATE-----

MIIFJDCCKKgAwIBAgIJAJA2BpFoYohBMAoGCCqGSM49BAMDMIGbMUEwPwYDVQQD  
DDhFQURUcnVzdCBFQ0MgMzg0IFJvb3QgQ0EgRm9yIFFf1YWxpZml1ZCZBDXZJ0aWZp  
Y2F0ZXMGMjAxOTEvMCA0GA1UECgwmRXVyb3BlYW4gQWdlbmN5IG9mIERpZ210YWwg  
VHJ1c3QsIFMuTC4xCzAJBgNVBAYTAkVTMRgwfGgYDVQRhDA9WQVRFUy1CODU2MjYy  
NDAAwHhcNMTkxLzAtBgNVBAoMJKkVlcm9wZWVudIEFmZW5jeSBvZiBEaWdpdGFsIFRydXN0  
RUFEVHJ1c3QgRUNDIDM4NCBtdWJDQSBG3IqUXVhbGlmaWVkiENlcnRpbWljYXRlcjYy  
MDE5MS8wLQYDVQKDCZFdxJvcGVhbiBBZ2VuY3kgb2YgRGlnaXRhbCBUcnVzdCwgUy5ML  
jELMAKGA1UEBhMCNVBMGEMD1ZBVEVTLUI4NTYyNjI0MDExMDAeFw0xOTAyMDYxMTIzMZaFw0z  
NTA2MDIxMTIzMZaMIIGwMT8wPQYDVQDDZFQURUcnVzdCBFQ0MgMzg0IFNlYkNBIEZvcjBRdWFsaWZp  
ZWQgQ2VydGlmaWNhdGVzIDIwMTkxLzAtBgNVBAoMJKkVlcm9wZWVudIEFmZW5jeSBvZiBEaWdpdGFsIFRydXN0  
LCBTLkkuMQswCQYDVQGEwJFUzEYMBYGA1UEYQwPvFURVMtQjg1NjI2MjQwMRUwEwYDVQQLDAxMZWdhdhCBQZlZm24wZjAQBgcqhkjOPQIBBgUrgQQAIgNiAATZ  
zrGktCAEuUZV2ZqHdfb7uiaQRwTpzALrdQHT4DHCAuTGInFLIododPkkvVdMaVMb  
ZmDzOBHfd2uJslxeI6v4ztnSXh3Ib0nK7/ODNjtK1gfF8BpRgQsbwLP1Vm42mD6j  
ggKgMIICnDCBqAYDVR0gBIGgMIGdMAYGBFUDIAAwgZIGDSsGAQQBg3UCAQEBgxEw

```
gYAwJQYIKwYBBQUHAgEWGWh0dHA6Ly9wb2xpY3kuZWFKdHJ1c3QuZXUwVwYIKwYB
BQUHAgIwSwxJU3Vib3JkaW5hdGUgQ2VydGlmaWNhdGUgQXV0aG9yaXR5LiBFdXJv
cGVhbiBBZ2VuY3kqb2YgRGlnaXRhbCBUcnVzdCwgUy5MLjASBgNVHRMBAf8ECDAG
AQH/AgEAMA4GA1UdDwEB/wQEAwIBhjAdBgNVHQ4EFgQUj7roZnJ0IkzMJ4lICDFz
Cx6bS4IwYwYDVR0SFBFwwWoeOY2FAZWFkdHJ1c3QuZXWGFmh0dHA6Ly93d3cuZWFK
dHJ1c3QuZXWGFWh0dHA6Ly9jYS5lYWR0cnVzdC5ldYYZaHR0cDovL3BvbG1jeS5l
YWR0cnVzdC5ldTBjBgNVHREEXDBagQ5jYUBlYWR0cnVzdC5ldYYWaHR0cDovL3d3
dy5lYWR0cnVzdC5ldYYVaHR0cDovL2NhLmVhZHRydXN0LmV1hhlodHRwOi8vcG9s
aWN5LmVhZHRydXN0LmV1MB8GA1UdIwQYMBaAFHGU/e7RCWBcdadnbiZiGeTqxJIB
MEgGA1UdHwRBMd8wPaA7oDmGN2h0dHA6Ly9jcmwuZWFKdHJ1c3QuZXUvZWFKdHJ1
c3Qtcm9vdC1lY2MzODRlYWRxMjAxOS5jcmwudwYIKwYBBQUHAQEeazBpMEIGCCsG
AQUFBzAChjZodHRwOi8vY2EuZWFKdHJ1c3QuZXUvZWFKdHJ1c3Qtcm9vdC1lY2Mz
ODRlYWRxMjAxOS5jcnQwIwYIKwYBBQUHMAGGF2h0dHA6Ly9vY3NwLmVhZHRydXN0
LmV1MAoGCCqGSM49BAMDA2cAMGQCMH6hKBIXDD6FtWe0lgEKC0+eqz91aZCzIf6t
W7kWG6B6nXAR/iwp05213d7uDzP9SAIwf/zs2GCNSqLLLTaFiuk/pVy69WAhNqUd
/mL7Qh36ObWETT46WU/q5PbcJlRDbMmC
-----END CERTIFICATE-----
```

### 13.3.23 EADTrust RSA 2048 SubCA For Qualified Certificates 2019

```
-----BEGIN CERTIFICATE-----
MIIGdTCCBV2gAwIBAgIIIdGgFWUGBFicwDQYJKoZIhvcNAQELBQAwgZwxQjBAbGNV
BAMMOUVBRFRydXN0IFJFTQSAyMDQ4IFJvb3QgQ0EgRm9yIFFlYWxpZml1ZCZBDZl0
aWZpY2F0ZXMGmJAxOTEvMC0GA1UECgwmRXVyb3B1YW4gQWdlbmN5IG9mIERpZ2l0
YWwgVHJ1c3QsIFMuTC4xZCzAJBgNVBAYTAKVTMRgwFgYDVQRhDA9WQVRFUy1CODU2
MjYyNDAwHhcNMjkwNjA2MTA1NjIzWhcNMzUwNjAyMTA1NjIzWjCBSTFAMD4GA1UE
Aww3RUF0ZXMGmJAxOTEvMC0GA1UECgwmRXVyb3B1YW4gQWdlbmN5IG9mIERpZ2l0
YWwgVHJ1c3QsIFMuTC4xZCzAJBgNVBAYTAKVTMRgwFgYDVQRhDA9WQVRFUy1CODU2
MjYyNDAwFTATBgNVBASMDExlZ2FsIFBlcnVbjCCASiWdQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAPBQEUTudXNGvxaYBi9k1Te3sYjYRwRLzCqLe0cUze6adEvcTSVN
MMzXu4hL+YSgm+2WrJDSbjLKVtLjXIXIwGr1b3YzdYMyfKaZw6in76MNO0gUm1BFS
f7catMHzyqkQJ9GBUF0iEecERo1SF0eFltpXemXK5d1eApNchjQLDS7GduRgDb6r
gX+54yeLqh4opLsVEnYh0umb5XXc08m/tDhhUNqPWQZhUBubN3oPqdam9CO5Q+n
Y2tVqKp3HtC2W0Mc6rvUitlKtopIwVjvNDTnSWxDdtPy5pWmA42Ko4+a5fRNDBJ
55JT4FgPyjHsi5PZTtiSIF60y38ys7feOMUCAwEAaOAcqIwggKeMIGoBgNVHSAE
gaAwgZ0wBgYEVR0gADCBkgYNKwYBBAGDdQIBAQQDETCBgDALBgggBgEFBQcCARYZ
aHR0cDovL3BvbG1jeS5lYWR0cnVzdC5ldTBXBgggBgEFBQcCAjBLDELtdWJvcMjYy
NDAwFTATBgNVBASMDExlZ2FsIFBlcnVbjCCASiWdQYJKoZIhvcNAQEBBQADggEP
aWdpdGFsIFRydXN0LCBTLkwuMBIGA1UdEwEB/wQIMAYBAf8CAQAwdGyDVR0PAQH/
BAQDAgGGMB0GA1UdDgQWBbT62Qqiacv/aK/ymon/VpRUG7OZjzBjBgNVHRIEXDBa
gQ5jYUBlYWR0cnVzdC5ldYYWaHR0cDovL3d3dy5lYWR0cnVzdC5ldYYVaHR0cDov
L2NhLmVhZHRydXN0LmV1hhlodHRwOi8vcG9saWN5LmVhZHRydXN0LmV1MGMGA1Ud
EQRcMFqBDMNhQGvHhZHRydXN0LmV1hhZodHRwOi8vd3d3LmVhZHRydXN0LmV1hhVo
dHRwOi8vY2EuZWFKdHJ1c3QuZXWGGWh0dHA6Ly9wb2xpY3kuZWFKdHJ1c3QuZXUw
HwYDVR0jBBGwFoAUH9RrsGOGDAsJjEJU916HRQxK5kwSQYDVR0fBEIwQDA+oDyG
OoY4aHR0cDovL2Nybc5lYWR0cnVzdC5ldS9lYWR0cnVzdC1yb290LXJzYTlWNDhl
YWRxMjAxOS5jcmwweAYIKwYBBQUHAQEeBDBqMEMGCCsGAQUFBzAChjdodHRwOi8v
Y2EuZWFKdHJ1c3QuZXUvZWFKdHJ1c3Qtcm9vdC1yc2EyMDQ4ZWFKcTIwMTkuY3J0
MCMGCCsGAQUFBzABhhodHRwOi8vb2Nzc5lYWR0cnVzdC5ldTANBgkqhkiG9w0B
AQsFAAOCAQEAI5MNqYKLh2Is3Hps6xy0E4AYTmWqdlvNjRI9syzlPcEt5UxTk24
M7qzJ1wlC7I+xyJ11vR8FNTCXXHnCS0rgDXTIVl3YhxvfvhwxcXYITUPzK1LTte5
```



sJ4cyaAE5c701XWZFPPhicRxCPCPN1vgjD5CMuHB31LwbDzda28kpuvv247+WudKbG  
XoHw6dyM5MJEU0f4q7X/Tw+Eiv917+zIcfCn5A9hS3RSYb023DrqKQkrQoH/zhoH  
EdBwdGldCHMfy/nox/RhfSy5YCZY380hzf01RB/i25hHsMBZpLjN673d3a2nsOQ  
ShUd/8socvS7/YbN09fOuEcSZItak8uZyA=  
-----END CERTIFICATE-----

