ENTRUST EU, S.L.

Declaración de Prácticas de Certificación
Para Certificados Cualificados

Versión: 1.9
12 de mayo de 2023

Historial de cambios

Publicación	Fecha	Actualización
1.0	11 de diciembre de 2019	Versión inicial.
1.1	10 de junio de 2020	Adición de certificados Qseal y Qsig
1.2	22 de julio de 2020	Actualización de 6.6.2 Controles de gestión de seguridad, actualización 9.6.4 Representaciones y garantías de partes que confían y adición de extensiones AATL al perfil de certificado QSignature
1.3	30 de octubre de 2020	Actualizar la marca Entrust, la dirección de correo electrónico para CPR, agregar la raíz Q4, la implementación de las propuestas del CAB Forum (SC23, SC24, SC25, SC28, SC30, SC31, SC33 y SC35), la eliminación del lenguaje no inclusivo y los términos y condiciones en la sección 9
1.4	18 de diciembre de 2020	Actualizar marca y período de retención
1.5	7 de mayo de 2020	Actualizar Subject name serial number, verificación de identidad de persona física
1.5.1	15 de noviembre de 2021	Cambio Entrust Datacard Europe a Entrust Solutions Spain
1.6	30 de noviembre de 2021	Actualización de las propuestas del CAB Forum (CSC7, CSC8, SC42, SC44, SC45, SC46, SC47 y SC48), actualización de la política de Mozilla 2.7.1, CRL/OCSP período máximo de validez, actualizar nuevas CA
1.7	1 de Agosto de 2022	Propuestas del CAB Forum (SC53), aclarar los métodos de verificación de solicitudes, aclaración de terceras partes delegadas, actualizaciones de validación de EV, actualización de reconocimiento de marca registrada, comunicación del solicitante y actualizaciones de respuesta de CRL/OCSP, eliminación de administradores de CA
1.8	9 de Enero de 2023	Actualizar la Autoridad y los Certificados Cualificados de Sello de Tiempo, última CRL/OCSP, cambiar QTSC a 5 años máximo
1.9	12 de mayo de 2023	Propuestas del CAB Forum SC61, CCADB clarificaciones de autoevaluación, actualización de

		Enterprise RA, actualización de Autoridad de Política.

Contenido

1. Introducción

Entrust EU, S.L. ("Entrust EU") utiliza sus productos de software para proporcionar certificados digitales que cumplen con los estándares y permiten comunicaciones en línea más seguras.

Las CA de Entrust EU emiten certificados que incluyen los siguientes tipos:

- Certificado(s) Cualificado(s) de Firma Electrónica de tipo eIDAS ("QSigC de tipo eIDAS" por sus siglas inglesas) emitido de acuerdo con la política QCP-n-qscd
- Certificado(s) Cualificado(s) de Sello Electrónico de tipo eIDAS ("QSealC de tipo eIDAS" por sus siglas inglesas) emitido de acuerdo con la política QCP-l (incluyendo NCP +)
- Certificado(s) Cualificado(s) de Sello Electrónico de tipo PSD2 ("QSealC de tipo PSD2" por sus siglas inglesas) emitido de acuerdo con la política QCP-l (incluyendo PSD2)
- Certificado(s) Cualificado(s) de Autenticación de Sitio Web de tipo eIDAS ("QWAC de tipo eIDAS" por sus siglas inglesas) emitido de acuerdo con la política QCP-w
- Certificado(s) Cualificado(s) de Autenticación de Sitio Web de tipo PSD2 ("QWAC de tipo PSD2" por sus siglas inglesas) emitido de acuerdo con la política QCP-w-psd2
- Certificado(s) Cualificado(s) de Sello de Tiempo de tipo eIDAS ("eIDAS QTSC(s)") emitido de acuerdo con la política de sello de tiempo de mejores prácticas (BTSP).

1.1 Visión general

Esta CPS (Declaración de Prácticas de Certificación por sus siglas en inglés) describe las prácticas y los procedimientos de (i) las CA y (ii) las RA que operan bajo las CA. Esta CPS también describe los términos y condiciones bajo los cuales Entrust ofrece los servicios de CA y RA disponibles con respecto a los certificados. Esta CPS es aplicable a todas las personas, entidades y organizaciones, incluyendo todos los Solicitantes, Suscriptores, Partes que Confían, Revendedores, Comerciales y otras personas, entidades u organizaciones que tienen una relación con (i) Entrust con respecto a certificados y / o cualquier servicio proporcionado por Entrust con respecto a los Certificados, o (ii) cualquier RA que opera bajo una CA, o cualquier Revendedor o Comercial que brinde cualquier servicio con respecto a los certificados. Esta CPS se incorpora como referencia en todos los certificados emitidos por las CA de Entrust. Esta CPS proporciona a los Solicitantes, Suscriptores, Partes que Confían, Revendedores, Comerciales y otras personas, entidades y organizaciones una declaración de las prácticas y políticas de las CA y también de las RA que operan bajo las CA. Esta CPS también proporciona una declaración de los derechos y obligaciones de Entrust a cualquier tercera parte que opere RA bajo las CA, Solicitantes, Suscriptores, Partes que Confían, Revendedores,

Comerciales y cualquier otra persona, entidad u organización que pueda usar o confiar en los Certificados o tener una relación con una CA o una RA que opera bajo una CA con respecto a los Certificados y / o cualquier servicio con respecto a los Certificados. Esta CPS está estructurada de acuerdo con la RFC 3647e incluye toda la información requerida por la misma.

Con respecto a los Certificados Cualificados, Entrust cumple con el Reglamento (UE) no 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, sobre identificación electrónica y servicios de confianza para transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93 / CE, incluido su anexo IV ("eIDAS"). En caso de contradicción entre esta CPS y los requisitos eIDAS, estos últimos prevalecen.

Con respecto a los Certificados de tipo PSD2, Entrust cumple con el Reglamento (UE) no 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, sobre identificación electrónica y servicios de confianza para transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93 / CE, incluido su anexo IV ("eIDAS"); asimismo, Entrust se ajusta a la Directiva (UE) 2015/2366 [i.2] 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 ("PSD2") En caso de contradicción entre esta CPS y los requisitos eIDAS y/o PSD2. estos últimos prevalecen.

Además, con respecto a los QWAC de tipo eIDAS y los QWAC de tipo PSD2, Entrust se ajusta a la versión actual de las Directrices para la emisión y gestión de Certificados de Validación Extendida (EV) publicados en https://www.cabforum.org. La guía de EV SSL (EV SSL Guidelines) describe los requisitos mínimos que debe cumplir una CA para emitir Certificados EV. En caso de contradicción entre esta CPS y la Guía de EV SSL, esta última prevalece.

1.2 Nombre del documento e identificación

Este documento se denomina Declaración de Prácticas de Certificación de Entrust EU, S.L.

1.3 Participantes del sistema de PKI

1.3.1Autoridades de Certificación

En la infraestructura de clave pública de Entrust, las CA pueden aceptar Solicitudes de Firma de Certificado (CSR) y Claves Públicas de los Solicitantes cuya identidad haya sido verificada según lo dispuesto en este documento por una RA. Si una Solicitud de Certificado se valida, la RA de verificación enviará una solicitud a una CA para la emisión de un Certificado. Las CA crearán un Certificado que contenga la Clave Pública y la información de identificación contenida en la solicitud enviada

por la RA a esa CA. El Certificado creado en respuesta a la solicitud será firmado digitalmente por la CA.

Esta CPS cubre todos los Certificados emitidos y firmados por las siguientes CA. El propósito de estas CA es permitir que Entrust emita los tipos de certificados cualificados de confianza que se enumeran en la Sección 1 de acuerdo con las normas y reglamentos aplicables.

Raíz
CN: Entrust Root Certification Authority - G2
Identificador de clave: 6a 72 26 7a d0 1e ef 7d e7 3b 69 51 d4 6c 8d 9f 90 12 66 ab
Huella digital (SHA-1): 8c f4 27 fd 79 0c 3a d1 66 06 8d e8 1e 57 ef bb 93 22 72 d4

CA subordinada(s) a G2
CN: Entrust Certification Authority – QTSP1
Identificador de clave de sujeto: 1c ad 3f 9c d7 2d 22 19 a1 9c 4b e9 da f1 2a 33 f7 fb ba 0d

CN: Entrust Certification Authority – ES QWAC2
Identificador de Clave de Sujeto:
41:cf:ae:2b:1d:63:3b:cb:4c:f5:90:44:79:b6:5a:24:89:df:92:9c

Raíz
CN: Entrust Root Certification Authority – G4
Identificador de clave: 9f 38 c4 56 23 c3 39 e8 a0 71 6c e8 54 4c e4 e8 3a b1 bf 67
Huella digital (SHA-1): 14 88 4e 86 26 37 b0 26 af 59 62 5c 40 77 ec 35 29 ba 96 01

CN: Entrust Certification Authority – AATL1
Subject Key Identifier:
63:f1:84:dd:03:be:a3:9f:64:fa:76:7a:47:c4:56:7e:c0:6d:a0:20

CA subordinada(s) a AATL1
CN: Entrust Certification Authority – ES QSeal1
Identificador de clave de sujeto:
56:80:15:23:95:71:7f:e7:2d:90:d0:cd:06:3a:4f:67:63:7d:3d:75

CN: Entrust Certification Authority – ES QSig1
Identificador de clave de sujeto:
5a:53:08:8a:61:30:a9:0d:ea:d5:43:97:d3:98:3b:95:1e:2e:6d:02

Raíz
CN: Entrust Root Certification Authority – DSR1
Identificador de clave: a6 65 41 81 f2 5b 87 05 6a dd fd 8a 54 4e 8f 98 7b dc 23 b8

Huella digital (SHA-1): 10 4f e7 37 00 18 6e 69 2e 78 a0 15 6a 3f 9e d8 07 b0 60 8e

CA subordinada(s) a DSR1

CN: Entrust Certification Authority – ES QSeal2
Identificador de clave de sujeto:
36:18:25:6e:d9:5d:f7:10:05:7c:27:2e:b8:ec:fa:41:4a:60:ed:1f

CN: Entrust Certification Authority – ES QSig2
Identificador de clave de sujeto:
f5:56:0d:69:d7:da:6a:c9:d8:c9:a2:09:6e:74:be:db:80:c6:17:00

CN: Entrust Certification Authority – ES QTS1
Identificador de clave de sujeto:
69:63:82:ca:c2:f1:11:9a:71:43:32:85:8b:ae:37:ca:96:76:be:80

Entrust será responsable de garantizar que todas las CA subordinadas cumplan con todos los requisitos de política aplicables para la raíz "Entrust Root Certification Authority - G2", la raíz "Entrust Root Certification Authority – G4" y la raíz "Entrust Digital Signing Root Certification Authority – DSR1".

Certificados cruzados emitidos externamente

La notificación del siguiente Certificado Cruzado se proporciona solo por motivos de transparencia. Microsoft ha emitido el Certificado Cruzado para admitir firmas de código con productos de Windows. El Certificado Cruzado no afecta la funcionalidad de los Certificados Cualificados o Certificados PSD2. No habrá ningún impacto en los Certificados Cualificados o Certificados PSD2 si el Certificado Cruzado expira o ha sido revocado.

Emisor: CN = Raíz de verificación de código de Microsoft, O = Microsoft Corporation, L = Redmond,
S = Washington, C = US
Asunto: CN = Entust Root Certification Authority - G2, OU = (c) 2009 Entrust, Inc. – solo para uso autorizado, OU = Ver www.entrust.net/legal-terms, O = Entrust, Inc., C = US
Número de serie: 33 00 00 00 42 00 ba 5e 23 b0 a1 f3 99 00 00 00 00 00 00 42
Identificador de clave del sujeto: 6a 72 26 7a d0 1e ef 7d e7 3b 69 51 d4 6c 8d 9f 90 12 66 ab
Válido hasta el 7 de julio de 2025.
Huella digital (SHA-1): d8 fc 24 87 48 58 5e 17 3e fb fb 30 75 c4 b4 d6 0f 9d 8d 08

1.3.2 Autoridades de registro

Entrust no utiliza terceras partes delegadas para realizar funciones de RA.

Las RA (Autoridades de Registro) de la CA pueden aceptar Solicitudes de Certificado de los Solicitantes y realizar la verificación de la información contenida en dichas Solicitudes de Certificado de acuerdo con los procedimientos establecidos por la Autoridad en Materia de Políticas. Una RA que opera bajo una CA puede enviar una solicitud a dicha CA para emitir un Certificado al Solicitante.
Sólo las RA autorizadas por Entrust pueden enviar solicitudes a una CA para la emisión de Certificados.

No se puede delegar en las RA de terceros para validar FQDN ni direcciones IP según §3.2.2.4 o §3.2.2.5.

La CA puede delegar en Empresas RA para verificar las solicitudes de Certificados de la misma Empresa RA o de una organización de la que la Empresa RA es un agente. Los FQDN solicitados deben encontrarse dentro del Espacio de Nombres de Dominio de la Empresa RA.

1.3.3 Suscriptores

Los Suscriptores pueden usar los servicios de CA en sus transacciones y comunicaciones. El Sujeto de un Certificado es la parte nombrada en el Certificado. En el presente documento, un Suscriptor puede referirse tanto al Sujeto del Certificado como la entidad que contrató a la CA para la emisión del Certificado. Antes de la verificación de identidad y emisión de un Certificado, el Suscriptor es un Solicitante.