13.3.24 EADTrust RSA 2048 SubCA For Qualified Certificates 2019

-----BEGIN CERTIFICATE-----  
MIIGeDCCBWCgAwIBAgIJAJYIF4d0g4kSMA0GCSqGSIb3DQEBCwUAMIGcMUIwQAYD  
VQQDDdlFQURUcnVzdCBSU0EgMJA0OCBSb290IENBIEZvcjBRdWFsaWZpZWQgQ2VY  
dGhmaWNhdGVzIDlwMTkxLzAtBgNVBAoMJKV1cm9wZWZuIEFnZW5jeSBvZiBEaWdp  
dGFsIFRydXN0LCBTLkwuMQswCQYDVQQGEwJFUzEYMBYGA1UEYQwPVkFURVmtQjg1  
NjI2MjQwMjB4XDTE5MDYwNjEwNTYyMVoXDTM1MDYwMjEwNTYyMVowgBmXQDA+BgNV  
BAMMN0VBRFRydXN0IFJFTQSAyMDQ4IFN1YknBIEZvcjBRdWFsaWZpZWQgQ2VydGlm  
aWNhdGVzIDlwMTkxLzAtBgNVBAoMJKV1cm9wZWZuIEFnZW5jeSBvZiBEaWdpdGFs  
IFRydXN0LCBTLkwuMQswCQYDVQQGEwJFUzEYMBYGA1UEYQwPVkFURVmtQjg1NjI2  
MjQwMRcWFQYDVQQLDA5OYXRlcmFsIFB1cnNvbWVkbWwvOpZ6VootOuD4eLdm4KrZ8AFwdUAvzu  
u5ckSIINcwDjxP3wcoA1Dtp5PKLoPeniDQ+LABxKpZr+IbTJw3MRoJMCxyd3FoZG  
riqorsVPH9SD8wM/ppNULtdW+K1WD6KTy6vwrJ+f4tLCW8/DmCFbOYYAnAeiATP5  
oCLdl5JU62DeKdj085n31q0STN2wu6B9bqLer85FuhpoJagGVMM4r4sGAhH8mLGC  
B+/o+kNQLXENXmf/U8gSnfixB6QDRGuW57i6QUnrig301fYYluPNl4CqLnWwVGLM  
L5AtCGQYFEIe89ixmQ9H/osuewn/tDzuqCAAiMCAwEAAaOCAQIwggKeMIGoBgNV  
HSAEgaAwgZ0wBgYEVR0gADCBkgYNkwyBBAGDdQIBAQGDETCBgDA1BggrBgEFBQcC  
ARYZaHR0cDovL3BvbGljeS5lYWR0cnVzdC5ldTBXBggrBgEFBQcCAjBLDELtdWJv  
cmRpbmF0ZSBZDZkXj0aWZpY2F0ZSBBDXR0b3JpdHkuIEV1cm9wZWZuIEFnZW5jeSBv  
ZiBEaWdpdGFsIFRydXN0LCBTLkwuMBIGA1UdEwEB/wQIMAYBAf8CAQAwDgYDVROp  
AQH/BAQDAGGMB0GA1UdDgQWBRR3P0yqvu62v7vRk7JZ9w9/nundTBjBgNVHRIE  
XDBagQ5jYUBlYWR0cnVzdC5ldYYWaHR0cDovL3d3dy5lYWR0cnVzdC5ldYYVaHR0  
cDovL2NhLmVhZHRydXN0LmV1hhlodHRwOi8vcG9saWN5LmVhZHRydXN0LmV1MGMG  
A1UdEQRCMFqBDMNhhZHRydXN0LmV1hhZodHRwOi8vd3d3LmVhZHRydXN0LmV1  
hhVodHRwOi8vY2EuZWZkdHJlc3QuZXZlZWdWWh0dHA6Ly9wb2xpY3kuZWZkdHJlc3Qu  
ZXUwHwYDVROjBBGwFoAUH9RrsGOGDAsJJEJum916HRQxK5kWSQYDVROfBEIwQDA+  
oDygOoY4aHR0cDovL2Nybc5lYWR0cnVzdC5lds9lYWR0cnVzdC1yb290LXJzYTlw  
NDhlYWwRmJAxOS5jcmwweAYIKwYBBQUHAQEEdBqMEMGCCsGAQUFBzAchjdodHRw  
Oi8vY2EuZWZkdHJlc3QuZXUvZWZkdHJlc3QtcmlvZC1yc2EyMDQ4ZWZkcTlwMTku  
Y3J0MCMGCCsGAQUFBzABhhhdodHRwOi8vb2Nzc5lYWR0cnVzdC5ldTANBgkqhkiG  
9w0BAQsFAAOCAQEAdBpKcP8Acq/FqeeytxZPPJPJ78EygUtnOoSmt4KSmQ80teG8  
kKkd+ZQp7z3bsfxywShRXJjBFXq/ulzXBbClTrw6jWYCF6HbQKBdv6pE8g6vw3h/  
Zv2QB48PjbcJx8pyTos6bd8qTb99m5XPZPdx5pxQv6gjZ33seizHpsOv+PvCXRLQ  
65OnvbrNIZpgmt eqAb/Uj7swKuW2TkF7jeadbsAltb5W7Vs2D1Jf+FvWx4asqpCC  
Od8Ec1LBiaVeQ3fzP41/Se/plE3YhqlAckr8hGmz4ILCNkssePtORbFdr3jh4FtU  
cka3JrUxJgQ0PEk2lCdWrtRrJywKValDWs0E3w==  
-----END CERTIFICATE-----

13.3.25 EADTrust RSA 2048 SubCA For Non-Qualified Certificates 2019

-----BEGIN CERTIFICATE-----  
MIIGaDCCBVCgAwIBAgIIR0EHGHZVvkWdQYJKoZIhvcNAQELBQAwwAaxRjBEBgNV  
BAMMPUVBRFRydXN0IFJTSQAyMDQ4IFJvbn3QgQ0EgRm9yIE5vbi1RdWFSaWZpZWQg  
Q2VydGlnaWNhdGVzIDIwMTkxLzAtBgNVBAoMJKV1cm9wZWFuIEFnZW5jeSBvZiBE  
aWdpdGFsIFRydXN0LCBTLkxwMQswCQYDVQQGEWJFUzEYMBYGA1UEYQwPvPkFURVMT  
Qjg1NjI2MjQwMB4XDTE5MDYwNjExNDkzMl0XDTM1MDYwMjExNDkzMlowZ4xRDBC  
BgNVBAMMO0VBRFRydXN0IFJTSQAyMDQ4IFN1YkNBIEZvcjBOb24tUXVhbGlnaWVkbG  
IENlcnRpbzZm1jYXRlcjYyMDE5MS8wLQYDVQQKDCZFdXJvcGVhbiBBZ2VuY3kgb2Yg  
RGlnaXRhbCBUcnVzdCwgUy5MLjELMAkGA1UEBhMCRVMxGDAWBgNVBGE1ZBVEVT  
LUI4NTYyNjI0MDCCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAN6kUKdb  
TiD/z68si8qvnGoJyr80GkHl5yaorZto0clBeSNCu8Xna8DBvWHtBm6nFqoMIpXB  
aKUGXCCNY0FeXSDY0g3XnUsJm88aaosRs+DpXPiCrJuoGWeH9q7ASnE2ty14X2T  
lK/+tuozxx3qg+oS1Zk0wC+DroHbTDeTrfQfjRgycmL8NSa0l6+OwidXNx/63q4l  
X7pu/7TyxcyTC/ujrpsSHGrEXFyG9QdzfmokcDjBIx/IEZzuGghs+1b1Xhr2UFAj  
QnelueZHUoLM+uXXYeFoAqbbUDs7lGW7iJ+Z5MURs/idrWUAuNl6ferJE9W3kkGr  
5Lc0DBuSIMknNEsCAwEAAaOCAqQwggKgMIGoBgNVHSAEgaAwgZ0wBgYEVR0gADCB  
kgYNkYBBAGDdQIBAQQGpIDCBGdAlBggrBgEFBQcCARYZaHR0cDovL3BvbG1jeS5l  
YWR0cnVzdC5ldTBXBggrBgEFBQcCAjBLDELtdWJvcmlpYmF0ZSBZSDZlJ0aWZpY2F0  
ZSBBDXRob3JpdHkuIEV1cm9wZWFuIEFnZW5jeSBvZiBEaWdpdGFsIFRydXN0LCBT  
LkxwMBIGA1UdEwEB/wQIMAYBAf8CAQAwDgYDVR0PAQH/BAQDAgGMB0GA1UdDgQW  
BBTn6+kvcuv5Wb19U0LOGNDPKFkXIjBjBgNVHRIEXDBagQ5jYUB1YWR0cnVzdC5l  
dYYWaHR0cDovL3d3dy5lYWR0cnVzdC5ldYYVaHR0cDovL2NhLmVhZHRydXN0LmV1  
hhlodHRwOi8vcG9saWN5LmVhZHRydXN0LmV1MGMA1UdEQRCMFqBDmNhhQGVhZHRy  
dXN0LmV1hhZodHRwOi8vd3d3LmVhZHRydXN0LmV1hhVodHRwOi8vY2EuZWFKdHJ1  
c3QuZXZlZG90dHA6Ly9wb2xpY3kuZWFKdHJ1c3QuZXUwHwYDVR0jBBgwFoAUHj90  
U0LYXX1X0p370mwGG1FA288wSgYDVR0fBEMwQTA/oD2gO4Y5aHR0cDovL2Nybc5l  
YWR0cnVzdC5ldS9lYWR0cnVzdC1yb290LXJzYTIwNDhlYWRucTIwMTkuY3JsMHkG  
CCsGAQUFBwEBBG0wazBEBggrBgEFBQcCAoY4aHR0cDovL2NhLmVhZHRydXN0LmV1  
L2VhZHRydXN0LXJvbn3QtcnNmMjA0OGVhZG5xMjAxOS5jcnQwIwYIKwYBBQUHMAGG  
F2h0dHA6Ly9vY3NwLmVhZHRydXN0LmV1MA0GCSqGSIb3DQEBCwUAA4IBAQB16M+K  
gaegSWpNfr4AIdPBWn2Tr9nRSaNCQ18j4H4MyavrKdyjiLuOvSfQzhYVsxDv8oy1  
zmHaG2ZX1IZKic24KiGnzJQ8TerrYBozjmd19jifyEKLicRIUEojVENKDNQPBcoT  
qxHFNPpL5VjOS/ga+s8iKBkBCMNkiCXwVaThq5QYr0fu8Kuf1u5xV1EN02ju82pm  
RfHppoDAZycCqFq31VmoMIc3g3hHpdkxmWdc5vAAAtKfWAvAlm2VCG6BJLEt/sk7o  
219gnZ63MDT61E01IkCrW06sCt5kPgXxRUde6IenbAhfGzcfZ8mPvoTveJpRUEgd  
lGARsw6cTjNMK8mg  
-----END CERTIFICATE-----

13.3.26 EADTrust RSA 4096 SubCA For Qualified Web DV/OV Cert 2019

-----BEGIN CERTIFICATE-----  
MIIHkzCCBROgAwIBAgIIZGZmQkr4M5cwDQYJKoZIhvcNAQELBQAwwAYQxRDBCBgNV  
BAMMO0VBRFRydXN0IFJTSQA0MDk2IFJvbn3QgQ0EgRm9yIFF1YWxpZm1lZCBXZWIG  
RFYvT1YgQ2VydCAyMDE5MS8wLQYDVQQKDCZFdXJvcGVhbiBBZ2VuY3kgb2YgRGl  
naXRhbCBUcnVzdCwgUy5MLjELMAkGA1UEBhMCRVMwHhcNMTEyMDE5MDYwMjExNDkz  
Ml0XDTM1MDYwMjExNDkzMl0wZ4xRDBCBgNVBAMMO0VBRFRydXN0IFJTSQA0MDk2IF  
Jvbn3QgQ0EgRm9yIFF1YWxpZm1lZCBXZWIGRFYvT1YgQ2VydCAyMDE5MS8wLQYD  
VQQKDCZFdXJvcGVhbiBBZ2VuY3kgb2YgRGlnaXRhbCBUcnVzdCwgUy5MLjELMAkG  
A1UEBhMCRVMwHhcNMTEyMDE5MDYwMjExNDkz



RVMwggIiMA0GCSqGSIB3DQEBAQUAA4ICDwAwggIKAoICAQCwSupgVOitys8szrKDeMCvqgHgQyX3HA02ifanOGpBFbEpZc2Ts8y7ueKj5t6BVHPIEcvQolUR7202L9Ii2TnjfyIWF6vwwrtuKF4vOy3PUJMohrFOAGGfwoBcltSmfY09jNqolWBlG25cxLYIEa2WCSVYzolaPiio9Az/BMTZBm87RgIUqIs+6SDPAyA6ZUCERziKZaK1zAGS51SaDaDYhkttApjbtFv055clX7QX/hQes8EuRL6S/FDTWRWkGiUUVITZKqAZnNU9ZnjCmoV5gD7Gv/zQeOgpzDSyDP3ZdMKWObAlcS65sP0s+Oy+tv90RejYQljoJg70EC/Vg1i1aNR6sT3tdi2PN1UDPLNGoXtUDAsmrsNC97X0nj0LSLw+fsHxjZFB77eXy5KvneohNg8z8u/1lDUiO+3XdRym6uk3HLXyJTaYpZwn/F6NrZgSnwhvR/s2FMjO+cdEUfyYG0JczU9PmxYp0vDU94etdWYFTRel037MO79Td3W7fSOhfhwHSO4SAycVXJI0foCdHRCVPH0GgBVQmrh2zH80dmZcmFeNO7qrc7v4GyLl54ZNw9kK0RiblrwJdJVRSU3FmDV2PNvkScti/ZyJdFXWmXhlTaA92eSa8h6KtVb+th09nmhobUaw/XJl1r9TEuGegl4UhlqPZ52daBEQ51eQQIDAQABO4IBnzCCAzwSwYDVR0gBEQwQjAGBgRVHSAAMDgGDSsGAQQBg3UCAQEBGxEwJzAlBggrBgEFBQcCARYZaHR0cDovL3BvbGljeS51YWR0cnVzdC5ldTASBgNVHRMBAf8ECDAGAQH/AgEAMA4GA1UdDwEB/wQEAwIBhjAdBgNVHQ4EFgQUUGru8dcfpa4oD6W5AMAn884urLcwHwYDVR0jBBgwFoAUtsV5nhYchdlSHcsc0ojFLMmvDUcwTAYDVR0fBEUwQzBBOD+gPYY7aHR0cDovL2Nybc51YWR0cnVzdC5ldS91YWR0cnVzdC1yb290LXJzYTQwOTZlYWRkdm92MjAxOS5jcmwwewYIKwYBBQUHAQEebzBtMEYGCCsGAQUFBzACHjpodHRwOi8vY2EuZWFKdHJlc3QuZXUvZWFKdHJlc3Qtcm9vdC1yc2E0MDk2ZWFKZHZvdjIwMTkuY3J0MCMGCCsGAQUFBzABhhodHRwOi8vb2NzcC51YWR0cnVzdC5ldTAdBgNVHSUEFjAUBGgrBgEFBQcDAQYIKwYBBQUHAwIwDQYJKoZIhvcNAQELBQADggIBAG0egb6nmjfLyVdrWKq2CsZu8pSEV5ixWAw4AvID5ruZ6DNp4VMYBEHKNiY2EQFCOIi1Gg79B2oYUwRXzD6lkorN3zix0dnn8fvpwv+kWTI2LyIUlRtyv0/Vg/orE/ZNVtEqrnY7hcGiFh+Kufw8uN84TusMCDOLdxVVb+0lYmhEjN3S6y9Gjp41KK4Hw2Ou4RBmJSv5D7HZibgWVwwWEk2sdnt0319YTbRC3A+3jAK2CKRPmZvkBPdJDXFbHi3Bd7qnf80yOsn+Fig/Ej8+F+CIb8+97/kAngAS8L0uRHU9CW/4/ogA8ypHTScQLWPeHRFwV0lC1S0AmP6rGM+OEK3vpFsrtp0kHHBROS5Mmtek3CFssdXal7ftZZJs2l2HQ1MM/OgplNSKHku/soVC8bTdn5g5+yfUStdURRIjgkDxQCuyqXfCJf29smDzGCwQ2y7RSgLS0Qr0uasDojs92r3BPrp/hFvvlkjsN4IvfgArnJfndzEfubf4tgUT8doxadAgHect64fMwlkwdtns3cVFmvg9lySzKRWe5KIWVO2NymeuryRbRvAY2dVYBr1ARFcX4Nv1I0apLGrAmJxRD4elDNuDCzE1T2EvVar0l68W90I5WVACn0+eQCAworop0lXK12YcsaaRKd3NhlVrDxjv1Dg1sLTsbhUFv2RvQK  
-----END CERTIFICATE-----

13.3.27 EADTrust RSA 4096 SubCA For Qualified Web EV/PSD2 Cert 2019

-----BEGIN CERTIFICATE-----  
MI IHMzCCBRugAwIBAgIIRhJxmAQWRCYwDQYJKoZIhvcNAQELBQAwYYxRjBEBGvN BAMMPUVBRFRydXN0IFJtQSA0MDk2IFJvb3QgQ0EgRm9yIFFlYWxpZml1ZCBXZWIG RVYvUFNEMiBDZXJ0IDIwMTkxLzAtBgNVBAoMjKv1cm9wZWZuIEFnZW5jeSBvZiBE aWdpdGFsIFRydXN0LCBTLkwuMQswCQYDVQQGEwJFUzAeFw0xOTA2MDYxMTM3MDJa Fw0zMTA2MDMxMTM3MDJAMIGEMUQwQgYDVQQDDDFURUcnVzdCBSU0EgNDA5NiBT dWJDQSBB3IGUXVhbGlmaWVkiFdlYiBFVi9QU0QyIENlcnQgMjAxOS5jcmwwewYIKwYBBQUHAQEebzBtMEYGCCsGAQUFBzACHjpodHRwOi8vY2EuZWFKdHJlc3QuZXUvZWFKdHJlc3Qtcm9vdC1yc2E0MDk2ZWFKZHZvdjIwMTkuY3J0MCMGCCsGAQUFBzABhhodHRwOi8vb2NzcC51YWR0cnVzdC5ldTAdBgNVHSUEFjAUBGgrBgEFBQcDAQYIKwYBBQUHAwIwDQYJKoZIhvcNAQELBQADggIBAG0egb6nmjfLyVdrWKq2CsZu8pSEV5ixWAw4AvID5ruZ6DNp4VMYBEHKNiY2EQFCOIi1Gg79B2oYUwRXzD6lkorN3zix0dnn8fvpwv+kWTI2LyIUlRtyv0/Vg/orE/ZNVtEqrnY7hcGiFh+Kufw8uN84TusMCDOLdxVVb+0lYmhEjN3S6y9Gjp41KK4Hw2Ou4RBmJSv5D7HZibgWVwwWEk2sdnt0319YTbRC3A+3jAK2CKRPmZvkBPdJDXFbHi3Bd7qnf80yOsn+Fig/Ej8+F+CIb8+97/kAngAS8L0uRHU9CW/4/ogA8ypHTScQLWPeHRFwV0lC1S0AmP6rGM+OEK3vpFsrtp0kHHBROS5Mmtek3CFssdXal7ftZZJs2l2HQ1MM/OgplNSKHku/soVC8bTdn5g5+yfUStdURRIjgkDxQCuyqXfCJf29smDzGCwQ2y7RSgLS0Qr0uasDojs92r3BPrp/hFvvlkjsN4IvfgArnJfndzEfubf4tgUT8doxadAgHect64fMwlkwdtns3cVFmvg9lySzKRWe5KIWVO2NymeuryRbRvAY2dVYBr1ARFcX4Nv1I0apLGrAmJxRD4elDNuDCzE1T2EvVar0l68W90I5WVACn0+eQCAworop0lXK12YcsaaRKd3NhlVrDxjv1Dg1sLTsbhUFv2RvQK  
-----END CERTIFICATE-----