Entrust dará acceso a sus servicios a todos los Solicitantes y Suscriptores cuyas actividades se encuentren dentro de su ámbito de operaciones declarado y que acepten cumplir con todas las obligaciones especificadas en el Acuerdo de Suscriptor de Entrust y esta CPS.

1.3.4 Partes que Confían

Las Partes que Confían son entidades que actúan confiando en un Certificado y / o firma digital. Las Partes que Confían deben asegurarse de que el Certificado no esté caducado ni revocado antes de confiar en el Certificado o la firma digital. El estado de revocación del certificado se puede confirmar comprobando la CRL apropiada o la respuesta de OCSP. La ubicación del punto de distribución CRL y / o la respuesta OCSP se detallan en el Certificado.

1.3.5 Otros participantes

La CA puede hacer uso de terceros para proporcionar partes del servicio de certificación como se describe en esta CPS. Los terceros que presten servicios para apoyar las actividades cumplirán con las prácticas actuales declaradas en este CPS.

1.4 Uso del Certificado

1.4.1 Usos apropiados del Certificado

Este CPS es aplicable a los siguientes tipos de Certificado.

QSigC de tipo eIDAS
Los QSigC de tipo eIDAS emitidos en virtud de esta CPS tienen como objetivo respaldar las firmas electrónicas avanzadas basadas en un certificado cualificado definido en los artículos 26 y 27 del Reglamento (UE) no 910/2014 y firmas electrónicas cualificadas basadas en un certificado cualificado definido en el artículo 3 (12) del Reglamento (UE) no 910/2014.

QSealC de tipo eIDAS
Los QSealC de tipo eIDAS emitidos en virtud de esta CPS tienen como objetivo permitir los sellos electrónicos avanzados basados en un certificado cualificado definido en los artículos 36 y 37 del Reglamento (UE) no 910/2014.

QTSC de tipo eIDAS
Los QTSC de tipo eIDAS emitidos en virtud de esta CPS tienen por objeto dar soporte a los sellos de tiempo electrónicos basados en un Certificado Cualificado y en los artículos 41 y 42 del Reglamento (UE) n.º 910/2014.

QWAC de tipo eIDAS
Los QWAC de tipo eIADS emitidos en virtud de esta CPS tienen como objetivo permitir la autenticación de sitios web con base en un certificado cualificado definido en los artículos 3 (38) y 45 del Reglamento (UE) no 910/2014.

Certificados de tipo PSD2
Los Certificados PSDS emitidos en virtud de esta CPS tienen como objetivo permitir la aplicación de los requisitos de las Normas Técnicas Reguladoras de PSD2 para el uso de certificados cualificados según lo definido en eIDAS (Reglamento (UE) no 910/2014), incluyendo el Anexo IV, para cumplir con los requisitos reglamentarios de PSD2 (Directiva (UE) 2015 / 2366), incluidos los requisitos de ETSI TS 119 495 y las Directrices de ETSI relacionadas.

1.4.2 Usos prohibidos de Certificados

El uso de todos los Certificados emitidos por la CA será para fines legales y de conformidad con las leyes aplicables, incluyendo sin limitación alguna las leyes aplicables de exportación o importación.

Los Certificados y los servicios proporcionados por Entrust con respecto a los Certificados no están diseñados, fabricados, o destinados a ser usados encualquier aplicación en la que un fallo pueda provocar la muerte, lesiones personales o daños físicos o materiales graves , como la monitorización, el funcionamiento o el control de instalaciones nucleares, sistemas de tránsito masivo, sistemas de navegación o comunicaciones aéreas, o sistemas de control de tráfico, sistemas de armas, dispositivos médicos o máquinas de soporte vital directo, y todos esos usos están prohibidos.

Los Certificados emitidos en virtud de esta CPS no se pueden utilizar para fines de "gestión de tráfico" ni “intermediario”.

1.5 Administración de Políticas

1.5.1 Organización que administra el documento

La CPS es administrada por la Autoridad en Materia de Políticas; se basa en las políticas establecidas por Entrust EU, S.L.

1.5.2 Persona de contacto

Los datos de contacto para preguntas sobre Certificados son los siguientes:

Entrust EU, S.L.
Pe La Finca. Paseo Club Deportivo, 1 Bloque 3 BJ
28223 Pozuelo de Alarcón (Madrid)
España
A la atención de: Entrust EU Servicios de Certificado

Tel: +1-866-267-9297 o +1-613-270-2680
Email: ecs.support@entrust.com

Los Informes de Problema de Certificado, como el uso incorrecto de Certificados, informes de vulnerabilidad o informes externos de puesta en riesgo de la clave debne ser comunicados por correo electrónico a ecs.support@entrust.com

1.5.3 Persona que determina la idoneidad de CPS para la política

La Autoridad en Materia de Políticas determina la idoneidad y aplicabilidad de esta CPS. La Autoridad en Materia de Políticas se asegurará de que la CPS cumpla con los requisitos de cualquier Política de Certificado aplicable.
La autoridad política:

(i) Supervisa e implementa las boletas aprobadas del CA/Browser Forum;
(ii) Supervisa e implementa los cambios de política de los ASV aplicables; y
(iii) Supervisa los debates del foro de políticas de seguridad de Mozilla y la lista pública de CCADB.

1.5.4 Procedimientos de aprobación de CPS

Esta CPS y cualquier cambio posterior serán aprobados por la Autoridad en Materia de Políticas.

Esta CPS se publicará en el Repositorio de Entrust, donde todos los Solicitantes, Suscriptores, Partes que Confían y otros terceros podrán verlo. Una vez que la Autoridad en Materia de Políticas haya aprobado los cambios a esta CPS, se distribuirán a los empleados, agentes y terceros de Entrust que participen en la prestación de los servicios proporcionados en este documento y que se vean afectados por los cambios.

Entrust puede (i) revisar los términos de esta CPS; y / o (ii) cambiar parte de los servicios proporcionados en este documento en cualquier momento. Cualquier cambio de este tipo será vinculante y efectivo inmediatamente después de la publicación del cambio en el Repositorio de Entrust. Si usted no está de acuerdo con el cambio, debe dejar de usar o confiar en cualquier Certificado de Entrust inmediatamente. Al continuar utilizando o confiando en cualquier Certificado de Entrust después de dicho cambio, usted acepta cumplir y estar obligado por el mismo. Se recomienda que los Solicitantes, Suscriptores, Partes que Confían y otros terceros busquen versiones actualizadas de esta CPS periódicamente consultando nuestro Repositorio. Estas disposiciones se aplican a todos los Solicitantes, Suscriptores, Partes que Confían y otros terceros.

1.6 Definiciones y acrónimos

1.6.1 Definiciones

Afiliado: Se entiende por Afiliado con respecto a Entrust a una persona o entidad que directa o indirectamente a través de uno o más intermediarios, controle, esté controlada o esté bajo control común de Entrust, y con respecto a cualquier otra parte, cualquier corporación u otra entidad que esté directa o indirectamente controlada por esa parte. En este contexto, una parte "controla" una corporación u otra entidad si posee directa o indirectamente o controla el cincuenta por ciento (50%) o más de los derechos de voto de la junta directiva u otro mecanismo de control o, en el caso de una entidad no corporativa, un interés equivalente.
Solicitante: Persona, entidad u organización que solicita un Certificado, pero que aún no lo ha recibido, o una persona, entidad u organización que actualmente tiene un Certificado o Certificados y que está solicitando la renovación de los mismos o un Certificado o Certificados adicionales.

Representante del Solicitante : véase la definición en los Requisitos de Referencia ("Baseline Requirements")
Proveedor de Aplicaciones de Software: Desarrollador de software de navegador de Internet u otro software que muestra o utiliza Certificados.
Carta de Declaración: véase la definición en los Requisitos de Referencia ("Baseline Requirements")
Nombre de Dominio de Autorización : véase la definición en los Requisitos de Referencia ("Baseline Requirements")
Puerto Autorizado : véase la definición en los Requisitos de Referencia ("Baseline Requirements").
Representante Autorizado: Un representante autorizado de una persona jurídica.
Nombre de Dominio Base : véase la definición en los requisitos de referencia ("Baseline Requirements")
Requisitos de Referencia o "Baseline Requirements": Los requisitos establecidos por el CA/Brower Forum para la emisión y gestión de Certificados Públicos de Confianza publicados en https://www.cabforum.org.
Día hábil : Cualquier día exceptuando sábado, domingo, festivo oficial o local en la ciudad de Madrid, España.
Par de Claves de CA: véase la definición en los requisitos de referencia ("Baseline Requirements").
Certificado: Documento digital emitido por la CA que, como mínimo: (a) identifica a la CA que lo emite, (b) nombra o identifica a un Sujeto, (c) contiene una Clave Pública de un Par de Claves, (d) identifica su Período Operativo, y (e) contiene un número de serie y está firmado digitalmente por una CA. El Certificado incluye los siguientes tipos de Certificados emitidos por la CA: Certificado Cualificado; y Certificado de tipo PSD2.
Solicitud de Certificado: El formulario y los datos de la solicitud realizada por una RA que opera bajo una CA y presentada por un Solicitante al requerir la emisión de un Certificado.
Aprobador de Certificados: Empleado o agente autorizado para aprobar una Solicitud de un Certificado para una organización.
Beneficiarios del Certificado : Todos los proveedores de aplicaciones de software con los que Entrust ha firmado un contrato para incluir su Certificado Raíz en el software distribuido por dichos proveedores, y los terceros que dependen de dicho Certificado durante su Período Operativo.
Solicitante de Certificado: Empleado o agente autorizado para solicitar un Certificado para una organización.
Lista de Revocación de Certificados: Lista con sellos de tiempo de los números de serie de los certificados revocados que han sido firmados digitalmente por una CA.
Informe de Problema de Certificado: véase la definición en los requisitos de referencia ("Baseline Requirements").
Perfil de Certificado: véase la definición en los requisitos de referencia ("Baseline Requirements").

Sistemas de Certificados: véase la definición en los Requisitos de Seguridad de la Red y del Sistema de Certificados.
Transparencia del Certificado: método para registrar públicamente Certificados de acuerdo con IETF RFC 6962.
Autoridad de Certificación: Autoridad de certificación operada por Entrust o en su nombre con el propósito de emitir, administrar, revocar, renovar y proporcionar acceso a Certificados. La CA (i) crea y firma digitalmente los Certificados que contienen, entre otras cosas, la Clave Pública de un Sujeto y otra información que tiene como objetivo identificar al Sujeto, (ii) pone a disposición Certificados para facilitar la comunicación con el Sujeto identificado en el Certificado, y (iii) crea y firma digitalmente las listas de revocación de Certificados que contienen información sobre los Certificados que han sido revocados y que ya no deben ser utilizados o no son garantes de confianza.
Autorización de la Autoridad de Certificación: véase la definición en los requisitos de referencia ("Baseline Requirements").
Declaración de Práctica de Certificación (CPS): este mismo documento, el cual es una declaración de las prácticas que la CA usa en la emisión, administración, revocación, renovación y provisión de acceso a Certificados, y los términos y condiciones bajo los cuales la CA pone a disposición dichos servicios.
Comerciales: se refiere a cualquier persona, entidad u organización a quien Entrust o una RA que opera bajo una CA le haya otorgado el derecho de promocionar Certificados.
Base de datos común de CA: depósito de datos de información de Certificados y CA.
Compromiso: significa una pérdida, divulgación o pérdida de control supuesta o real sobre información sensible o datos.
Firmante del Contrato: significa un empleado o agente autorizado para firmar el Acuerdo de Suscriptor en nombre de la organización.
Certificado(s) Cruzado(s) : véase la definición en los requisitos de referencia ("Baseline Requirements").
Cliente: significa la persona física o jurídica que ha celebrado un contrato con Entrust para la emisión de Certificados a los Suscriptores.
Contacto de Dominio: véase la definición en los requisitos de referencia ("Baseline Requirements").
Etiqueta de Dominio: véase la definición en los requisitos de referencia ("Baseline Requirements").
Nombre de Dominio: véase la definición en los requisitos de referencia ("Baseline Requirements").
Espacio de Nombre de Dominio: véase la definición en los requisitos de referencia ("Baseline Requirements").
Propietario de Nombre de Dominio: véase la definición en los requisitos de referencia ("Baseline Requirements").
Registrador de Nombre de Dominio: véase la definición en los requisitos de referencia ("Baseline Requirements").