EGuDzmmDyVRc9tE1GiSSp53esfEj7tXXmH74032rOJz0ycGVs51KaMNClyNHeUOW  
SsYvaeHAmG3fWl7Z+/9SBac6dlEh8Imip2sagmLiQLKs+CflU6N+rkmX7deOM6hs  
dJDnHsXB/WhBm8gBj1WuX4dnkjs67HK6MKh/FGoMCyihISNN9PMFJQOMGIy1LvW7  
U1LdlxcJfwqmT4rzUiXNL3DcHa9Aj+Qd7SEGw0Rjz0oWustEdLPqfZXVsvzJDLep  
fhTnzc290tvPaMuppDLXkVAGuHoTmVkcAwEAAaOCAaMwggGfMEsGA1UdIAREMEIw  
BgYEVROgADA4Bg0rBgEEAYN1AgEBAYMRMCcwJQYIKwYBBQUHAQEwGWh0dHA6Ly9w  
b2xpY3kuZWFKdHJ1c3QuZXUwEgYDVR0TAQH/BAGwBgEB/wIBADA0BgNVHQ8BAf8E  
BAMCAYYwHQYDVR0OBBYEFIT082uqplcwJ/fDEpKg5eCbWh5EMB8GA1UdIwQYMBAA  
FLQeKNTqgmAPEAR0y3eUaUwRh+JEME4GA1UdHwRHMEUwQ6BBOD+GPWh0dHA6Ly9j  
cmwuZWFKdHJ1c3QuZXUvZWFKdHJ1c3Qtcm9vdC1yc2E0MDk2ZWFKkZXZwc2QyMjAx  
OS5jcmwWFQYIKwYBBQUHAQEECTBvMEgGCCsGAQUFBzACHjxodHRwOi8vY2EuZWFK  
dHJ1c3QuZXUvZWFKdHJ1c3Qtcm9vdC1yc2E0MDk2ZWFKkZXZwc2QyMjAxOS5jcnQw  
IwYIKwYBBQUHMAGGF2h0dHA6Ly9vY3NwLmVhZHRydXN0LmV1MB0GA1UdJQQWMBQG  
CCsGAQUFBwMBBggrBgEFBQcDAjANBgkqhkiG9w0BAQsFAAOCAgEAnVdxWWcf0ME  
71hVxgNgaiGr5lsxPnZvme9gc1XL8WLq8Nbcq57ZHwHtgWwIHfVpUDzlgxPC963  
jfgZgr/6ows7S5lQ9fOZqPsoL9axi9L0k9F74s7/JRyRgqpvkmW2ulh4WLB92KJH  
XgbCazHS87a+uTjqrUBerU2lMNM0HD3FD1QbXWvb2pK5ukdaaaQKnujAJRLLiUso  
rhUdGMM/0uUjokzyAiZc051DGzIUdrbqfVoplyik2zdS3XmcG0mY+/P+0ILiKff  
fV10jyTnyxIt5zL/b9uliyjq3Uy2ZJ6WPdYuFhIyVCjEW8Nns3Gne4KgHUwitM5D  
KS39q4U/MzuY2E5p9E5gRT5ZWxekrc2MCGSoQcjbKozDlAFx7V6Fzdn3D8tJA0C  
22MLblaSNg0Wxh1HnN3/tP93JogwKNuHQcYAZ1vXK5PI4JCok8QuQNHGZT3nJlLM  
lFtEhNdxjBI/Lahje2/yhfUt+1ZUGHYjVEk03CQv35zTPDcWZSUj/GxxOURoAvQc  
loTPCF/y0bfqD4vVaoESERX0vvijbZw2TW4HHvsx6uGY+INVSsUTHjoWbuwsx/x/  
jmdHoVilQrQbWfzlpYovhcoyxuFNDeBd8RB0PXv003dWTMzSeQWPga7HZmo24ZHQ  
ivDguM8/3NuSF/1KI2p/Eh7g2JPEGSI=  
-----END CERTIFICATE-----

### 13.3.28 EADTrust RSA 4096 SubCA For Qualified Certificates 2019

-----BEGIN CERTIFICATE-----  
MIIDtCCBl2gAwIBAgIIIZDAGdySXC3IwDQYJKoZIhvcNAQELBQAwGzWxQjBABGNV  
BAMMOUVBRFRydXN0IFJFTQSA0MDk2IFJvbnR3QgQ0EgRm9yIFF1YWxpZml1ZCZBDZSJ0  
aWZpY2F0ZXMGmJAxOTEvMC0GA1UECgwmRXVyb3BlYW4gQWdlbmN5IG9mIERpZ2l0  
YWwgVHJ1c3QsIFMuTC4xZCzAJBgNVBAYTAKVTMRgwFgYDVRQRhDA9WQVRFUy1CODU2  
MjYyNDAwHhcNMtKwNjA2MTA1NjU3W3hcnmZUwNjAyMTA1NjU3WjCBsTFAMD4GA1UE  
Aww3RUFEVHJ1c3QgUlNBIDQwOTYgU3ViQ0EgRm9yIFF1YWxpZml1ZCZBDZSJ0aWZp  
Y2F0ZXMGmJAxOTEvMC0GA1UECgwmRXVyb3BlYW4gQWdlbmN5IG9mIERpZ2l0YWwg  
VHJ1c3QsIFMuTC4xZCzAJBgNVBAYTAKVTMRgwFgYDVRQRhDA9WQVRFUy1CODU2MjYy  
NDAXFTATBgNVBASMDExlZ2F5IFBlcnNvbWVjCCAiIwDQYJKoZIhvcNAQEBBQADggIP  
ADCCAgcCggIBAKsZ4po900f2BEfKsZB1FhlIgfqXksUEDv+aj+QSQkdXhmU3XYIgt  
2vd2PtjUNrglCyuxr8ix9x90yEhz1wMwVVRs10btEN4Aw9qzSZrQyKewx5SY7Y  
7YSYa4P4SYrVZSWO/4RXLfcAec9Q4eM3owyuYFTfFFyGHJE43hKu+THfHw0bghPy  
DjqGe+15/xh7JcDv1Mc56kOU/tcKQd7ack3FQqiV9v+D+ki70f2E2pbUY1zhCvx9  
/vTAPVOzQ977IqzW0CsU51VnSjsxwph4XI3HdTQot4FKY7/U72/oDQGaJg6Dzd2  
awfBRQSLfASL1rfHSLCo18ycEog90MiG0wJ0dL82gU+sCdFxsja6clc/tDpa6A4k  
feTHHJocHmbhkkBtTxw55CdUSdymbb6+c0brqotKiCbM2NPINTLGNAAwERW0N2gM  
mbgq13tQlY4FvGU9oIk1FzFfWpiP7ELOEAA+7f+3YscaoQ7z1VvcZ17xF/gi/KnE  
EjB0UBL10K8naU61FXS0fakgG7JF0Tt5GSGDiNX/HE8p+0VOu6GOKKogTvkthgs+  
K1h66tHoa3sUA3aMo1IgMifOzwr7sfzKktTuTvDFRptvifx7/svtCjOu5k7sPxU4  
vNgULtWHcwe9glkgdf0p79+Sj0BDac+kPMIIMaSTAr4m70EdlWU1mBD3AgMBAAGj  
ggKiMIICnJCbqAYDVR0gBIGgMIGdMAYGBFUDIAAwgZIGDSsGAQQBg3UCAQEBGxEw

gYAwJQYIKwYBBQUHAgEWGWh0dHA6Ly9wb2xpY3kuZWFKdHJ1c3QuZXUwVwYIKwYB  
BQUHAgIwSwxJU3Vib3JkaW5hdGUgQ2VydGlmaWNhdGUgQXV0aG9yaXR5LiBFdXJv  
cGVhbiBBZ2Vuy3kqb2YgRGlnaXRhbCBUcnVzdCwgUy5MLjASBgNVHRMBAf8ECDAG  
AQH/AgEAMA4GA1UdDwEB/wQEAwIBhjAdBgNVHQ4EFgQUUMS5X72kv2esv2yA4CeOE  
pyxJ/0UwYwYDVR0SBFwwWoEOY2FAZWFkdHJ1c3QuZXWGFmh0dHA6Ly93d3cuZWFK  
dHJ1c3QuZXWGFWh0dHA6Ly9jYS51YWR0cnVzdC5ldYYZaHR0cDovL3BvbG1jeS51  
YWR0cnVzdC5ldTBjBgNVHREEXDBagQ5jYUB1YWR0cnVzdC5ldYYWaHR0cDovL3d3  
dy51YWR0cnVzdC5ldYYVaHR0cDovL2NhLmVhZHRydXN0LmV1hhlodHRwOi8vcG9s  
aWN5LmVhZHRydXN0LmV1MB8GA1UdIwQYMBaAFOPCMDRHA8APF7JjsFAT5RSxDFn0  
MEKGA1UdHwRCMEAwPqA8oDqGOGh0dHA6Ly9jcmwuZWFKdHJ1c3QuZXUvZWFKdHJ1  
c3Qtcm9vdC1yc2E0MDk2ZWFKcTIwMTkuY3JsMHgGCCsGAQUFBwEBBGwwajBDBggr  
BgEFBQcwAoY3aHR0cDovL2NhLmVhZHRydXN0LmV1L2VhZHRydXN0LXJvb3QtcnNh  
NDA5NmVhZHEyMDE5LmNydDAjBggrBgEFBQcwAYYXaHR0cDovL29jc3AuZWFKdHJ1  
c3QuZXUwDQYJKoZIhvcNAQELBQADggIBAB5p4UleQ5K3+sw0s2TPQLbleanJmCEX  
MjeNkv4wpxndMXcKI6x7qkZvwtP/vW6a8OhpTeRR2pmQwbhh4vFTI1GeHGxSDF6N  
hJi71K5xy71YL/P4etc5P12MlycKAtDFPSJoN1+utmXhADZQ4r65riNTwhJHCqq3  
abXd13fkoJzqouqOpy8ndFY5tuVDMXU9ih411gV5dMs2pVgre/gS7U4nPA3OFRSV  
mxZR+u7Q6YPmXoq06iG5F6uAhQGibiaUf4pUYcTJTQF5xhLSEmfHs2fwkFs70YBF  
wLVdpDsPwLieYtZlpKvQcOWWpC1wujklxOzBlUWB/0ohm9Qw6ykw+2MUyFcZcQRT  
C/Fn9UqAlFyUMT0F5hIvZ4w9YvqsBJXI2taPg1dMgM5TvXa41pjPAqN7+1BgtDH0  
gfEmERpQpbbfILCYvl/uoVn25ZoEr6SKSCfBV1MFRr7Fm0G23x5vARR82chFOVF4  
c8MVAsfCKJZKmirQLLedf8cSMPB4pkFrTKPkXPjs8RsHLBOQONT9pNm/DVSD7xwe  
Y+qqfoHEiD3vNqiQXTFvUNlkcbhAGzqAMZC2GGejoASNq9VQACu6vNww1nd/CPIL  
PPPCnJKPKLbYQPWqndA24K9ZlrpOECg0YGFqxW5mbv4uWD5dAYC/bokXPezxa jyv  
eVNwq7shidsX  
-----END CERTIFICATE-----