Contacto de correo electrónico de DNS CAA: véase la definición en los requisitos de referencia ("Baseline Requirements").
Contacto telefónico de DNS CAA: véase la definición en los requisitos de referencia ("Baseline Requirements").
Contacto de correo electrónico de registro DNS TXT: véase la definición en los requisitos de referencia ("Baseline Requirements").
Contacto telefónico de registro DNS TXT: véase la definición en los requisitos de referencia ("Baseline Requirements").
Empresa RA: véase la definición en los requisitos de referencia ("Baseline Requirements").
Entrust: abreviatura de Entrust Limited.
Entrust Group: colectivamente, Entrust, sus Afiliados, sus otorgantes de licencias (inclusive, para evitar cualquier duda, Microsoft), sus revendedores, sus proveedores, sus comerciales, sus subcontratistas, sus distribuidores y los directores, funcionarios, empleados, agentes y contratistas independientes de cualquiera de ellos.
Afiliados de Entrust Group: colectivamente, Entrust Limited y Afiliados.
Entrust EU: abreviatura de Entrust EU, S.L.
Guía ETSI: las pautas de ETSI que figuran en ETSI EN 319 411-1 (V1.2.2); ETSI EN 319 411-2 (V2.2.2); ETSI TS 119 495 (V1.3.1) y documentos relacionados que se aplican a los Certificados Cualificados y a los Certificados Cualificados de tipo PSD2.
Certificado EV SSL: Certificado SSL emitido por una CA que cumple con los requisitos de las Guías EV SSL.
Guías EV SSL: Guías del CA / Browser Forum para la emisión y gestión de certificados de validación extendida (EV) publicados en https://www.cabforum.org. Las Guías EV SSL describen los requisitos que debe cumplir una CA para emitir certificados EV SSL. En caso de contradicción entre esta CPS y las Guías EV SSL, estas últimas tienen prioridad.
FIPS: Estándares Federales de Procesamiento de la Información, son las normas federales de los Estados Unidos que prescriben requisitos específicos de rendimiento, prácticas, formatos, protocolos de comunicación y otros requisitos para el de hardware, software, datos y telecomunicaciones.
Nombre de Dominio Completo: véase la definición en los requisitos de referencia ("Baseline Requirements").
IETF: Grupo de Trabajo de Ingeniería de Internet, comunidad internacional de diseñadores de redes, operadores, proveedores e investigadores interesados en la evolución de la arquitectura de Internet y su eficiente funcionamiento.
Agencia Incorporadora: véase la definición en las Guías EV SSL.
Estándares de la industria: significa, en conjunto, las versiones más actualizadas de cada uno de los siguientes: Guías SSL EV, Requisitos de Referencia o "Baseline Requirements", Guías ETSI y leyes y reglamentos, en cada caso, que son aplicables a los diversos tipos de Certificados de confianza pública emitidos por Entrust según

esta CPS, y a los que Entrust está sujeto y obligado como emisor de dichos Certificados.

Nombre Interno: véase la definición en los requisitos de referencia ("Baseline Requirements").

Dirección IP: Véase la definición en los requisitos de referencia ("Baseline Requirements").

Contacto de Dirección IP: véase la definición en los requisitos de referencia ("Baseline Requirements").

Autoridad de Registro de Dirección IP: véase la definición en los requisitos de referencia ("Baseline Requirements").

CA Emisora: En relación con un Certificado en particular, la CA que emitió el Certificado. Puede ser una CA Raíz o una CA Subordinada.

Compromiso de Clave: Véase la definición en los requisitos de referencia ("Baseline Requirements").

Par de Claves: Dos claves criptográficas relacionadas matemáticamente, que tienen las siguientes propiedades: (i) una clave puede ser utilizada para cifrar un mensaje que solo puede ser descifrado usando la otra clave, e (ii) incluso conociendo una clave, se considera que es inviable descubrir la otra clave mediante un proceso informático.

Autoridad Nacional Competente: tal como se usa en ETSI TS 119 495.

Identificador de objeto: Secuencia de números especialmente formateada que se registra de acuerdo con los procedimientos reconocidos internacionalmente para el registro de identificador de objeto.

Período Operativo: Con respecto a un Certificado, el período de su validez. El Período Operativo normalmente comenzaría en la fecha en que se emitió el Certificado (o en una fecha posterior como se especifique en el Certificado), y finaliza en la fecha y hora en que caduca, como se indique en el Certificado, o antes, si se revoca el Certificado.

Empresa matriz: Véase la definición en los requisitos de referencia ("Baseline Requirements").

PKIX: Grupo de Trabajo IETF que desarrolla especificaciones técnicas para componentes PKI basadas en Certificados X.509 de la versión 3.

Lugar de Negocios: Véase la definición en las Guías EV SSL.

Autoridad en Materia de Políticas: Personal que trabaja para Entrust EU o en su nombre y que es responsable de determinar las políticas y procedimientos que rigen el funcionamiento de las CA. La Autoridad en Materia de Políticas es responsable de crear, implementar y mantener una declaración de las prácticas y procedimientos utilizados para abordar todos los requisitos identificados para cada política de Entrust EU aplicable y su trabajo es supervisado por la gerencia ejecutiva senior de Entrust EU.

Clave Privada: Clave de un Par de Claves que se usa para descifrar un mensaje cifrado. Esta clave debe mantenerse secreta.

Certificado de tipo PSD2: Certificado Cualificado de Autenticación de Sitio Web de tipo PSD2 y / o Certificado Cualificado de Sello Electrónico de tipo PSD2.

Certificado Cualificado de Sello Electrónico de tipo PSD2: Certificado Cualificado de Sello Electrónico que se emite adicionalmente según los requisitos de las Normas técnicas de regulación PSD2 para el uso de certificados cualificados según lo definido en eIDAS (Reglamento (UE) No 910/2014) que incluye el Anexo IV para cumplir con los requisitos reglamentarios de PSD2 (Directiva (UE) 2015/2366), incluidos los requisitos de ETSI TS 119 495 y las Directrices ETSI relacionadas.

Certificado Cualificado de Autenticación de Sitio Web de tipo PSD2: Certificado Cualificado de Autenticación de Sitio Web emitido además según los requisitos de las Normas Técnicas Reguladoras de PSD2 para el uso de certificados cualificados según lo definido en eIDAS (Reglamento (UE) no 910/2014) incluyendo el Anexo IV para cumplir con los requisitos reglamentarios de PSD2 (Directiva (UE) 2015 / 2366), incluidos los requisitos de ETSI TS 119 495 y las Directrices de ETSI relacionadas.

Clave Pública: Clave de un Par de Claves que se usa para cifrar un mensaje. La Clave Pública está disponible para cualquier persona que desee enviar mensajes cifrados al titular de la Clave Privada. La Clave Pública generalmente se hace pública en un certificado emitido por una CA y se obtiene a menudo accediendo a un repositorio o base de datos. Se utiliza una Clave Pública para cifrar un mensaje que solo se puede descifrar por el titular de la correspondiente Clave Privada.

Certificado Cualificado: Certificado Cualificado de Autenticación de Sitio Web de tipo eIDAS, Certificado Cualificado de Sello Electrónico de tipo eIDAS y/o Certificado Cualificado de Firma Electrónica de tipo eIDAS.

Dispositivo Cualificado de Creación de Sello/Firma Electrónica: significa un dispositivo de creación de sello o firma electrónica que cumple con los requisitos estipulados en el Anexo II del Reglamento eIDAS (UE) 910/2014.

Fuente Gubernamental Cualificada de Información: Véase la definición en las Guías EV SSL.

Fuente Gubernamental Cualificada de Información Fiscal:Véase la definición en las Guías EV SSL.

Fuente Independiente Cualificada de Información: Véase la definición en las Guías EV SSL.

Certificado Cualificado de Sello Electrónico: Certificado emitido para su uso como un Certificado Cualificado de Sello Electrónico como se define en eIDAS (Reglamento (UE) No 910/2014), que incluye el Anexo III y los requisitos de ETSI EN 319 411-2 y las Directrices ETSI relacionadas

Certificado Cualificado de Firma Electrónica: Certificado emitido para su uso como un Certificado Cualificado de Firma Electrónica como se define en eIDAS (Reglamento (UE) No 910/2014), que incluye el Anexo I y los requisitos de ETSI EN 319 411-2 y las Directrices ETSI relacionadas

Certificado Cualificado de Sello de Tiempo: Certificado emitido para su uso como soporte de Sellos de Tiempo electrónicos como se define en eIDAS (Reglamento (UE) No 910/2014), incluyendo el Anexo III y los requisitos de ETSI EN 319 411-2 y las Directrices ETSI relacionadas.

Certificado Cualificado de Autenticación de Sitio Web: Certificado emitido para su uso como certificado cualificado de autenticación de sitio web según lo definido en eIDAS (Reglamento (UE) nº 910/2014), incluidos el anexo IV y los requisitos de ETSI EN 319 411-2 y las Directrices de ETSI relacionadas.
Valor Aleatorio: Véase la definición en los requisitos de referencia ("Baseline Requirements").
Agencia de Registro: Véase la definición en las Guías EV SSL.
Autoridad de Registro: Entidad que realiza dos funciones: (1) la recepción de información de un Sujeto nombrado en un Certificado, y (2) la verificación de la información proporcionada por el Sujeto siguiendo los procedimientos prescritos por las CA. En el caso de que la información proporcionada por un Sujeto cumpla con los criterios definidos por las CA, una RA puede enviar una solicitud a una CA solicitando que la CA genere, firme digitalmente y emita un Certificado que contenga la información verificada por la RA. Una RA puede ser operada por Entrust o por un tercero independiente.
Número de registro: Véase la definición en las Guías EV SSL.
Fuente Confiable de Datos: Véase la definición en los requisitos de referencia ("Baseline Requirements").
Método confiable de comunicación: Véase la definición en los requisitos de referencia ("Baseline Requirements").
Parte que Confía: Persona, entidad u organización que confía o utiliza un Certificado y / o cualquier otra información provista en un repositorio bajo una CA para obtener y confirmar la Clave Pública y la identidad de un Suscriptor. Para evitar dudas, un ASV no es una "Parte que Confía" cuando el software distribuido por dicho ASV simplemente muestra información sobre un Certificado.
Acuerdo de Parte que Confía: acuerdo entre la Parte que Confía y Entrust o entre la Parte que Confía y una RA de tercero independiente o un Revendedor bajo una CA con respecto a la disposición y el uso de cierta información y servicios con respecto a los Certificados.
Repositorio: Colección de bases de datos y sitios web que contienen información sobre los Certificados emitidos por una CA incluyendo, entre otras cosas, los tipos de Certificados y servicios proporcionados por la CA y las tarifas correspondientes, listas de revocación de certificados, respuestas de OCSP, descripciones de las prácticas y procedimientos de la CA, y otra información y acuerdos que están destinados a regir la utilización de Certificados emitidos por la CA.
Token de Solicitud: Véase la definición en los requisitos de referencia ("Baseline Requirements").
Valor de Solicitud: Véase la definición en los requisitos de referencia ("Baseline Requirements").
Contenido Requerido del Sitio Web: Véase la definición en los requisitos de referencia ("Baseline Requirements").
Revendedores: Cualquier persona, entidad u organización a la que Entrust o una RA que opera bajo una CA le haya otorgado el derecho de licenciar o el derecho de usar Certificados.

Dirección IP Reservada: Véase la definición en los requisitos de referencia ("Baseline Requirements").
Revocar o Revocación: Con respecto a un Certificado, finalizar prematuramente el Período Operativo de ese Certificado desde un momento concreto en adelante.
CA Raíz: CA de nivel superior enumeradas en §1.3.1.
Certificado SSL: Certificado emitido por una CA para su uso en servidores seguros.
CA Subordinada: CA subordinadas enumeradas en §1.3.1.
Certificado de CA Subordinada: Certificado que (i) incluye la Clave Pública de un Par de Claves Público-Privado generado por una Autoridad de Certificación; e (ii) incluye la firma digital de una CA raíz.
Sujeto: la persona, entidad u organización identificada en el campo "Subject" de un Certificado.
Suscriptor: Persona, entidad u organización que ha solicitado y ha recibido un Certificado.
Acuerdo de Suscriptor: Acuerdo entre un Suscriptor y Entrust (o un Afiliado de Entrust) o entre un Suscriptor y una RA de tercero independiente o un Revendedor bajo una CA con respecto a la emisión, gestión y provisión de acceso a un Certificado y la provisión de otros servicios con respecto a dicho Certificado. El Acuerdo de Suscriptor puede constar de una o más partes.
Compañía Subsidiaria: véase la definición en los requisitos de referencia ("Baseline Requirements").
Código Sospechoso: cualquier código o conjunto de instrucciones que contenga funciones maliciosas o vulnerabilidades graves, incluido el software espía, malware y otro código que se instala sin el consentimiento del usuario y/o resiste su propia eliminación, y código que pueda ser explotado de formas no previstas por sus diseñadores para comprometer la fiabilidad del entorno informático en el que se ejecuta.
CA Subordinada Técnicamente Restringida: Véase la definición en los requisitos de referencia ("Baseline Requirements").
Rol de Confianza: Véase la definición en los Requisitos del Sistema de Seguridad de Red y Certificado de CA/Browser Forum.
Especialista en Validación: Véase la definición en los requisitos de referencia ("Baseline Requirements").
Nombre de Dominio Comodín: véase la definición en los requisitos de referencia ("Baseline Requirements").
Método Verificado de Comunicación: Véase la definición en las Guías EV SSL.
Carta Profesional Verificada: Véase la definición en las Guías EV SSL.

1.6.2 Acrónimos

Por sus siglas en inglés:
ADN Nombre de dominio de autorización
ASV Proveedor de aplicación de software
CA Autoridad de certificación

CAA Autorización de autoridad de certificación
CCADB Base de Datos Común de CA
CPR Informe de problema de certificado
CPS Declaración de práctica de certificación
CRL Lista de revocación de certificados
CSR Solicitud de Firma de Certificado
CT Transparencia del certificado
DBA Haciendo negocios como
DN Nombre distinguido
DNS Sistema de nombres de dominio
DNSSEC Extensiones de seguridad del sistema de nombres de dominio
EAL Nivel de seguridad de la evaluación
eIDAS Identificación electrónica, autenticación y servicios de confianza
EKU Uso de clave extendida
ETSI Instituto europeo de estándares de Telecomunicación
EV Validación extendida
FIPS (Gobierno de los Estados Unidos) Estándar de procesamiento de información federal
FQDN Nombre de dominio completo
HTTP Protocolo de transferencia de hipertexto
HTTPS Protocolo de transferencia de hipertexto seguro
IANA Autoridad de asignación de números de Internet
ICANN Corporación de Internet para Nombres y Números Asignados
IETF Grupo de Trabajo de Ingeniería de Internet
ISO Organización Internacional de Normalización
ITU-T Unión Internacional de Telecomunicaciones - Sector de Normalización de las Telecomunicaciones
NCA Autoridad Nacional Competente
NDA Acuerdo de Confidencialidad
NIST (Gobierno de los Estados Unidos) Instituto Nacional de Estándares y Tecnología
OCSP Protocolo en línea de estado de certificado
OID Identificador de objeto
PA Autoridad en Materia de Políticas
PSD2 Directiva de servicios de pago (revisada)PDS Declaración de divulgación de PKI
PIN Número de identificación personal
PKI Infraestructura de Clave Pública
PSP Proveedor de servicios de pago
QGIS Fuente Gubernamental Cualificada de Información
QIIS Fuente Independiente Cualificada de Información
QSCD Dispositivo Cualificado de Creación de Sello/Firma Electrónica
QSealC Certificado Cualificado de Sello Electrónico
QSigC Certificado Cualificado de Firma Electrónica

QTIS Fuente Gubernamental Cualificada de Información Fiscal
QTSC Certificadl Cualificado de Sello de Tiempo
QWAC Certificado Cualificado de Autenticación de Sitio Web
RA Autoridad de Registro
RFC Petición de comentario
RSA Criptosistema Rivest – Shamir – Adleman
SAN Nombre alternativo del sujeto
SSL Capa de sockets seguros
S / MIME Secure MIME (Extensiones multipropósito de correo de Internet)
TLS Protocolo de la capa de transporte (Transport Layer Security)
TSA Autoridad de sello de tiempo
URL Localizador de recursos universal

2. Responsabilidades de publicación y Repositorio

Entrust mantiene el Repositorio para almacenar información diversa relacionada con los certificados y la operación de las CA y RA. La CPS y otra información relacionada se publica en el Repositorio.

2.1 Repositorios

Las CA mantienen los Repositorios para permitir el acceso a la información relacionada con los Certificados y la revocación de Certificados. La información en los Repositorios es accesible a través de una interfaz web, disponible 24x7, y se actualiza periódicamente como se establece en esta CPS. Los Repositorios son la única fuente aprobada de información sobre CRL y otra información sobre Certificados.

La CA se adherirá a la última versión de la CPS publicada en el Repositorio. Se puede acceder al Repositorio en https://www.entrust.net/CPS.

2.2 Publicación de información de certificación

La CA publica sus CPS, Certificados de CA, Acuerdos de Suscriptor, Acuerdos de Partes que confían, Informes de Auditoría, CRLs y la Declaración de divulgación de PKI en los Repositorios.

Esta CPS está estructurada en el formato RFC3647.

2.3 Plazo o frecuencia de las publicaciones

La CPS será reeditada y publicada al menos una vez al año. La CPS se actualizará con un número de versión incrementado y una nueva fecha anualmente, incluso si no se han realizado otros cambios en este documento.

Las CRLs se actualizarán según §4.9.7.

Las respuestas de OCSP se actualizarán de acuerdo con §4.9.10.

2.4 Controles de acceso a los Repositorios

La información publicada en el Repositorio es información pública. El acceso de solo lectura no está restringido. Las CA han implementado controles lógicos y físicos para evitar el acceso de escritura no autorizado a sus Repositorios.

Las versiones históricas de la CPS se mantienen en el Repositorio en la carpeta de archivo.

3. Identificación y autenticación

La Autoridad en Materia de Políticas exige prácticas de verificación para verificar la identificación y la autenticación, y podrá, a su discreción, actualizar dichas prácticas.

3.1 Nombramiento

Antes de emitir un Certificado, las CA aseguran que toda la información de la organización del Sujeto en el Certificado cumple con los requisitos de esta CPS, y ha sido verificada de acuerdo con los procedimientos prescritos en esta CPS y coincide con la información confirmada y documentada por la RA de conformidad con sus procesos de verificación.

QWAC de tipo eIDAS y QWAC de tipo PSD2

La CA y la RA deben seguir los procedimientos de verificación de esta CPS, las Guías EV SSL y las Guías ETSI y coincidir con la información confirmada y documentada por la RA de conformidad con sus procesos de verificación. Los procedimientos están destinados a lograr lo siguiente:

(i)Verificar la existencia e identidad del Solicitante, incluyendo;

a. Verificar la existencia legal y la identidad del Solicitante (como se estipula en las Guías EV SSL y las Guías ETSI),

b. Verificar la existencia física del Solicitante (presencia comercial en una dirección física), y

c. Verificar la existencia operativa del Solicitante (actividad comercial).

(ii)Verificar la autorización del Solicitante para el Certificado, incluyendo;

a. Verificar el nombre, el título y la autoridad del Firmante del Contrato, el Aprobador de Certificados y el Solicitante de Certificado;

b. Verificar que el Firmante del Contrato haya firmado el Acuerdo de Suscriptor; y

c. Verificar que un Aprobador de Certificados haya firmado o aprobado la Solicitud de Certificado

(iii) Para los Certificados Cualificados de Autenticación de Sitio Web de Tipo PSD2 verificar la información adicional requerida por ETSI TS 119 495, incluido el identificador de la organización del Solicitante asignado por una NCA y las funciones de proveedor de servicios de pago aprobadas del Solicitante

3.1.1 Tipos de nombres

Los nombres de los Sujetos en un Certificado cumplen con el formulario de Nombre Distinguido (DN) X.501. Las CA utilizarán una única convención de nomenclatura como se establece a continuación

Certificados Cualificados de Firma Electrónica
(i) “Nombre del país” (C), código ISO 3166 de dos letras para el país en el que el Solicitante está ubicado;
(ii) "Estado" (ST) (si aplica), estado o provincia en donde la organización realiza sus negocios;
(iii) “Localidad” (L), ciudad o localidad del lugar de negocios de la organización;
(iv) “Nombre de la organización” (O), nombre de la organización en el caso de una corporación, asociación, u otra entidad. En el caso de un propietario único, el nombre de la organización puede ser el nombre del Solicitante;
(v) "Nombre de la unidad organizativa" (OU), campo opcional. El campo OU puede ser usado para distinguir entre diferentes grupos organizativos dentro de una organización (por ejemplo, para distinguir entre recursos humanos, marketing y desarrollo:
(vi) "Apellido", apellido validado del Sujeto
(vii) "Nombre de pila", nombre de pila validado del Sujeto
(viii) "Número de serie", generado aleatoriamente y asignado al Sujeto;
(xix) "Nombre común" (CN), nombre de pila y apellido(s) del Sujeto.

Certificados Cualificados de Sello Electrónico
(i) “Nombre del país” (C), código ISO 3166 de dos letras para el país en el que el Solicitante está ubicado;
(ii) "Estado" (ST) (si aplica), estado o provincia en donde la organización realiza sus negocios;
(iii) “Localidad” (L), ciudad o localidad del lugar de negocios de la organización;
(iv) “Nombre de la organización” (O), nombre de la organización en el caso de una corporación, asociación, u otra entidad. En el caso de un propietario único, el nombre de la organización puede ser el nombre del Solicitante;
(v) "Identificador de la organización", identificador de la organización
(vi) "Nombre de la unidad organizativa" (OU), campo opcional. El campo OU puede ser usado para distinguir entre diferentes grupos organizativos dentro de una organización (por ejemplo, para distinguir entre recursos humanos, marketing y desarrollo:
(vii) "Nombre común" (CN), nombre común del Sujeto para denominarse a sí mismo.

Certificados Cualificados de Sello de Tiempo
(i) “Nombre del país” (C), el código ISO 3166 de dos letras para el país en el que se encuentra el Solicitante;
(ii) “Nombre de la Organización” (O), nombre de la organización en el caso de una corporación, sociedad u otra entidad. En el caso de una empresa unipersonal, el nombre de la organización puede ser el nombre del Solicitante;
(iii) “Identificador de la Organización”, el Identificador de la Organización;
(iv) “Nombre Común” (CN), identifica a la Autoridad de Sellado de Tiempo.

Certificados Cualificados de Sello Electrónico de tipo PSD2
(i) Igual que el Certificado Cualificado de Sello Electrónico, más
(ii) El "Identificador de organización" del Solicitante asignado por una NCA

Certificados Cualificados de Autenticación de Sitio Web
(i) "Nombre del país" (C), que es el código ISO 3166 de dos letras para el país en el que el Solicitante está ubicado y planea hospedar el servidor seguro en el cual el Solicitante tiene la intención de instalar el Certificado;
(ii)"Nombre de la organización" (O), que es el nombre de la organización en el caso de una corporación, asociación, u otra entidad. En el caso de un propietario único, el nombre de la organización puede ser el nombre del Solicitante;
(iii)"Nombre de la unidad organizativa" (OU), que es un campo opcional. El campo OU puede ser usado para distinguir entre diferentes grupos organizativos dentro de una organización (por ejemplo, para distinguir entre recursos humanos, marketing y desarrollo);
(iv)"Nombre común" (CN), que es el nombre de host, el nombre de host completo o la ruta utilizada en el DNS del servidor seguro en el que el Solicitante pretende instalar el Certificado;
(v)"Localidad" (L), que es la ciudad o localidad del lugar de negocios de la organización;
(vi)"Estado" (ST) (si corresponde), que es el estado o provincia del lugar de la organización negocio;
(vii)"Número de serie", que es el número de registro del Suscriptor;
(viii)" Categoría de negocio", que es la cláusula de categoría de negocio aplicable según las Guías EV SSL;
(ix)"JurisdiccióndeConstituciónLocalidadNombre" (si corresponde) que es la jurisdicción de registro o localidad de constitución del Suscriptor;
(x)"JurisdiccióndeConstituciónNombredeRegiónOProvincia" (si corresponde) que es la jurisdicción del registro o región o provincia de constitución del Suscriptor; y
(xi)"JurisdiccióndePaísdeCorporación" que es la jurisdicción de registro o país de constitución del Suscriptor.

A partir del 1 de septiembre de 2022 o antes, el campo OU no se incluirá en los QWAC de tipo eIDAS.

La CA no incluye ningún atributo de nombre de Sujeto que no esté definido en la sección 9.2 de las Guías de EV SSL.

Certificados Cualificados de Autenticación de Sitio Web de tipo PSD2
(i) Mismo nombre de Sujeto que los Certificados Cualificados de Autenticación de Sitio Web, más
(ii) El "Identificador de organización" del Solicitante asignado por una NCA se incluye en una extensión separada.

A partir del 1 de septiembre de 2022 o antes, el campo OU no se incluirá en los QWAC de tipo PSD2.

3.1.2 Necesidad de que los nombres sean significativos

Los Certificados emitidos de conformidad con esta CPS son significativos solo si los nombres que aparecen en los Certificados pueden ser entendidos y utilizados por las Partes que Confían. Los nombres utilizados en los Certificados deben identificar a la persona u objeto al que están asignados de forma clara. Las CA no emitirán Certificados a los Suscriptores que contengan Nombres de Dominio, Direcciones IP, DN, URL y / o direcciones de correo electrónico de los que los Suscriptores no tengan legítimamente propiedad o control. Ejemplos de campos y extensiones donde aparecen estos nombres incluyen DN y nombres alternativos del sujeto.

QSigC de tipo eIDAS

El valor del Nombre Común que se utilizará en un QSigC de tipo eIDAS es el nombre de pila y apellido(s) del Sujeto.

QSealC de tipo eIDAS y QSealC de tipo PSD2

El valor del Nombre Común que se utilizará en un QsealC de tipo eIDAs y en un QsealC de tipo PSD2 es el nombre de la organización del Solicitante.

QTSC de tipo eIDAS

El valor del Nombre Común a utilizar en eIDAS QTSC es el nombre de la Autoridad de Sellado de Tiempo.

QWAC de tipo eIDAS y QWAC de tipo PSD2

El valor del Nombre Común que se utilizará en un QWAC de tipo eIDAS o QWAC de tipo PSD2 será el FQDN del Solicitante que se utiliza en el DNS del servidor seguro en el que el Solicitante tiene la intención de instalar el Certificado. El FQDN de un QWAC de tipo eIDAS o QWAC de tipo PSD2 no puede ser una dirección IP o un Nombre de Dominio Comodín.

3.1.3 Anonimato o uso de seudónimo de los Suscriptores

Los Nombres de Dominio Internacionales (IDN) se verificarán y representarán en commonName y subjectAltName mediante Punycode.

3.1.4 Reglas para interpretar varios formas de nombres

No está estipulado.

3.1.5 Singularidad de los nombres

Los nombres se deberán definir de manera inequívoca para cada Sujeto en un Repositorio. El atributo de nombre de Sujeto deberá ser exclusivo del Sujeto para el que se emite.

QSigC de tipo eIDAS

Se incluye un número único en el atributo de número de serie del nombre del sujeto según ETSI EN 319 412-1 y se determina de la siguiente manera:
i. Si el Sujeto tiene un número de Documento Nacional de Identidad español, un número de identidad de extranjero español o un número de identificación fiscal español, entonces este número se incluye en el Certificado;
ii. Si el Sujeto no tiene Número de Documento Nacional de Identidad español, número de identidad de extranjero español, ni número de identificación fiscal español, entonces se incluirá en el Certificado un número aleatorio o un Número de Identidad Nacional de otro país.

QSealC de tipo eIDAS, QTSC de tipo eIDAS y QSealC de tipo PSD2
Se incluye un número único en el atributo de identificador de organización del nombre del Sujeto según ETSI 319 412-1. Este número será un número de identificación fiscal o, en su defecto, otro código identificativo que lo identifique de manera única y permanente en el tiempo según conste en los registros oficiales.