### 13.3.29 EADTrust RSA 4096 SubCA For Qualified Certificates 2019

-----BEGIN CERTIFICATE-----  
MIIIDzCCBl+gAwIBAgIISHZjZSJOMyIwDQYJKoZIhvcNAQELBQAwwZwQjBABgNV  
BAMMOUVRFRydXN0IFJTSQA0MDk2IFJvb3QgQ0EgRm9yIFF1YWxpZm1lZCZBDZSJ0  
aWZpY2F0ZXMGmJAxOTEvMC0GA1UECgwmRXVyb3B1YW4gQWdlbmN5IG9mIERpZ210  
YWwgVHJ1c3QsIFMuTC4xZCzAJBgNVBAYTAkVTMRgwFgYDVQRhDA9WQVRFUy1CODU2  
MjYyNDAwHhcNMtkwNjA2MTA1NjM1WhcNMzUwNjA5MTA1NjM1WjCBszFAMD4GA1UE  
Aww3RUFEEVHJ1c3QgUlNBIDQwOTYgU3ViQ0EgRm9yIFF1YWxpZm1lZCZBDZSJ0aWZp  
Y2F0ZXMGmJAxOTEvMC0GA1UECgwmRXVyb3B1YW4gQWdlbmN5IG9mIERpZ210YWwg  
VHJ1c3QsIFMuTC4xZCzAJBgNVBAYTAkVTMRgwFgYDVQRhDA9WQVRFUy1CODU2MjYy  
NDAXFzAVBgNVBAsMDk5hdHVyYWwgUGVyc29uMIIICiJANBgkqhkiG9w0BAQEFAAOOC  
Ag8AMIICGKCAgEAv4Lh3uZWD1QyEEpjSrPdYiZ5dVY8BqFjx2hvn1odk8q0R9/I  
8AXxtTR2AmqgsDdVXOPCg3hRr+1xaY+fs1WkyfknTzTjXEy9dxXd9Z0MPlRLI3A9  
oZNkFLuQcu/qq19bLV1igrWGwgrJXPyY9T0rAdShfO+1pun5UXRlZAsjtFBM8FCQ  
Uu+8g0yEhRf8yJfjhlaQvTRCtt6305aBsUwyjkSSZl10L3IxgUCs9Kzv2iQXn8te  
B6Gsc380BpgDT3lppS1grRUwzc3nlYw7+NisRxMvjZ0xCdyMl24+PgZ99fKGzDik  
OoKwIJLLUa3ecxgA4xslkcc/F5c4PfbJnUu8oWsp6MO7Z9U09MHA18IFUrW6y5q0  
5aQORm3qLQOXCUO+A6B7EVdJ5VtQZeZsS713G9u5Q1A5xA28KAuqxpIqSEAXWsDu  
nx3j5KKvObIZjVD11iPcXupqn2VoANphS2PHR1pkJIKtbQFoyMEz7pw6VSz4rCmp  
1tE6uwHKPyehXBUnIEbHLYOWLXUED4teNUB+WZpEFC7RyLYdJRKjfpNXC++shc4  
tSsmBzH6CRWcdyxEbgNfaLV82zCGk0wY9OXsQfQZMqAAE/kYDCZelKr5G1Jh/DR8  
SdHet9EuBT92AspFkVbBHoeE2qUlyMG/1X9apNq44P+z3t1aQ8z0m7GOJ7UCAwEA  
AaOCAqIwggKeMIGoBgNVHSAEgaAwgZ0wBgYEVR0gADCBkgYNKwYBBAGDDQIBAQQD

ETCBgDA1BggrBgEFBQCcARYZaHR0cDovL3BvbGljeS51YWR0cnVzdC5ldTBXBggrBgEFBQCcCAjBLDElTdWJvcnRpbmF0ZSBkZXJ0aWZpY2F0ZSBbdXR0b3JpdHkuIEV1cm9wZWFuIEFnZm51jeSBvZiBEaWdpdGfIFRydXN0LCBTLkwUMBIGA1UdEwEB/wQIMAYBAf8CAQAwDgYDVR0PAQH/BAQDAgGMB0GA1UdDgQWBQGM9orzumBUU9p3c3Irr98sLz2+XjbJgNVHRIEXDbaGQ5jYUB1YWR0cnVzdC5ldYYVaHR0cDovL3d3dy51YWR0cnVzdC5ldYYVaHR0cDovL2NhLmVhZHRydXN0LmV1h1odHRwOi8vcG9saWN5LmVhZHRydXN0LmV1MGMA1UdEQRCmfqBDmNhgVhZHRydXN0LmV1hhZodHRwOi8vd3d3LmVhZHRydXN0LmV1hhVodHRwOi8vY2EuZWZkdHJ1c3QuZXWGWW0dHA6Ly9wb2xpY3kuZWZkdHJ1c3QuZXUwHwYDVR0jBBgwFoAU48IwNEcDwA8XsmOwUBPLFLEMFwFwSQYDVR0fBEIwQDA+oDygoOy4aHR0cDovL2Nybc51YWR0cnVzdC5ldS91YWR0cnVzdC1yb290LXJzYTQwOTZlYWRxMjAxOS5jcmwweAYIKwYBBQUHAQEebDBqMEMGCCSAQUFBZACHjdodHRwOi8vY2EuZWZkdHJ1c3QuZXUvZWZkdHJ1c3Qtc9vdc1yc2E0MDk2ZWZkcm9wY3J0MCMGCCSAQUFBZABhhdodHRwOi8vb2Nzc51YWR0cnVzdC5ldTANBgkqhkiG9w0BAQsFAAOCAgEAcPvvo/49EIRP4e0YD9FdeJoBWGImWwFuEIGNw9wizXj7JDISuk/UXZo7ogmpGe4aB219gnJkZhHTAQ4gEIW4yKCUwbyGefmhwmcYoxz/Z9emWzRadrouXGjO+bvVefDr0Azbu0Wotr+aWwp0H6RhUJyZPdTe+r26PskmPxAljbXLrb1JYYbfBEPX13u0jZBQm7BNjGcp5vgjIWTwrT5q8mA3Rakhii1+uv4E7prk05CeSEdbwQz7aJo7snGw2RLO0RmvoPMQe+utRZMYNjWlEyh0ejvivFGcZ5vjL0lFuqHV10+TcZu27zHgpB046XF79rnSpslkeL9MA+7pmUTNLisqTKSVY6LXZjpiudEReMe3q5zdRvfYZAWlarUOMGFNWam/NJswxtPtCxx0Y3QhvbJxL0TzkP+ruxkoKhjUkLH1uWlbrqG1Lg9CNGG14Db16fVwUlyRRqaJH/aRKTZTgNHZRpt6gFxpO3q6YIy4TE/+odcIqlIrJNbt5FiqOt2D82WQjTKIGbgy+BqtdG40xh/BaXMVkx08VjJHiETKpombbm6gUedEXhqFcxLe3V3H8hoq0AS48YId5GndkZJxww/pA7Hx2d9J1IgpsP1QGdYc3fAtxCMB/RoeMklzgRilG9mT5pkBK3epxZA+oEamXcIXzflLzmCrrerEILw=