QWAC de tipo eIDAS y QWAC de tipo PSD2
Se incluye un número único en el atributo de número de serie del nombre del Sujeto según las Guías EV SSL. Este número podrá ser un número de identificación fiscal o, en su defecto, otro código identificativo que lo identifique de manera única y permanente en el tiempo según conste en los registros oficiales.

3.1.6 Reconocimiento, autenticación y función de las marcas comerciales
Los Suscriptores no deben solicitar Certificados con ningún contenido que infrinja los derechos de propiedad intelectual de otra entidad. A menos que se indique específicamente lo contrario en esta CPS, Entrust no verifica el derecho de un Solicitante a usar una marca comercial y no resuelve disputas de marcas comerciales. Entrust puede rechazar cualquier solicitud o solicitar la revocación de cualquier Certificado que sea parte de una disputa de marca registrada.

3.2 Validación inicial de identidad

3.2.1 Método para demostrar la posesión de una Clave Privada
Para los Pares de Claves generados por el Solicitante, las CA realizan pruebas de posesión para los CSRs creados usando algoritmos asimétricos reversibles (como RSA) mediante la validación de la firma en el CSR presentado por el Solicitante con la Solicitud de Certificado.

3.2.2 Autenticación de la identidad de la organización
Entrust utiliza un proceso interno para verificar la precisión de las fuentes de información y las bases de datos para garantizar que los datos sean aceptables, incluida la revisión de los términos de uso del proveedor de la base de datos. Antes de utilizar cualquier fuente de datos como fuente de datos confiable o QIIS, la fuente se evalúa en cuanto a su confiabilidad, precisión y resistencia a la alteración o

falsificación. El proceso de precisión aborda los requisitos de la sección 3.2.2.7 de los Requisitos de Referencia y la sección 11.11.5 de las Guías SSL EV.

3.2.2.1 Identidad

La CA o la RA realiza la verificación de cualquier identidad organizativa que sea presentada por un Solicitante o Suscriptor de acuerdo con las prácticas exigidas por la Autoridad en Materia de Políticas. La CA o la RA determina si la identidad de la organización, la dirección y el Nombre de Dominio suministrados en una Solicitud de Certificado están en consonancia con la información contenida en bases de datos de terceros y / o fuentes gubernamentales. La información y las fuentes utilizadas para la verificación de las Solicitudes de Certificado pueden variar dependiendo de la jurisdicción del Solicitante o Suscriptor.

En el caso de identidades de organizaciones que no estén registradas por ninguna fuente gubernamental, la CA o la RA hace esfuerzos comercialmente razonables para confirmar la existencia de dichas organizaciones. Tales esfuerzos pueden incluir visitas a los locales o una carta de certificación de un tercero.

QWAC de tipo eIDAS, QWAC de tipo PSD2, QSealC de tipo eIDAS, QSealC de tipo PSD2 y QTSC de tipo eIDAS

La CA o RA identificará la organización y, si corresponde, cualquier atributo específico de la organización será verificado por un Representante Autorizado.

QWAC de tipo eIDAS y de tipo PSD2

Las RA que operan bajo las CA determinarán:

(i) Nombre legal completo
(ii) Categoría de Negocio , que puede ser “Organización Privada”, “Entidad Gubernamental” o “Entidad No Comercial”
(iii) Jurisdicción de Constitución o Registro, que no incluirá información que no sea relevante para la Agencia de Constitución o Registro;
(iv) Número de Registro o en su defecto, la fecha de registro;
(v) Dirección física del lugar de negocios; y
(vi) Existencia Operacional.

Entrust no emite Certificados a Sujetos de Entidades Comerciales como se define en la sección 11.2.2 de las Guías SSL EV.

Antes del uso de una Agencia Incorporadora o Agencia de Registro para cumplir con estos requisitos de verificación, la información de la agencia sobre la Agencia Incorporadora o Agencia de Registro se divulgará en https://www.entrust.net/CPS.

La información de esta agencia incluye lo siguiente:

(vii) Información suficiente para identificar inequívocamente la Agencia Incorporadora o la Agencia de Registro (como un nombre, jurisdicción y sitio web);

(viii) El valor o valores aceptados para cada uno de los campos: subject:jurisdictionLocalityName (OID: 1.3.6.1.4.1.311.60.2.1.1), subject:jurisdictionStateOrProvinceName (OID: 1.3.6.1.4.1.311.60.2.1.2), y subject:jurisdictionCountryName (OID: 1.3.6.1.4.1 .311.60.2.1.3), cuando se emite un Certificado utilizando información de esa Agencia Incorporadora o Agencia de Registro, indicando las jurisdicciones para las que la agencia es apropiada; y,
(ix) Un historial de revisión que incluye un número de versión único y la fecha de publicación para cualquier adición, modificación y/o eliminación de esta lista.

Certificados de tipo PSD2
Las RA que operan bajo las CA también determinarán:
(x) NCA aplicable
(xi) Identificador de la organización asignado por la NCA
(xii) Roles de proveedores de servicios de pago aprobados por la NCA.
Nota: Las RA deben cumplir con las reglas específicas de NCA para verificar estos atributos.

3.2.2.2 DBA / nombre comercial

Si el campo organización del sujeto es un DBA o nombre comercial, la CA o la RA verificará el derecho del Solicitante de usar el DBA / nombre comercial utilizando al menos uno de los siguientes medios:

(i) La RA puede verificar el nombre mediante el uso de una Fuente de Información Gubernamental Cualificada operada por una agencia gubernamental, o en su nombre, apropiada en la jurisdicción del Lugar de Negocios o por contacto directo y en persona con dicha agencia gubernamental.
(ii) La RA puede verificar el nombre mediante el uso de una Fuente de Información Independiente Cualificada (QIIS), siempre que la QIIS haya verificado el nombre asumido con la agencia gubernamental correspondiente.
(iii) La RA puede confiar en una Carta Profesional Verificada que indique el nombre bajo el cual el Solicitante realiza negocios, la agencia gubernamental en la que está registrado el nombre y la vigencia de dicho registro.

La CA o RA garantiza que el registro del DBA o nombre comercial es válido.

QWAC de tipo eIDAS y de tipo PSD2
La CA verifica que el Solicitante haya registrado su uso del DBA o el nombre comercial con la agencia gubernamental correspondiente para dichas presentaciones en la jurisdicción de su lugar de negocios. Si se utiliza un DBA o un nombre comercial, se incluirá al principio del campo de la organización seguido del nombre legal completo de la organización entre paréntesis.

3.2.2.3 Verificación del país

La verificación del país se realizará de acuerdo con los métodos indicados en § 3.2.2.1.

3.2.2.4 Validación de la autorización o control de dominio

La CA confirmará que antes de la emisión, la CA o la RA validaron cada Nombre de Dominio totalmente calificado (FQDN) listado en el Certificado usando al menos uno de los métodos listados a continuación.

Las validaciones completas de la autoridad del Solicitante se pueden utilizar para la emisión de múltiples Certificados a lo largo del tiempo. Para la validación de dominio, el término Solicitante incluye la Compañía matriz del Solicitante, Empresa Filial o afiliada.

La CA mantiene un registro de qué método de validación de dominio se utilizó para validar cada dominio.

3.2.2.4.1 Validación del Solicitante como un Contacto de Dominio

Este método de validación de dominio no se utiliza.

3.2.2.4.2 Correo electrónico, Fax, SMS o Correo Postal a un Contacto de Dominio

Se confirmará el control del Solicitante sobre el FQDN enviando un Valor Aleatorio por correo electrónico, fax, SMS o correo postal y recibiendo después una respuesta de confirmación que utilice el Valor Aleatorio. El Valor Aleatorio debe ser enviado a una dirección de correo electrónico, número de fax / SMS o dirección de correo postal identificada como un Contacto de Dominio.

Cada correo electrónico, fax, SMS o correo postal puede confirmar el control de múltiples ADNs.

La CA o RA puede enviar el correo electrónico, fax, SMS o correo postal identificado en esta sección a más de un destinatario siempre que cada Registrador de Nombre de Dominio identifique a cada destinatario como representante del Propietario de Nombre de Dominio para cada FQDN que se verifique mediante el correo electrónico, fax, SMS o correo postal.

El Valor Aleatorio es único en cada correo electrónico, fax, SMS o correo postal.

La CA o la RA puede reenviar el correo electrónico, fax, SMS o correo postal en su totalidad, incluida la reutilización del Valor Aleatorio, siempre que el contenido completo de la comunicación y los destinatarios no se modifiquen.

El Valor Aleatorio seguirá siendo válido para su uso en una respuesta de confirmación durante no más de 30 días a partir de su creación.

3.2.2.4.3 Contacto Telefónico con Contacto de Dominio
Este método de validación de dominio no se utiliza.

3.2.2.4.4 Correo electrónico creado para Contacto de Dominio
Se confirmará el control del Solicitante sobre el FQDN (i) enviando un correo electrónico a una o más direcciones creadas utilizando 'admin', 'administrador', 'webmaster', 'hostmaster' o 'postmaster' como parte local, seguido de at-sign ("@"), seguido de un ADN, (ii) incluyendo un Valor Aleatorio en el correo electrónico, y (iii) recibiendo una respuesta de confirmación utilizando el Valor Aleatorio.

Cada correo electrónico puede confirmar el control de múltiples FQDN, siempre que el ADN utilizado en el correo electrónico sea un ADN para cada FQDN que se confirma.

El Valor Aleatorio será único en cada correo electrónico.

El correo electrónico puede reenviarse en su totalidad, incluida la reutilización del Valor Aleatorio, siempre que los contenidos y el destinatario permanezcan sin cambios.

El Valor Aleatorio seguirá siendo válido para su uso en una respuesta de confirmación durante no más de 30 días a partir de su creación.

3.2.2.4.5 Documento de Autorización de Dominio
Este método de validación de dominio no se utiliza.

3.2.2.4.6 Cambio acordado en el sitio web
Este método de validación de dominio no se utiliza,

3.2.2.4.7 Cambio de DNS
Se confirmará el control del solicitante sobre el FQDN al confirmar la presencia de un Valor Aleatorio en el registro DNS CNAME, TXT o CAA para un ADN o un ADN que tenga un prefijo con una Etiqueta de Dominio que comience con un carácter subrayado.
Si se utiliza un Valor Aleatorio, la CA o RA proporcionará un Valor Aleatorio único para la solicitud de Certificado y no deberá usar el Valor Aleatorio después de (i) 30 días o (ii) si el Solicitante presentó la solicitud del Certificado, en el período de tiempo permitido para la reutilización de información validada relevante para el Certificado.

3.2.2.4.8 Dirección IP

Se confirmará el control del Solicitante sobre el FQDN al confirmar que el Solicitante controla una Dirección IP devuelta de una búsqueda de DNS para los registros A o AAAA para el FQDN de acuerdo con la sección § 3.2.2.5.

Una vez que se haya validado el FQDN utilizando este método, la CA NO PUEDE emitir también Certificados para FQDNs para niveles de dominio de nivel superior que terminan en el FQDN validado a menos que la CA realice una validación por separado para ese FQDN utilizando un método autorizado.

3.2.2.4.9 Certificado de prueba
Este método de validación de dominio no se utiliza.

3.2.2.4.10 TLS usando un número aleatorio
Este método de validación de dominio no se utiliza.

3.2.2.4.11 Cualquier otro método
Este método de validación de dominio no se utiliza.

3.2.2.4.12 Validación del Solicitante como un Contacto de Dominio
Este método de validación de dominio no se utiliza.

3.2.2.4.13 Correo electrónico para el contacto de DNS CAA
Se confirmará el control del Solicitante sobre el FQDN enviando un Valor Aleatorio por correo electrónico y luego recibiendo una respuesta de confirmación utilizando el Valor Aleatorio. El Valor Aleatorio se enviará al correo electrónico de contacto de la DNS CAA. El conjunto relevante de registros de recursos de la CAA se encontrará utilizando el algoritmo de búsqueda definido en RFC 8659 Sección 3.

Cada correo electrónico puede confirmar el control de múltiples FQDN, siempre que cada dirección de correo electrónico sea un Contacto de Correo Electrónico de DNS CAA para cada nombre de ADN que se valide. Se puede enviar el mismo correo electrónico a múltiples destinatarios siempre que todos los destinatarios sean los Contactos de Correo Electrónico de DNS CAA para cada ADN que se esté validando.

El Valor Aleatorio será único en cada correo electrónico. El correo electrónico puede reenviarse en su totalidad, incluida la reutilización del Valor Aleatorio, siempre que su contenido y destinatarios permanezcan sin cambios. El Valor Aleatorio seguirá siendo válido para su uso en una respuesta de confirmación durante no más de 30 días desde su creación.

3.2.2.4.14 Correo electrónico para el contacto DNS TXT
Se confirmará el control del Solicitante sobre el FQDN enviando un Valor Aleatorio por correo electrónico y luego recibiendo una respuesta de confirmación utilizando

el Valor Aleatorio. El Valor Aleatorio se enviará al Contacto de Correo electrónico de registro DNS TXT para el ADN seleccionado para validar el FQDN.

Cada correo electrónico puede confirmar el control de múltiples FQDN, siempre que cada dirección de correo electrónico sea el correo electrónico de contacto de registro DNS TXT para cada ADN que se valide. Se puede enviar el mismo correo electrónico a múltiples destinatarios siempre que todos los destinatarios sean los correos electrónicos de contacto de registro DNS TXT para cada ADN que se esté validando.