-----END CERTIFICATE-----

13.3.30 EADTrust RSA 8192 SubCA For Qualified Web DV/OV Cert 2019

-----BEGIN CERTIFICATE-----

MIILKzCCBxOgAwIBAgIIi1xABI5kTcwDQYJKoZIhvcNAQENBQAwYQYxRDBCBgNVBAMMO0VBRFRydXN0IFJFTQSA4MTkyIFJvb3QgQ0EgRm9yIFF1YWxpZmllZCBXZWlgrRfYvTlYgQ2VydCAyMDE5MS8wLQYDVQQKDCZlZXRydXN0LCBTLkwUMBIGA1UdEwEB/wQIMAYBAf8CAQAwDgYDVR0PAQH/BAQDAgGMB0GA1UdDgQWBQGM9orzumBUU9p3c3Irr98sLz2+XjbJgNVHRIEXDbaGQ5jYUB1YWR0cnVzdC5ldYYVaHR0cDovL3d3dy51YWR0cnVzdC5ldYYVaHR0cDovL2NhLmVhZHRydXN0LmV1h1odHRwOi8vcG9saWN5LmVhZHRydXN0LmV1MGMA1UdEQRCmfqBDmNhgVhZHRydXN0LmV1hhZodHRwOi8vd3d3LmVhZHRydXN0LmV1hhVodHRwOi8vY2EuZWZkdHJ1c3QuZXWGWW0dHA6Ly9wb2xpY3kuZWZkdHJ1c3QuZXUwHwYDVR0jBBgwFoAU48IwNEcDwA8XsmOwUBPLFLEMFwFwSQYDVR0fBEIwQDA+oDygoOy4aHR0cDovL2Nybc51YWR0cnVzdC5ldS91YWR0cnVzdC1yb290LXJzYTQwOTZlYWRxMjAxOS5jcmwweAYIKwYBBQUHAQEebDBqMEMGCCSAQUFBZACHjdodHRwOi8vY2EuZWZkdHJ1c3QuZXUvZWZkdHJ1c3Qtc9vdc1yc2E0MDk2ZWZkcm9wY3J0MCMGCCSAQUFBZABhhdodHRwOi8vb2Nzc51YWR0cnVzdC5ldTANBgkqhkiG9w0BAQsFAAOCAgEAcPvvo/49EIRP4e0YD9FdeJoBWGImWwFuEIGNw9wizXj7JDISuk/UXZo7ogmpGe4aB219gnJkZhHTAQ4gEIW4yKCUwbyGefmhwmcYoxz/Z9emWzRadrouXGjO+bvVefDr0Azbu0Wotr+aWwp0H6RhUJyZPdTe+r26PskmPxAljbXLrb1JYYbfBEPX13u0jZBQm7BNjGcp5vgjIWTwrT5q8mA3Rakhii1+uv4E7prk05CeSEdbwQz7aJo7snGw2RLO0RmvoPMQe+utRZMYNjWlEyh0ejvivFGcZ5vjL0lFuqHV10+TcZu27zHgpB046XF79rnSpslkeL9MA+7pmUTNLisqTKSVY6LXZjpiudEReMe3q5zdRvfYZAWlarUOMGFNWam/NJswxtPtCxx0Y3QhvbJxL0TzkP+ruxkoKhjUkLH1uWlbrqG1Lg9CNGG14Db16fVwUlyRRqaJH/aRKTZTgNHZRpt6gFxpO3q6YIy4TE/+odcIqlIrJNbt5FiqOt2D82WQjTKIGbgy+BqtdG40xh/BaXMVkx08VjJHiETKpombbm6gUedEXhqFcxLe3V3H8hoq0AS48YId5GndkZJxww/pA7Hx2d9J1IgpsP1QGdYc3fAtxCMB/RoeMklzgRilG9mT5pkBK3epxZA+oEamXcIXzflLzmCrrerEILw=

PXX234aA147rAYMO+FteetVPAXeZbf+cWz j2iLEPUYSa2Dl4DJ7LXBIzdrJ83bGo  
KvZeSPuPxt1GvW8OtSk9DeS0S7uAWLeYFVJu8hIAHTRaulsflGolivKLsclp8iy9  
3DushjiID4+RsE5FN/6coq/pprxA6qwnhWWLkdkgyRNJxa8rP9/fW4vQiI+7kfqF  
GM8j17b/iHpXzoiHbrXPM+gGWyZZ/MJlTodFLNq5jZup+6+1S2S/sYBhAl8fAM67  
KNDst008VkgPjSHIjM6QA4pwcLLhCd2aClzwdEWO30+wwuS+7tpneP4P78r1ECN  
nrAgpUBVYKF5F+2h7xOiZu6IZifa0Ri1TKfxVPGUVG/5wKrFzUvEys2SMaD/9C9p  
oKioY/maBjNMHnTiLHwspS5TQaUAd0glUXwIKJaLj1ncsn5jntAv+OCzveSSZOxD  
2PaaStQNr0Bm6PecUvUlu1hm8se7YTXlQnJtGP8us3ifFq1lXRIV8RqHPSB6KLlI  
AIfjAgMBAAGjggGfMIIBmzBLBgNVHSAERDBCMAyGBFUdIAAwOAYNKwYBBAGDdQIB  
AQGDETANMCUGCCsGAQUFBwIBFhloDHRwOi8vcG9saWN5LmVhZHRydXN0LmV1MBIG  
A1UdEwEB/wQIMAYBAf8CAQAwDgYDVR0PAQH/BAQDAgGMB0GA1UdDgQWBRRzoY4  
OeBXoJWZsYxjv2WKyn57FTAfBgNVHSMEGDAWgBSe7QxBgWpv+mYJ+nx/jEhJCDZ9  
ADBMBgNVHR8ERTBDMEGGP6A9hjtodHRwOi8vY3JSLmVhZHRydXN0LmV1L2VhZHRy  
dXN0LXJvb3QtcnNhODE5MmVhZGR2b3YyMDE5LmNybDB7BggrBgEFBQcBAQRvMG0w  
RgYIKwYBBQUHMAKGomh0dHA6Ly9jYS5lYWR0cnVzdC5ldS9lYWR0cnVzdCl1yb290  
LXJzYTgxOTJlYWRkdm92MjAxOS5jcnQwIwYIKwYBBQUHMAGGF2h0dHA6Ly9vY3Nw  
LmVhZHRydXN0LmV1MB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjANBgkq  
hkiG9w0BAQ0FAAOCAEAulcF47Uj9RV84rdUSpbjPve5mB4843uhTTCE1NwGC+uQ  
pkMk+JNG968iRbv2l1aJFz6Rdb0FeXyqN5ppo9ry+aHG4fMNz jGNbVUq77Ua1NAQ  
9uWUHMFBH5Qm05StXuGwbHdqWzOP6PEpYzBpETjUmwUNz jR8HG9SYEs+kPG63x  
xN0R6gynM+aYQPAut+IA/oMrrBeEavYggj9XyJTbHpRj5/b1LYe7CA6J5ru8P9BQ  
PYGnO9M5YWrKd2ua9Znvu91uy7pehUiztOluKbV9GBHszvEUtSis/5eWq7jJ6CMz  
hp9AIOrq35KZI3weyDyw3I7knMZbJIXJj0e7OQds27TDCJWg5b6rY/YBegluZI2x  
kbtZec6NDcV2312luvi93uqyg5ZKOjTm1EQEyhr7UlCxcqQY09j+CtnolH4ng/iX  
AKjon2ve4fM3jVmaulTk4JmQaXRYtuyUJxBP2vNmtHVCQ8mSNUbHucZGQAisNdq7  
DvdSdlXsLKEv4V8Cp9vEhWZ+0iHKUAhITeychOhE1Hnxg/mrD0n4SIOMSxuIPM4j  
lmByaeVUPF2UGQnOnCTsuBgvAuX8zfLXELhg+VZLZ6ZqN1ZeuRQ4F1KKX+jm6zmj  
6pV8dXvs/sUahglxQAmhj4+MQY3lq0kLUkw2h1PKG7Dy/iAvcPXyadh921ZQgztp  
QTKn7J5VvJF7P8w6HbbXa5Em1P3nnfSiuuPhxs/q+2VvhuVm48iCl8913CA82biY  
Kkv7IXGV9Bn4m07YODnw4tJW8SX/Wl072PLQEM85kljeANbVQG0T4/sgDq1QKaVd  
gaYytaabtTpjVXgkaQBIXtCI6TL1mruPGiy7NHmaP6+/RFxsSEYk7QI2ZPEBOK9  
jEVCc2ZpIGTNmg8+eXVU/QrEe41mjwkYrmAbHrqd7mQFovXUrg4QThhcBXE08Tiv  
DHid2PZAYJWE+dZBgKChbV1l/hsTMUaphKFz1Rrvk6CPhs46AaFvbcVeeYJyOIdy  
e3/EJXta/bsRVONbGiVkspkweD2JwbjSRy/FwKs0oHGpBETRbOC9h2VXKC7wpfyt  
6JedKk1TRKR0cH94oOtJD6Q1em5phpSH+CEXogdJCwpYMlnTha0NFujYSfBC/zpU  
1PtAWS1tt8e9YKoBfiaTcqvUtv6pnrBeOyC4Z24nLJtolxGNz/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-----  
MIILMzCCBxugAwIBAgIIIdpISCXEXmWAwDQYJKoZIhvcNAQENBQAwYYxRjBEBGnV  
BAMMPUVBRFRydXN0IFJTTQSA4MTkyIFJvb3QgQ0EgRm9yIFFlYWxpZml1ZCBXZWIg  
RVYyVUFNEMiBDZXXJ0IDIwMTkxLzAtBgNVBAoMjKv1cm9wZWFuIEFfnZW5jeSBvZiBE  
aWdpdGFsIFRydXN0LCBTLkwuMQswCQYDVQQGEwJFuzAeFw0xOTA2MDYxMTQ5MTBa  
Fw0zMTA2MDMxMTQ5MTBaMIGEMUQwQgYDVQQDDDFURUcnVzdCBSU0EgODE5MmVhZHRy  
dXN0LXJvb3QtcnNhODE5MmVhZGR2b3YyMDE5LmNybDB7BggrBgEFBQcDAjANBgkq  
hkiG9w0BAQ0FAAOCAQIAIwMTkxLzAtBgNVBAoMjKv1cm9wZWFuIEFfnZW5jeSBvZiBE  
CgwmRXVyb3BlYW4gQWdlbmn5IG9mIERpZ210YWwvVHJlc3QsIFMuTC4xZCZAJBgNV