El Valor Aleatorio será único en cada correo electrónico. El correo electrónico puede reenviarse en su totalidad, incluida la reutilización del Valor Aleatorio, siempre que su contenido y destinatarios permanezcan sin cambios. El Valor Aleatorio seguirá siendo válido para su uso en una respuesta de confirmación durante no más de 30 días desde su creación.

3.2.2.4.15 Teléfono con Contacto de Dominio

Se confirmará el control del Solicitante sobre el FQDN llamando al número de teléfono del Contacto de Dominio y obteniendo una respuesta de confirmación para validar el ADN. Cada llamada telefónica puede confirmar el control de múltiples ADN siempre que el mismo número de teléfono de Contacto de Dominio esté en la lista para cada ADN que se verifica y se proporcione una respuesta de confirmación para cada ADN.

En el caso de que se contacte con alguien que no sea el Contacto de Dominio, la CA puede solicitar que se transfiera la llamada al Contacto de Dominio.

En caso de llegar al correo de voz, la CA puede dejar el Valor Aleatorio y el ADN o ADNs que está siendo validado. El Valor Aleatorio debe devolverse a la CA para aprobar la solicitud.

El Valor Aleatorio seguirá siendo válido para su uso en una respuesta de confirmación durante no más de 30 días desde su creación.

3.2.2.4.16 Contacto telefónico con Contacto Telefónico de Registro DNS TXT

Se confirma el control del solicitante sobre el FQDN llamando al número de teléfono del Contacto Telefónico de Registro DNS TXT y se obtiene una respuesta de confirmación para validar el ADN. Cada llamada telefónica puede confirmar el control de múltiples ADN, siempre que el mismo número de teléfono del Contacto Telefónico de Registro DNS TXT aparezca en la lista para cada ADN que se verifica y proporcione una respuesta de confirmación para cada ADN.

La CA no debe ser transfiera conscientemente o solicitar ser transferida ya que este número de teléfono se ha incluido específicamente para fines de validación de dominio.

En caso de acceder al buzón de voz, la CA puede dejar el Valor Aleatorio y el/los ADN a validar. El Valor Aleatorio debe devolverse a la CA para aprobar la solicitud.

El Valor Aleatorio seguirá siendo válido para su uso en una respuesta de confirmación durante no más de 30 días desde su creación.

3.2.2.4.17 Contacto telefónico con el Contacto Telefónico de DNS CAA

Se confirma el control del solicitante sobre el FQDN llamando al número de teléfono del Contacto Telefónico de DNS CAA y se obtiene una respuesta de confirmación para validar el ADN. Cada llamada telefónica puede confirmar el control de múltiples ADN siempre que el mismo número de teléfono de Contacto Telefónico de DNS CAA aparezca en la lista para cada ADN que se verifica y proporcione una respuesta de confirmación para cada ADN. El conjunto de registros de recursos de CAA relevante se debe encontrar utilizando el algoritmo de búsqueda definido en RFC 8659 Sección 3.

La CA no debe ser transfiera conscientemente o solicitar ser transferida ya que este número de teléfono se ha incluido específicamente para fines de validación de dominio.

En caso de acceder al buzón de voz, la CA puede dejar el Valor Aleatorio y el/los ADN a validar. El valor aleatorio debe devolverse a la CA para aprobar la solicitud. El valor aleatorio seguirá siendo válido para su uso en una respuesta de confirmación durante no más de 30 días desde su creación.

3.2.2.4.18 Cambio acordado en el sitio web v2

Se confirma el control del solicitante sobre el FQDN verificando que el Token de Solicitud o el Valor Aleatorio esté contenido en un archivo.

> (i) El Token de Solicitud o el Valor Aleatorio completo no debe aparecer en la solicitud utilizada para recuperar el archivo, y
> (ii) la CA DEBE recibir una respuesta HTTP satisfactoria de la solicitud (lo que significa que se debe recibir un código de estado HTTP 2xx).

El archivo que contiene el Token de Solicitud o el Valor Aleatorio:

> (iii) Debe estar ubicado en el Nombre de Dominio de Autorización, y
> (iv) Debe estar ubicado en el directorio "/.well-known/pki-validation", y
> (v) Debe recuperarse a través del esquema "http" o "https", y
> (vi) Debe ser accesible a través de un Puerto Autorizado.

La CA sigue redirecciones y se aplica lo siguiente:

(vii) Las redirecciones deben iniciarse en la capa de protocolo HTTP.

a) Para las validaciones realizadas a partir del 1 de julio de 2021, las redirecciones solo serán el resultado de una respuesta de código de estado HTTP 301, 302 o 307, como se define en RFC 7231, Sección 6.4, o una respuesta de código de estado HTTP 308, como se define en RFC 7538, Sección 3. Los redireccionamientos deben ser al valor final del encabezado de respuesta de HTTP de Ubicación, como se define en RFC 7231, Sección 7.1.2.
b) Para las validaciones realizadas antes del 1 de julio de 2021, las redirecciones solo serán el resultado de un resultado de código de estado HTTP dentro de la clase de redirección 3xx de códigos de estado, como se define en RFC 7231, Sección 6.4.

(vii) Las redirecciones deben ser a las URL de recurso con el esquema "http" o "https".

(ix) Los redireccionamientos deben realizarse a las URL de recursos a las que se accede a través de Puertos Autorizados.

Si se usa un Valor Aleatorio, entonces:

(x) La CA debe proporcionar un Valor Aleatorio exclusivo para la solicitud de certificado.

(xi) El Valor Aleatorio debe permanecer válido para su uso en una respuesta de confirmación durante no más de 30 días desde su creación. La CPS PUEDE especificar un período de validez más corto para los valores aleatorios, en cuyo caso la CA debe seguir su CPS.

Nota: Una vez que el FQDN ha sido validado utilizando este método, la CA NO emite Certificados para otros FQDN que terminen con todas las Etiquetas de Dominio del FQDN validado.

3.2.2.4.19 Cambio acordado en el sitio web - ACME

Este método de validación de dominio no se utiliza.

3.2.2.4.20 TLS con ALPN

Este método de validación de dominio no se utiliza.

3.2.2.5 Autenticación de una Dirección IP

Las direcciones IP no están permitidas para Certificados.

3.2.2.6 Validación de comodines

Los comodines no están permitidos para los QWAC de tipo eIDAS o los QWAC de tipo PSD2.

3.2.2.7 Precisión de la fuente de datos

Antes de utilizar cualquier fuente de datos como fuente de datos confiable, la RA evaluará la fuente para determinar su fiabilidad, precisión, y resistencia a la alteración o falsificación.

3.2.2.8 Registros CAA
La política de Entrust sobre los registros CAA se establece en §4.2.4.

3.2.2.9 Autenticación de dirección de correo electrónico
La CA no incluye direcciones de correo electrónico en los Certificados.

3.2.2.10 Identificador de la organización
El identificador de la organización debe contener una referencia de registro para una entidad jurídica asignada de acuerdo con el esquema de registro identificado.

El esquema de registro debe identificarse utilizando la siguiente estructura en el orden presentado:
(i) identificador de esquema de registro de 3 caracteres;
(ii) código de país ISO 3166 de 2 caracteres para el país en el que se opera el esquema de registro,
o
(iii) si el esquema se opera globalmente se utilizará el código ISO 3166 "XG";
(iv) para el identificador del esquema de registro NTR, si es necesario, un identificador ISO 3166-2 de 2 caracteres para la subdivisión (estado o provincia) del país en el que opera el esquema de registro, precedido por más "+" (0x2B (ASCII), U + 002B (UTF-8));
(v) un guión menos "-" (0x2D (ASCII), U + 002D (UTF-8));
(vi) referencia de registro asignada de acuerdo con el esquema de registro identificado

Nota: Las referencias de registro pueden contener guiones, pero los esquemas de registro, los códigos de país ISO 3166 y los identificadores ISO 3166-2, no. Por lo tanto, si aparece más de un guión en la estructura, el guión más a la izquierda es un separador, y los guiones restantes son parte de la referencia de registro.

La CA o RA deberá:

> (vii) confirmar que la organización representada por la referencia de registro es la misma que la organización nombrada dentro del contexto de la jurisdicción del Sujeto según §3.2.2.1;
> (viii) verificar que la referencia de registro coincida con otra información verificada de acuerdo con §3.2.2;
> (ix) tomar las medidas apropiadas para desambiguar diferentes organizaciones, como se describe en el Apéndice B para cada esquema de registro;

(x) aplicar las reglas de validación relevantes para el esquema de registro como se especifica en el Apéndice B.

3.2.3 Autenticación de la identidad individual

La CA o la RA utiliza los métodos que se detallan a continuación para verificar las identidades individuales presentadas por un Solicitante o Suscriptor.

La CA o RA verificará al Representante Autorizado o Sujeto mediante:

(i) Presencia física;

a) Una persona física que solicite un Certificado Cualificado deberá comparecer ante la CA o RA y aportar una identificación como el Documento Nacional de Identidad, pasaporte u otro medio admitido por Ley. Se podrá dispensar la presencia física de la persona física que solicita el Certificado Cualificado si su firma en la solicitud de emisión de Certificado Cualificado ha sido legitimada ante notario.
b) Si la persona física que solicita un Certificado Cualificado ya tiene una relación preexistente con la CA y ha tenido una identificación presencial en los últimos 5 años, entonces no será necesario repetir la verificación presencial.
c) La CA o RA verifica datos relativos a la constitución y personalidad jurídica, así como la extensión y vigencia de las facultades de representación del Representante Autorizado mediante los documentos que sirven para acreditar de forma fehaciente los puntos antes mencionados y su inscripción en el correspondiente registro público si así se requiere;

(ii) Mediante un Certificado de una firma electrónica cualificada o de un sello electrónico cualificado.

o

(iii) Mediante la utilización de identificación remota por video de acuerdo con la Orden Española ETD 465/2021 de 6 de mayo, que regula los métodos de identificación remota por video para la emisión de certificados electrónicos cualificados.

QWAC de tipo eIDAS y QWAC de tipo PSD2

Las RA que operan bajo las CA deben realizar una verificación de la identidad y la autoridad del Firmante del Contrato, el Aprobador de Certificados y el Solicitante de Certificados asociados con las Solicitudes de Certificados presentadas por un Solicitante o Suscriptor. Para establecer la exactitud de una identidad individual, la RA que opera bajo una CA deberá realizar una verificación de identidad y autoridad consistente con los requisitos establecidos en las Guías EV SSL publicadas por el CA / Browser Forum y las Guías ETSI.

3.2.4 Información del Suscriptor no verificada

Toda la información de solicitud de Certificado proporcionada por el Suscriptor se verifica de acuerdo con una fuente de información independiente o un canal de comunicación alternativo antes de incluirla en el Certificado.

3.2.5 Validación de Autoridad

Si el Solicitante de un Certificado que contiene información de identidad del sujeto es una organización, la CA o RA utilizará un Método Confiable de Comunicación para verificar la autoridad y aprobación del representante del Solicitante para actuar como RA de empresa, para solicitar la emisión y revocación de Certificados, o para asignar responsabilidades a otros para que actúen en estos roles.

La RA puede usar las fuentes enumeradas en §3.2.2.1 para verificar el Método Confiable de Comunicación. Siempre que la RA utilice un Método Confiable de Comunicación, la RA puede establecer la autenticidad del Certificado solicitado directamente con el representante del Solicitante o con una fuente autorizada dentro de la organización, como las oficinas de negocio principales del Solicitante, oficinas corporativas, oficinas de recursos humanos, oficinas de tecnología de la información u otro departamento que la RA considere apropiado.

La CA permite a un Suscriptor especificar las personas que pueden solicitar Certificados y no aceptará ninguna solicitud de Certificado que esté fuera de esta especificación. Las CA proporcionarán a un Suscriptor una lista de individuos autorizados, en respuesta a la solicitud por escrito verificada del Suscriptor.

QWAC de tipo eIDAS y QWAC de tipo PSD2

La CA o RA debe verificar la identidad y la autoridad del Firmante del Contrato y del Aprobador de Certificados de acuerdo con la sección 11.8 de las Guías EV SSL.

3.2.6 Criterios para la interpretación

Los Certificados Cruzados emitidos externamente que identifican a Entrust como el sujeto se encuentran en §1.3.1, siempre que Entrust haya dispuesto o aceptado el establecimiento de la relación de confianza (es decir, el Certificado Cruzado en cuestión).

3.3 Identificación y autenticación para solicitudes de cambio de clave

3.3.1 Identificación y autenticación para la rutina de cambio de clave

Cada Certificado deberá contener una fecha de vencimiento del Certificado. La razón de tener una fecha de vencimiento del Certificado es minimizar la exposición del Par de Claves asociado con el Certificado. Por esta razón, cuando se procesa una nueva solicitud de Certificado, la CA recomienda que se genere un nuevo Par de Claves y que la nueva Clave Pública de este Par de Claves se envíe junto con la solicitud de Certificado del solicitante. Si un Suscriptor desea continuar utilizando un Certificado más allá de la fecha de vencimiento del Certificado actual, el

Suscriptor debe obtener un nuevo Certificado y reemplazar el Certificado que está a punto de caducar. Los Suscriptores que envían una nueva solicitud de Certificado deberán completar el proceso de solicitud inicial, como se describe en §4.1. Las RA pueden reutilizar documentos y datos provistos en §3.2 para verificar la información del Certificado según la sección §4.2.1.2.