BAYTAKVTMIIIEI jANBgkqhkiG9w0BAQEFAAOCA8AMIIECgKCBAEAsSLKuBGGPqZp  
FmyeIJdi45KUoXxS8ikbxnLJsd5ShVdkSFLAhQWuhqrgXCuGCgoWdlmSN+6ERdZC  
XJ5TtIlCpVcHH0fvtuFQSk1PU+/ /Njs0IBw+iZk/5iUzX6+gpEl fhm2UDhND9JZK  
2S31MI0B27s/ZXB03LpjbUE/F0tcPiYec4iG23odTrqSczZEpJAnw42SB4To4Gf  
oFtFQhIRCAiem5OKKsbWN9pfsI4mhIEepTnVd8umSOkEPNecOuf6izlKncOBPkkz  
kJorgLwP/C8YTAeyXSPdI4KCz8pQQSmf1GfJ7b4DSs/DpR1dKTOXko5Sx5ouz3H5  
TY4x6/LXxJBzKTDcy4Dpaon3OaDulAUHO0xH872s5FEZu/QDoRlhQ6fQCdOQKKH  
IE9V6/RXyNrdBDDb+zL74aw7aydQRzv8R5v9RobMBjDAQujnZH2P8/dz3bTh8bOr  
TWZMBKQ0uOWoVr7GhcgwZthxVqEGxYv+rD+3ROpvvNar2nm/ /sZKm5On0kqw3a7Y  
Tqj4+rqq+N2QHNphSnCTCb5yqBP5fZ0a4t1L+zs08lyCl8UblI7wlyy/BwiPR90g  
2ddIVmmLXes6FAI/nzVgdZgQsyrjfhOjYXBlf3PKNRx7GiBYpGLAhN/EQLsvksU  
NTMZWgeor46S6u/makH95yNPENQc/2ycBGv1IAQ9yq5D2gNOM/AVBQ/u85yYNa9R  
XsG1OcgdusnNm7lvut2GjhlwaAchFmG+W+AmteQtQdAsEoZsNLHTzZjw0F9fgt1N  
QqXXm3lIzKpULmQge5XYpr/cip2+NhL9lJYkIT+1NxDskovEidjRfdbvZgu2uGMv  
dssPl1GLXlwnaLP304ZcKcPdGE59WWuGPD2XabhCx5JcbG+LsXNUiaf8KStqAVqp7  
cporbQxoqPzxxvXD1NrvWojuaJhp+Ad0WVGqPuQ9+FkwANs9NrjavMLd6z/+7ycXP  
UK6ASLLCRh9En5WGi9IpgvZNonTYDX/s/S1Z1hrcjo2etzocMhedUaStQhnoXLNx  
NwMRAvqKz0avn1BlVpRhHLyZ5hU0geudkmzPtodtq9vbbHzyEJACSpbr+jS4wQfL  
zhwSMRVfEGa016kmV2qbA26IdzAZBoQei7fUm1lEpMLQwV/JFA/X9MKRLNrksovn  
EsX2N9V0LOXzQsmIywv/rqEDKv+nypoEn/xV2pVXx8yOjjqzmzIrlzOVYvYd/ex0g  
Jj803vbxcMQWF+/4ENNB0aU3PsbXC7KiWVxq/qulX3jv6KqCrjCL/+bdf9xcmZzx  
7byreMyfJTBMOAAoPo/k7UhmVQKdbezkPbgnUk0uPNYi2te5ggMTVdZc7rrzJVDn  
zEAgyTH42QIDAQABO4IBozCCAz8wSwYDVR0gBEQwQjAGBgRVHSAAMDgGDSsGAQQB  
g3UCAQEbgxEwJzAlBggrBgEFBQcCARYZaHR0cDovL3BvbGljeS5lYWR0cnVzdC5l  
dTASBgNVHRMBAf8ECDAGAQH/AgEAMA4GA1UdDwEB/wQEAwIBhjAdBgNVHQ4EFgQU  
DmLLaHy9YxsoilQhrg+NpHEnl4wHwYDVR0jBBgwFoAUumoOmCc2Hko0Tdtv992w  
c0nzXfcwTgYDVR0fBEcwRTBDoEGGP4Y9aHR0cDovL2Nybc5lYWR0cnVzdC5lS9l  
YWR0cnVzdC1yb290LXJzYTgxOTJlYWRldnBzZDIyMDE5LmNybdB9BggrBgEFBQcC  
AQRxMG8wSAYIKwYBBQUHMAKGPh0dHA6Ly9jYS5lYWR0cnVzdC5lS9lYWR0cnVz  
dC1yb290LXJzYTgxOTJlYWRldnBzZDIyMDE5LmNydDAjBggrBgEFBQcwAYYXaHR0  
cDovL29jc3AuZWFkdHJlYWRldnBzZDIyMDE5LmNydDAjBggrBgEFBQcCAGAQUF  
BwMCMA0GCSqGSIb3DQEBAQUAA4IEAQDGezJzPVt6JVluaxQLSGg9WHhd8era05Ft  
03h9WO6jZJ0FQUn79hze619uap5Cj6NhLiRXL2HbN2F7HqgU591Ced1lvMsZnCgP  
6+itrMfxvSBC5R578SjfjwErezD1P6lylD7r68of3mSn0YdihkVWXE0Ja+uvsNl0  
Hl4VjGho9RuSTdbl4sctFifd7C9Y9F+koF2Ge6SUnlCamcnqvM1KC88dBszfCMPT  
KiDoLI49B/Plb31f06a6aKk/WZg77hGzi16FOVKHdKkoDowzv74HTp9JJM/kJVhW  
kZjlnEA3yX8KK96+bx0YpGuywuEMTKazfujuWwXViam5DDzWB921QeBO0Kwa3ev8L  
uHGLbSNyriRhZsvx/Bj3i9r4CoqTtyRpfJA8EkafHjWATXrtqeSI2KrpP6V7m/2X  
e66HFfndDrFvfrOIqjS9+L0rpjFuFrNyG9Wmi1kk2MlMXXf1U5NjYq3m5LXZm4M  
COd+3yZfvsqGtDYw5JV8Zfw7i0CbdD+Vfuupvl7yXkP+0rmrPvc3RktABzkf1lzY  
Yz4AkJuWfAZ1TSC+e3/zTy01rN9LkKFq2ioOky3GLReTjUmVjMRf/quUsHacbcqQZ  
mHTw1wjK073vk7kEMlrB+awFGhBVg8vUKfooAAoSr9c27ZkONJcjsjRFTMa1/2l/  
oAXxSebF7dILguLA31aiMn0VqMWUnBCYcDgA89EXQ0vGyoWFSzoU5JNOy4gWvav  
pAvJM07rAah37sh6OwkrEn8GBLD3m+eeFCaNRd1EnSdIF/PZKn/XLXvbMKIlLFU1  
a689HWwVcYQhXk03WwJBvpNcsCUQKuzQtYGuTVhoj+BiXPzKI9H2ZKyWqbTISvxS  
atjEWl+FQ9DCi3jGLAZcQDVCNxs+I7Tx0Ex3nVGg2nsKU61dIbKdPh9hJBkgWsid  
5mytHiYuwRb01Dd8ZHRG0jL/cQwC0WfpB/VQtN4Rjiaa0GJjuKAudJcV4y2y1XIs  
E6GZUiRw9kaAcMbmZtTcLwdDCTjzNKSUX6WfYTsfpbxph6y2Ch3t59VG8UmwJO90  
kwQiQ1VnG4ooFsevgqmmgqTOv59X6KV3sqwAcKWU4MUBvsJiRzQQ5fHL5fSkqx8s  
cxruyJXTosvH6iGPONzGKZQGYLA4EVCzMoYncnXykM13GS25eVoQs715ckOPmkf1  
e5JWVDn7udyaZCTSRGZaJKonLSFnVC7oEheBCqGe9eL6y4GalcTNHlhtIdXsFGVh  
mjc6EAmZ96fB4L6fbFihBglfulMUnwuARK32EDcSACvS7ilc/mZrSm+GXYw0S8nV  
bet1gNq198wWM/PJnEVmQrO2JVQ2BSR/j9eiHFc6qKmc1/SZK91P

-----END CERTIFICATE-----



6uhDeG6zn8HhgIFkpvSPRBRfDSKnmvjXg0HPBsVUUjUMFboGy0J9ZHyKhv+/260D  
89Gmj4CwmI7mdHP04pCDMrIcKYHsH4FvLQP3Wp2uVvWWvA3A6eDPcsVXFdfEozrj  
itmsArWNpAjUlKfj+DpYRAeYh6wsWM7mzVbp1Taf2vz1RKSqkphKnuGaD8jtZUx4  
9YV/9+IHnAICuX1z483f8R4n94Mz2hJingUvGZxopY811ypASJ/2gQ71/3Dut7Ez  
kCOTXNcSjcv8hFVuSFMR9+dMdBz1TX1dHvW8BtwEhGkvtGHkdMIX+2AKw3Nan89f  
ZPK1r8n0oRaFufiE7uRAMSDmPVIStHyWds81K0NX04j7im47wpS41VOIGvXHWYNR  
N24y+jSkqtCtFbxryFXsaQKVNm77zwjSm+zTvPBjVo2JLX7itPxo9vYCDyLtMR6o  
boF4GYYV1YdSjJRdRoMMAPRjdHhOwGkUZ9GgDqvRElFIDa85kf+eOuiXKFUt9eTH  
tg5HLHUrplq+G2GIYIi8XV0IoZpUOQnf3zSufQr/0OUduTaKsybDBntiYjQuriM  
17z1j6QPG7h3MGkF6sdLGLMFE8KeUosIEKJyvcDthDuvJv4CuqNEZuR6pP8T29xv  
I+JcTBcb8boPKioo2f0tLUOf2SpT+hNnBvRpwKetZyFZPAkxwhYrX/z7DyVK95s+  
vzoWH/tmNSDFH97wdTOONfQfgr80B2RpZ6bpN5TCxX2IKyKdA4DpPk3nV15Z3oG9  
MfYfMYb18ZsQedpZYPnKrSRjtG+ZnRYLiY7H/4nRX1ciL25pVQu6hbvFgQ3sHXQK  
GXeatTxCJLRvFMduDST9henlgkol9UQIcu4/vT3R87f1/sWX9IB7KVIAPInVKaE9  
8xm9o2FQBR0iyFeLfsKyLOLXA0e1BKOU2BOepOeDpX7dr4EhF4806m8Eu7qh4eNu  
Q8xyuXu9pD9+3TH8czvN4WJVq466BYE/NlCWPxTcBloqx56NlvGGgnT4LZVMhHb8  
BkSBlNeGmEXAia+lauABuYZNE+OcVDh3TjisiZi1GU0auCzbilwp/ZrlxM+VPaG1A  
WoWcVv7rQ+bAVw78nULnJQNPRioK9gkvZOa=  
-----END CERTIFICATE-----