La RA que procesó la Solicitud de Certificado del Suscriptor realizará un esfuerzo comercialmente razonable para notificar a los Suscriptores de la próxima expiración de su Certificado mediante el envío de un correo electrónico al contacto técnico citado en la correspondiente Solicitud de Certificado. Al expirar un Certificado, el Suscriptor deberá cesar de usar dicho Certificado inmediatamente y lo eliminará de cualquier dispositivo y / o software en el que se ha instalado.

QWAC de tipo eIDAS y QWAC de tipo PSD2
El Suscriptor puede solicitar un Certificado de reemplazo utilizando un Par de Claves existente.

3.3.2 Identificación y autenticación para cambio de clave después de la revocación

Las CA y las RA que operan bajo las CA no renuevan los Certificados revocados. Si un Suscriptor desea utilizar un Certificado después de la revocación, el Suscriptor debe solicitar un nuevo Certificado y reemplazar el Certificado que ha sido revocado. Para obtener otro Certificado, se requerirá que el Suscriptor complete el proceso de solicitud inicial, como se describe en §4.1. Tras la revocación de un Certificado, el Suscriptor dejará de utilizar dicho Certificado inmediatamente y lo eliminará de cualquier dispositivo y / o software en el que se ha instalado.

3.4 Identificación y autenticación de Solicitudes de Revocación

Un Suscriptor puede solicitar la revocación de su Certificado en cualquier momento siempre que la CA pueda validar que el Suscriptor es la persona, organización o entidad a la que se emitió el Certificado. La CA autenticará la Solicitud del Suscriptor para la Revocación de su Certificado mediante la autenticación del Suscriptor o la confirmación de la autorización del Suscriptor a través de un Método Confiable de Comunicación. Tras la recepción y confirmación de tales informaciones, la CA procesará la Solicitud de Revocación como se estipula en §4.9.

Una Empresa RA puede usar la autenticación de factores múltiples para solicitar la Revocación de un Certificado.

4. Requisitos operacionales del ciclo de vida del Certificado

4.1 Solicitud de Certificado

Para obtener un Certificado, el Solicitante debe:

(i) generar un Par de Claves seguro y criptográficamente sólido, si no es generado por una CA

(ii) aceptar todos los términos y condiciones de la CPS y el Acuerdo de Suscriptor, y

(iii)completar y enviar una Solicitud de Certificado, proporcionando toda la información solicitada por una RA sin errores, falsa representación u omisiones.

Si el Solicitante no es el mismo que el Sujeto del Certificado solicitado por el Solicitante, entonces el Solicitante y el Sujeto deben aceptar todos los términos y condiciones de la CPS y el Sujeto debe aceptar todos los términos y condiciones aplicables del Acuerdo de Suscriptor.

Para evitar conflictos de intereses, el Suscriptor y Entrust serán entidades separadas. La única excepción es el caso en que Entrust ejecuta todas o parte de las tareas de RA cuando suscribe un Certificado para sí misma o para personas identificadas en asociación con Entrust como el Sujeto.

Una vez que el Solicitante complete la Solicitud de Certificado y acepte los términos y condiciones de esta CPS y el Acuerdo de Suscriptor, la RA deberá seguir los procedimientos descritos en §3.2 para realizar la verificación de la información contenida en la Solicitud del Certificado. Si la verificación realizada por la RA tiene éxito, la RA puede, a su sola discreción, solicitar la emisión para el Solicitante de un Certificado de una CA.

<u>QWAC de tipo eIDAS y QWAC de tipo PSD2</u>

(iv) Solicitante de Certificado: la solicitud de Certificado debe estar firmada y enviada por un Solicitante de Certificado autorizado.

(v) Aprobador de Certificados: la solicitud de Certificado debe ser revisada y aprobada por un Aprobador de Certificados autorizado.

(vi) Firmante del Contrato: un Acuerdo de Suscriptor aplicable al Certificado solicitado debe ser firmado por un Firmante de Contrato autorizado.

El Solicitante puede autorizar a una persona para que cumpla una, dos o las tres funciones. Un Solicitante puede también autorizar a más de una persona para cumplir cada uno de estos roles.

4.1.1 Quién puede presentar una Solicitud de Certificado

El Solicitante o una persona autorizada para solicitar Certificados en nombre del Solicitante puede presentar Solicitudes de Certificado. Los Solicitantes son

responsables de cualquier dato que el Solicitante o un agente del Solicitante suministre a la RA.

Las CA deben identificar las solicitudes de Certificados sospechosas posteriores de acuerdo con el proceso de alto riesgo de §4.2.1.3.

Las CA no emiten Certificados a ninguna persona o entidad que aparezca en una lista denegada mantenida por el gobierno de España o Canadá o que se encuentre en un país con el cual las leyes de España o de Canadá prohíben hacer negocios.

4.1.2 Proceso de inscripción y responsabilidades

Las CA requieren que cada Solicitante envíe una solicitud de Certificado e información de la solicitud antes de emitir un Certificado. Las CA o RA autentican todas las comunicaciones de un solicitante y protegen la comunicación contra modificaciones.

Los Solicitantes solicitan un Certificado completando los formularios de solicitud en línea. Los Solicitantes son únicamente
responsable de enviar una solicitud de Certificado completa y precisa para cada Certificado.

El proceso de inscripción incluye:
(i) Aceptar el Acuerdo de Suscriptor aplicable
(ii) Pagar las tarifas aplicables,
(iii) Presentar una solicitud de Certificado completa,
(iv) Generar un Par de Claves, y
(v) Entregar la Clave Pública del Par de Claves a la CA.

El Acuerdo de Suscriptor puede firmarse según cualquiera de los dos métodos siguientes:

(vi) Si el Acuerdo de Suscriptor es en formato electrónico, se firmará con un proceso de clic en línea.

(vii) Como alternativa, los Suscriptores pueden imprimir y firmar una página de firma refiriéndose al Acuerdo de Suscriptor, y enviar por correo electrónico o cargar el documento firmado a Entrust.

Al ejecutar el Acuerdo de Suscriptor, los Suscriptores garantizan que toda la información contenida en la solicitud de Certificado es correcta.

4.2 Procesamiento de solicitud de Certificado

4.2.1 Realización de funciones de identificación y autenticación

La CA seguirá un procedimiento documentado para verificar todos los datos solicitados para su inclusión en el Certificado. En los casos en que la solicitud de Certificado no contenga toda la información necesaria sobre el Solicitante, la CA obtendrá la información restante de una fuente de datos de terceros independiente y confiable.

QWAC de tipo eIDAS y QWAC de tipo PSD2
La información del Solicitante incluirá al menos un FQDN.

4.2.1.1 Comunicación del solicitante

QWAC de tipo eIDAS y QWAC de tipo PSD2
La CA utiliza un Método Verificado de Comunicación para verificar la autenticidad de la solicitud de certificado del representante del solicitante. La CA utiliza las siguientes fuentes para verificar el Método Verificado de Comunicación:

(i) Verificar que el Método Verificado de Comunicación pertenezca al Solicitante, o a una Matriz/Subsidiaria o Afiliada del Solicitante, comparándolo con uno de los Lugares de negocio de la Matriz/Subsidiaria o Afiliada del Solicitante en los registros provistos por la correspondiente compañía telefónica, un QGIS, un QTIS, un QIIS o una Carta Profesional Verificada; y

(ii) Confirmar el Método Verificado de Comunicación usándolo para obtener una respuesta afirmativa suficiente para permitir que una persona razonable concluya que el Solicitante, o una Matriz/Subsidiaria o Afiliada del Solicitante, puede ser contactada de manera confiable utilizando el Método Verificado de Comunicación .

4.2.1.2 Reutilización de información validada

Las CA y las RA pueden usar los documentos y datos proporcionados en §3.2 para verificar la información del Certificado.

QWAC de tipo eIDAS y QWAC de tipo PSD2
Exceptuando los atributos específicos de PSD2, se pueden reutilizar los datos de validación anteriores o la documentación obtenida de una fuente especificada en §3.2 no más de 13 meses después de la validación de dichos datos o documentos.

Certificados de tipo PSD2
Los atributos específicos de PSD2 solo se utilizarán durante 30 días después de que se complete la validación.

4.2.1.3 Solicitudes de certificados de alto riesgo

Las CA mantienen procedimientos para identificar solicitudes de Certificados de alto riesgo que requieren verificación adicional previa a la emisión del Certificado. Los procedimientos de certificación de alto riesgo incluyen procesos para verificar Nombres de Dominio de alto riesgo y / o evaluar Nombres de Dominio engañosos.

4.2.2 Aprobación o rechazo de Solicitudes de Certificado

La CA rechaza cualquier solicitud de Certificado que no pueda ser verificada. La CA también puede rechazar una solicitud de Certificado si cree que la emisión del Certificado podría dañar o disminuir la reputación o el negocio de la CA, incluido el negocio de Entrust.

QWAC de tipo eIDAS y QWAC de tipo PSD2

Las CA no emiten certificados que contengan nombres internos o Direcciones IP Reservadas.

La aprobación de la emisión del Certificado requiere la autenticación de dos Especialistas en Validación independientes. El segundo Especialista en Validación no puede ser la misma persona que recopiló la documentación de autenticación y aprobó originalmente la solicitud del Certificado. El segundo Especialista en Validación revisa la información y los documentos recopilados en busca de discrepancias o detalles que requieran una explicación más detallada. Si el segundo Especialista en Validación tiene alguna inquietud sobre la Solicitud, el segundo Especialista en Validación puede requerir explicaciones y documentos adicionales. Si no se reciben explicaciones satisfactorias y/o documentos adicionales dentro de un tiempo razonable, la CA o RA puede rechazar la solicitud de Certificado y notificar al Solicitante en consecuencia.

Si parte o la totalidad de la documentación utilizada para respaldar la solicitud está en un idioma que no sea el inglés, un empleado o agente de CA o RA con conocimientos en dicho idioma y que tenga la capacitación, la experiencia y el juicio adecuados para confirmar la identificación y autorización de la organización realiza la correlación cruzada final y la diligencia debida.

Si la solicitud de Certificado no se rechaza y se valida con éxito de acuerdo con esta CPS, la CA aprobará la solicitud de Certificado y emitirá el Certificado. El Suscriptor puede solicitar Certificados adicionales que contengan la misma información del Certificado validado a través de una comunicación confirmada y emitirse sin más autenticación durante el período permitido antes de que se requiera la reautenticación de la información del Certificado. La CA no es responsable de ninguna solicitud de Certificado rechazada y no está obligada a revelar los motivos del rechazo. Los Solicitantes rechazados pueden volver a realizar una solicitud. Los Suscriptores deben verificar la precisión de los datos enumerados en el Certificado antes de utilizar el Certificado.

4.2.3 Tiempo para procesar las Solicitudes de Certificado

No está estipulado.

4.2.4 Registros de Autorización de Autoridad de Certificación (CAA)

Antes de emitir QWAC de tipo eIDAS o QWAC de tipo PSD2, la CA verificará la autorización de la autoridad de certificación (CAA) para cada dNSName en la extensión subjectAltName del Certificado a emitir, de acuerdo con el procedimiento de RFC 8659, siguiendo las instrucciones establecidas en RFC 8659 para cualquier registro encontrado. Si el Certificado Cualificado de Autenticación de Sitio Web o el Certificado Cualificado de Autenticación de Sitio Web de tipo PSD2 es emitido, se emitirá dentro del tiempo de vida del registro CAA, o de 8 horas, lo que sea mayor.

Al procesar registros CAA, las CA procesan las etiquetas de propiedad como se especifica en RFC 8659. La CA no actúa sobre el contenido de la etiqueta de propiedad iodef. Las CA respetan el marcador de criticidad y no emitirán un Certificado si encuentran una propiedad no reconocida con este marcador.

Las CA pueden no verificar los registros de CAA en los siguientes casos excepcionales:

(i) Para Certificados para los cuales se creó y registró un certificado previo de Transparencia del Certificado en al menos dos registros públicos, y para los cuales se verificó la CAA.
(ii) Para los Certificados emitidos por un Certificado de CA Subordinada técnicamente restringido, según lo establecido en la sección 7.1.5 de los Requisitos de Referencia, donde la falta de verificación de la CAA es una disposición contractual explícita en el contrato con el Solicitante.

La CA trata un error de búsqueda de registros como permiso para emitir si:
(iv) El fallo está fuera de la infraestructura de la CA; y
(v) La búsqueda se ha vuelto a intentar al menos una vez; y
(vi) La zona del dominio no tiene una cadena de validación DNSSEC a la raíz de la ICANN.

La CA documenta las emisiones potenciales que fueron evitadas por un registro de la CAA con suficiente detalle para proporcionar retroalimentación al CAB Forum sobre las circunstancias, y enviará informes de dichas solicitudes de emisión al contacto o contactos estipulados en los registros de iodef de CAA, si están presentes. Las CA soportan esquemas de URL mailto: y https: en el registro iodef.

El dominio de identificación CAA de Entrust es ' **entrust.net** '.

4.3 Emisión del Certificado

Después de realizar la verificación de la información proporcionada por un Solicitante con una Solicitud de Certificado, una RA que opera bajo una CA puede solicitar que una CA emita un Certificado. Al recibir una solicitud de una RA que opera bajo una CA, la CA puede generar y firmar digitalmente un Certificado de

acuerdo con el perfil de Certificado descrito en §7. Una Empresa RA puede aprobar la emisión de Certificados y enviar la solicitud de certificado a una RA.