13.3.33 EADTrust RSA 8192 SubCA For Qualified Certificates 2019

-----BEGIN CERTIFICATE-----  
MIIMdzCCCF+gAwIBAgIIURY4c0dWMFkwDQYJKoZIhvcNAQENBQAwgZwxQjBAbGNV  
BAMMOUvBRFRydXN0IFJlTQSA4MTkyIFJvb3QgQ0EgRm9yIFFlYWxpZml1ZCZBDZl0  
aWZpY2F0ZXMgMjAxOTEvMC0GAlUECgwmRXVyb3BlYW4gQWdlbmN5IG9mIERpZ210  
YWwgVHJ1c3QsIFMuTC4xZCzAJBgNVBAYTAkVTMRgwFgYDVQRhDA9WQVRFUy1CODU2  
MjYyNDawHhcNMkwnjA2MTEyMDUxWhcNMzUwNjAyMTEyMDUxWjCBszFAMD4GAlUE  
AwW3RUFEEVHJ1c3QgUlNBIDgxOTIuU3ViQ0EgRm9yIFFlYWxpZml1ZCZBDZl0aWZp  
Y2F0ZXMgMjAxOTEvMC0GAlUECgwmRXVyb3BlYW4gQWdlbmN5IG9mIERpZ210YWwg  
VHJ1c3QsIFMuTC4xZCzAJBgNVBAYTAkVTMRgwFgYDVQRhDA9WQVRFUy1CODU2MjYy  
NDaxFzAVBgNVBAsMDk5hdHVyYUwgUGVyc29uMIIIEIjANBgkqhkiG9w0BAQEFAAOOC  
BA8AMIIECgKCBAAEAvdbc3AjQj1TTPjUs7iwmyPFGJRP6OCW+Y3/+xPX7tK0EVbyC  
IFK0M7XX1Iwt2YJk053r1v2MoCekjI9xGT3LHFfWAlHJx6IFzc0lwLfdeH/fbt3T  
0XPg+stZEa4cWtjtm8U0AihI9XHRD5d+0PnTG2PyjYrWE2wSUqqOnYUSHP17WJV7  
DD37ZQFCFlBoYvK8XCJbQoxFoBSnC+SSODzvKzR1a2L4YyDzL/ytPIDfpgP0qWI  
mUyNGayvVakSQ8jxOn3C7XgtwvTmAFS+TJS04mkmLS03E9ausLHZVEVogqQdtgLL  
dFeOJFKUONqlcDv9U80J5/D7DrgwBzUYz4Xx/LLVxmTk7A/7bu+qmnKi+y1NltIK  
CMWMSQkZZMePwYGG/T82nxR4ln+AyWYJWpMP9300XP8/SMBk5d3xl+aN15pdzTUP  
EKGQ8JGAF+HNfyZppFNpBEpXz9LRiTDQdcJHVpJ7E7dwdEfbM44Yciz8FZMLHxRA  
gfvwRKEUmWWR26HB+CgdqjC6lBxZRH+e2n6QwJl7U26kv3dY9bCDtWs4qu8BFjNn  
gEEwQ8G/zOhlp50888TKnzZwZEYV6zasz/3I37hAHKhfi0ke6KdhT0fERGvr1UBg  
7jpmQNYzLHShOCs+Tq2qBwYlOEoIGFICaUC7gvXKtzhyroqL8GbZ4L3VxsqLsVmr  
e5K0zV5eEHhBKjEF9KZFyBxDaWa65TNZcbSGGq3kc4NARUWdmkFMtQHF6GHUIxKe  
xfQYPu/U3pFqWFG4SGxyPCcFCGa0tqIjCuIIBQpcORKTvR+DhBAS/l8o+5N4rE8g  
qY1hn0//vxzQZ58DQtF0QrdeQYUjAP/VZrJq2bmjVWdfeF3UJQ6/YXkkMmlJrabq  
Kv5pBHPAFVbUpitOU0CK+1rY0UKWLWUJldgx+/TcnLK/vAnevAcTdKyVqQzKCYKs  
v7ZwUxpZVUwAeJHMTpY0EnhbVzz/5JnHHNqyU937cyRfyOMGovQfhoNc/RbkbWwC  
0WY8+IAC41kBPsq64oA6Y5yKQizzogyp6+4WGHqyhhuR7OHl41sXgSPoggI3oEfT  
s3I/NzsXyKilbCQsye4y0oHPd4BRuzafRIP63FAhiyJ7AlSH+BGIGDDzqqpknybd  
aysAyQdwjPqfh6PO6D80FPf+wflrtTt/mUMLIIgTTJHWRf1cpC47Bc+Tx3b/j5rh  
/X4d8jHLUDf4vzdowj1Gg2qdwJuGo0ikbUa2PafYmaDkfb70WgnHA/jv8+jPTz9A



RgEcPY/IGS522KdVQive449EP33SMY/Mfb6Q2h6n+TUpI5u8SLsvDPTugvwVU0Wi  
Upp2te3wcY2xj7diV0gKwsxT6sS7AvezdLisKQIDAQABo4ICojCCAp4wgagGA1Ud  
IASBoDCBnTAGBgRVHSAAMIGSBg0rBgEEAYN1AgEBAYMRMIGAMCUGCCsGAQUFBwIB  
Fh1odHRwOi8vcG9saWN5LmVhZHRydXN0LmV1MFcGCCsGAQUFBwICMEsMSVN1Ym9y  
ZGluYXRlIEN1cnRpZmljYXRlIEF1dGhvcml0eS4gRXVyY3B1Yw4gQWdlbmN5IG9m  
IERpZ210YWwgVHJ1c3QsIFMuTC4wEgYDVR0TAQH/BAGwBgEB/wIBADA0BgNVHQ8B  
Af8EBAMCAYYwHQYDVR00BBYEFOqZz2sBGpMRGn9yJpordU303OYMGMA1UdEgRc  
MFqBDMNhQGVhZHRydXN0LmV1hhZodHRwOi8vd3d3LmVhZHRydXN0LmV1hhVodHRw  
Oi8vY2EuZWFkdHJ1c3QuZXWGGWh0dHA6Ly9wb2xpY3kuZWFkdHJ1c3QuZXUwYwYD  
VR0RBfwwWoeOY2FAZWfkdHJ1c3QuZXWGFmh0dHA6Ly93d3cuZWFkdHJ1c3QuZXWG  
FWh0dHA6Ly9jYS51YWR0cnVzdC5ldYYZaHR0cDovL3BvbG1jeS51YWR0cnVzdC5l  
dTAFBgNVHSMEGDAWgBQG5nPZUT1Ap9FXjDZ/x+3Qed33yzBJBgNVHR8EQjBAMD6g  
PKA6hjodHRwOi8vY3JsLmVhZHRydXN0LmV1L2VhZHRydXN0LXJvb3QtcnNhODE5  
MmVhZHEyMDE5LmNybDB4BggrBgEFBQcBAQRsMGowQwYIKwYBBQUHMAKGN2h0dHA6  
Ly9jYS51YWR0cnVzdC5ldS91YWR0cnVzdC1y290LXJzYTgxOTJlYWRxMjAxOS5j  
cnQwIwYIKwYBBQUHMAGGF2h0dHA6Ly9vY3NwLmVhZHRydXN0LmV1MA0GCSqGSIB3  
DQEBDQUAA4IEAQBCE2VS5kD4qKddyF5XuTCAuyHeXXx9YUp3bmm+blEgSET/83BW  
UNeuwamsxPzkBhyejvGn8hNR0ncej073Rlfai03qlXo6K8jwVjwNwDzgtB4oYMBw  
vvKlnmuPRGd6qYdPtWMw6boMa2KQcEXqp0kp8F7yIY3agvt5wARRRM1K9Pgl+Fdd  
8xFpKRS2WFqONV4V3gIhOuCjzUGKkTms0H1DGJYwc3mI36bJe6kVLWfEEEnqm28t  
vF86BygX11zUz9MnZx5obFGSGqdlewWnQCGINOLi052ovyCiQIOG6TE9Lcs0PzcE  
9BqdWpxbGfnDK40U/05UCWDwIa9qcSa4SWtrt6VEe5gtkpnPVx07nYaFVY85fDN  
wz0LxzWM6zMucx85F3jtxuhaA+s9E6/qLxmFP8bnEDnb7HtYAKPF1pB98Beavpu9  
mxTVc4GiTdmG6NFzly25p33qTmw5yBwLdmi jvtlZWyrC6DwDx144KPYg63jT+FVI  
oWoWReKvD+c/t5pkOmfD+UCIAyMwnMEXABku549pR/3RBB/WfYjSwCUNN3V1xN8f  
uPPTv89tGW+kZ2WO2o4cUsd2vM2du9eFYhGESY0/KpUUS17Ismew+EKUPWzsopv5  
hlR6DXW/nj2bYrYp5A81hp8kk2sco8hIrkDqInHF6UhQDUhcYmFcsK0mJfKc+xVR  
qQhFtB3o2CuNNiC/NNw1WRVJKPv5gS0QI0tzLvukLiL7uiyrHYP80ExHWSy+/+1n  
bI3yjBaZc+bkJTz0jDemDSap+vT3x56dip2x+SBMfrgOxVuf2j3ex/y/udSvAseS  
x3e9PmyNRTca6x2DZhcbaWlT8kZwJt jN0GCK8FoAYXmJuPD2XXaDWauYU2Txlixb  
60Col0OfThXxcx0Ai5MSC8QMVI sN/1Zuydl4C+N4Z9mcZJcghH3gCaWodHA3lgQk  
TiVyhs7JHt0b/pemXrmRfzzVl3hgP9FgmIYV/YkDwdRbs9R3wuHYJ46RMUpKhHv5  
LK+fem163RuNthF7Cc+nrOczdf1rv6G6dR08nQlIAMMvfN0Rr6QnnC8sp2A+rAMD  
xN2U6JjZVecc/UB7I4RkinlZ83Ta9qPjkXwikGts3BwbaH6IFU5Y80wgqGRSSeIt  
aOIXjoH/1AqMEWaKpKzqtKap71r2JB6D9bw6Ke8yrVaiAZHCKaEFXzqwmJr0HnpL  
jrHJ21Iu4OewtVdSEWBbbu+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 el Reglamento (UE) 2016/679 (Reglamento general de protección de datos);
- 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.