4.3.1 Acciones de CA durante la emisión del Certificado

La emisión del Certificado por la CA Raíz requiere que una persona autorizada por la CA (es decir, el operador o director del sistema CA o el administrador de PKI) emita conscientemente un comando directo por el que la CA Raíz realiza una operación de firma de Certificado.

La CA no emitirá Certificados con período de vigencia superior al período de vigencia del correspondiente Certificado de CA Emisora. La CA no antedatará la fecha notBefore de un Certificado de Suscriptor.

Si un tribunal u organismo gubernamental con jurisdicción sobre las actividades cubiertas por un documento de requisitos de CA/Browser Forum determina que el cumplimiento de cualquier requisito obligatorio es ilegal, entonces dicho requisito se considera reformado en la medida mínima necesaria para que el requisito sea válido y legal. La CA notificará al CA/Browser Forum los hechos, circunstancias y leyes involucradas.

QWAC de tipo eIDAS y QWAC de tipo PSD2

Las solicitudes de eIDAS QWAC y PSD2 QWAC se revisan utilizando un software de linting previo a la emisión para monitorear el cumplimiento de esta CPS, los Requisitos de Referencia y las Guías EV SSL limitado a la cobertura de linter.

4.3.2 Notificación al Suscriptor por parte de la CA de la emisión del Certificado

Una vez que un Certificado se ha generado y colocado en un Repositorio, la RA que solicitó la emisión del Certificado realiza esfuerzos comercialmente razonables para notificar al Solicitante por correo electrónico que el Certificado está disponible. El correo electrónico puede contener un URL mediante el cual el Solicitante pueda obtener el Certificado.

4.4 Aceptación del Certificado

4.4.1 Conducta constitutiva de aceptación de Certificado

No está estipulado.

4.4.2 Publicación del Certificado por la CA

No está estipulado.

4.4.3 Notificación de la emisión de Certificados por parte de la CA a otras entidades

Certificados de CA Subordinada

Los Certificados de CA Subordinada se publican en la CCADB dentro de la semana siguiente a la emisión del Certificado.

QWAC de tipo eIDAS y QWAC de tipo PSD2
Los QWAC de tipo eIDAS y QWAC de tipo PSD2 incluirán dos o más sellados de tiempo de certificado firmados (SCT) de registros independientes de Transparencia de Certificados aprobados por un ASV.

Certificados de tipo PSD2
Si la NCA proporciona una dirección de correo electrónico donde la CA pueda informar a la NCA identificada en un Certificado recién emitido, la CA enviará a esa dirección de correo electrónico información sobre el contenido del Certificado en texto sin formato, incluido el número de serie del Certificado en hexadecimal, el nombre distinguido del sujeto, el nombre distinguido del emisor, el período de validez del Certificado, así como información de contacto e instrucciones para las solicitudes de revocación y una copia del archivo del Certificado.

4.5 Uso de Par de Claves y Certificado

4.5.1 Clave Privada del Suscriptor y uso del Certificado

El Suscriptor se ajustará a §9.6.3.

Módulo criptográfico administrado y alojado
En el caso de que se utilice un módulo criptográfico administrado y alojado en una CA, se requiere que el Certificado sea válido para permitir que el Sujeto active la Clave Privada asociada.

4.5.2 Clave Pública de la Parte que Confía y uso del Certificado

Las Partes que Confían se ajustarán a §9.6.4.

4.6 Renovación de Certificado

4.6.1 Circunstancia para la renovación del certificado

De acuerdo con el Acuerdo de Suscriptor, las CA o RA proporcionarán un servicio de monitorización del ciclo de vida del Certificado que incluirá la renovación del Certificado.

4.6.2 Quién puede solicitar la Renovación

Los Suscriptores o los agentes del Suscriptor pueden solicitar la renovación de los Certificados.

4.6.3 Procesamiento de solicitudes de renovación de Certificados

Las CA o RA procesarán las solicitudes de renovación de Certificado con datos de verificación validados. Los datos de verificación anteriores se pueden usar como se especifica en §4.2.1.2.

Los Certificados se pueden renovar utilizando la Clave Pública aceptada anteriormente si dicha Clave Pública cumple con el requisito de tamaño de la clave de §6.1.5. La Clave Pública no se puede reutilizar si otro Certificado con la misma Clave Pública ha sido revocado debido al Compromiso de la Clave.

4.6.4 Notificación de nueva emisión de Certificado al Suscriptor
Las CA o RA proporcionarán una notificación de renovación del Certificado al Suscriptor o a los agentes del Suscriptor a través de un enlace a Internet o por correo electrónico.

Los Suscriptores o los agentes del Suscriptor pueden solicitar que, al vencimiento de sus Certificados, los avisos de renovación de correo electrónico no se envíen.

4.6.5 Conducta que constituye la aceptación de un Certificado de renovación
No está estipulado.

4.6.6 Publicación del Certificado de Renovación por la CA
Las CA o RA proporcionarán un Certificado al Suscriptor a través de un enlace de Internet.

4.6.7 Notificación de la emisión de Certificados por parte de la CA a otras entidades
No está estipulado.

4.7 Cambio de clave de Certificado
4.7.1 Circunstancia para el cambio de clave del Certificado
No está estipulado.

4.7.2 Quién puede solicitar la certificación de una nueva Clave Pública
No está estipulado.

4.7.3 Procesamiento de solicitudes de cambio de clave de Certificados
No está estipulado.

4.7.4 Notificación de nueva emisión de Certificado al Suscriptor
No está estipulado.

4.7.5 Conducta que constituye la aceptación de un Certificado con cambio de clave
No está estipulado.

4.7.6 Publicación por la CA del Certificado con cambio de clave
No está estipulado.

4.7.7 Notificación de la emisión de Certificados por parte de la CA a otras entidades
No está estipulado.

4.8 Modificación del Certificado
4.8.1 Circunstancia para la modificación del Certificado
No está estipulado.

4.8.2 Quién puede solicitar la modificación del Certificado
No está estipulado.

4.8.3 Procesamiento de solicitudes de modificación de Certificados
No está estipulado.

4.8.4 Notificación de nueva emisión de Certificado al Suscriptor
No está estipulado.

4.8.5 Conducta constitutiva de aceptación del Certificado modificado
No está estipulado.

4.8.6 Publicación del Certificado Modificado por la CA
No está estipulado.

4.8.7 Notificación de la emisión de Certificados por parte de la CA a otras entidades
No está estipulado.

4.9 Revocación y Suspensión de Certificados
La CA revocará un Certificado después de recibir una solicitud de revocación válida de una RA que opere bajo esta CA. Una RA que opera bajo una CA tendrá derecho a solicitar y puede solicitar que una CA revoque un Certificado después de que dicha RA reciba una solicitud de revocación válida del Suscriptor para dicho Certificado. Una RA que opera bajo una CA tendrá derecho a solicitar y solicitará que una CA revoque un Certificado si dicha RA tiene constancia de la ocurrencia de cualquier evento que requiera que un Suscriptor deje de usar dicho Certificado.

Las CA no admiten la suspensión de Certificados.

4.9.1 Circunstancias para la revocación
4.9.1.1 Razones para revocar un Certificado de Suscriptor
La CA tendrá derecho a revocar y podrá revocar, y una RA que funcione bajo una CA tendrá derecho a solicitar la revocación de un Certificado de Suscriptor, si la CA o la RA tiene conocimiento o una base razonable para creer que cualquiera de los eventos enumerados en esta sección ha ocurrido.

La CA revocará un Certificado dentro de las 24 horas y usará el correspondiente reasonCode si ocurre una o más de las siguientes situaciones:

(i) El Suscriptor solicita por escrito, sin especificar un reasonCode, que la CA revoque el Certificado;

(ii) El Suscriptor notifica a la CA que la solicitud de Certificado original no fue autorizada y no otorga retroactivamente la autorización (privilegeWithdrawn (9) reasonCode);

(iii) La CA obtiene evidencia de que la Clave Privada del Suscriptor correspondiente a la Clave Pública del Certificado ha resultado comprometida (keyCompromise (1) reasonCode);

(iv) La CA tiene conocimiento de un método demostrado o comprobado que puede calcular fácilmente la Clave Privada del Suscriptor en función de la Clave Pública del Certificado (como una clave débil de Debian, consulte https://wiki.debian.org/SSLkeys) (keyCompromise (1) reasonCode); o

(v) La CA obtiene evidencia de que no se puede confiar en la validación de la autorización o control del dominio para cualquier FQDN o Dirección IP del Certificado (superseded (4) reasonCode).

La CA debería revocar un Certificado dentro de las 24 horas y debe revocar un Certificado dentro de los 5 días posteriores al acaecimiento de uno o más de los siguientes puntos:

(vi) El Certificado ya no cumple con los requisitos de las Secciones 6.1.5 y 6.1.6 (superseded (4) reasonCode);

(vii) La CA tiene constancia de que el Certificado fue mal utilizado (privilegeWithdrawn (9) reasonCode);

(viii) La CA tiene conocimiento de que un Suscriptor ha violado una o más de sus obligaciones materiales bajo el Acuerdo de Suscriptor (privilegeWithdrawn (9) reasonCode);

(ix) La CA tiene conocimiento de cualquier circunstancia que indique que el uso de un FQDN o de una Dirección IP del Certificado ya no está legalmente permitido (por ejemplo, un tribunal o un árbitro ha revocado el derecho del Propietario de un Nombre de Dominio de utilizar el Nombre de Dominio, un acuerdo de licencia o acuerdo de servicio relevante entre el Propietario de Nombre de Dominio y el Solicitante ha finalizado, o el Propietario de Nombre de Dominio no ha podido renovar el Nombre de Dominio) (cessationOfOperation (5) reasonCode);

(x) La CA tiene conocimiento de un cambio sustancial en la información contenida en el Certificado (privilegeWithdrawn (9) reasonCode);

(xi) La CA tiene conocimiento de que el Certificado no se emitió de acuerdo con esta CPS (superseded (4) reasonCode);

(xii) La CA determina que cualquier información que aparece en el Certificado es inexacta (privilegeWithdrawn (9) reasonCode);

(xiii) El derecho de la CA a emitir Certificados bajo esta CPS expira o se revoca o termina, a menos que la CA se haya preparado para continuar manteniendo el Repositorio de CRL / OCSP (no reasonCode en CRL);
(xiv) La revocación es requerida por cualquier otra sección en esta CPS por una razón que no se requiere especificar de otro modo en este §4.9.1.1 (no reasonCode en CRL);
(xv) La CA tiene conocimiento de un método demostrado o comprobado que compromete la Clave Privada del Suscriptor, o hay evidencia clara de que el método específico utilizado para generar la Clave Privada fue defectuoso (keyCompromise (1) reasonCode);
(xvi) El contenido o formato técnico del Certificado presenta un riesgo inaceptable para los ASV o Partes que Confían (no reasonCode en CRL);
(xvii) Un Certificado se utiliza para firmar digitalmente código sospechoso (keyCompromise (1) reasonCode); o
(xviii) Cualquier otra razón que plausiblemente pueda afectar la integridad, seguridad o fiabilidad de un Certificado o CA (no reasonCode en CRL).

4.9.1.2 Razones para revocar un Certificado de una CA Subordinada

La CA emisora revocará un Certificado de una CA Subordinada dentro de los siete (7) días siguientes al acaecimiento de uno o más de los siguientes puntos:
(i) La CA Subordinada solicita la revocación por escrito;
(ii) La CA Subordinada notifica a la CA Emisora que la solicitud de Certificado original no fue autorizada y no otorga retroactivamente la autorización;
(iii) La CA Emisora obtiene evidencia de que la Clave Privada de la CA Subordinada correspondiente a la Clave Pública del Certificado ha resultado comprometida o ya no cumple con los requisitos de §6.1.5 y §6.1.6,
(iv) La CA Emisora obtiene evidencia de que el Certificado fue mal utilizado;
(v) La CA Emisora tiene conocimiento de que el Certificado no se emitió de conformidad con los Requisitos de Referencia o de que la CA Subordinada no ha cumplido con los mismos, las Guías EV SSL, el requisito mínimo para la firma del código o esta CPS;
(vi) La CA Emisora determina que la información que aparece en el Certificado es inexacta o engañosa;
(vii) La CA Emisora o la CA Subordinada cesa las operaciones por cualquier motivo y no se ha preparado para que otra CA facilite la revocación del Certificado;
(viii) El derecho de CA Emisora o la CA Subordinada a emitir Certificados bajo los Requisitos de Referencia caduca o se revoca o termina, a menos que la CA Emisora se haya preparado para continuar manteniendo el Repositorio CRL / OCSP; o
(ix) La revocación es requerida por la CPS de la CA Emisora.

4.9.2 Quién puede solicitar la revocación

Las CA, las RA y los Suscriptores pueden iniciar la revocación.

Un Suscriptor u otra parte debidamente autorizada (como un contacto administrativo, un Firmante de Contrato, el Aprobador de Certificados, o el Solicitante de Certificados) puede solicitar la revocación de su Certificado en cualquier momento por cualquier razón. Si un Suscriptor solicita la revocación de su Certificado, el Suscriptor debe poder validarse, como se establece en §3.4, frente a la RA que procesó la Solicitud de Certificado del Suscriptor. No se requerirá a las CA que revoquen y no se requerirá que las RA que operan bajo las CA soliciten la revocación de un Certificado hasta que un Suscriptor pueda validarse adecuadamente como se establece en §4.9.3. Una CA tendrá derecho a revocar y revocará, y una RA que opera bajo una CA tendrá derecho a solicitar y solicitará la revocación de un Certificado de Suscriptor en cualquier momento por cualquiera de los motivos establecidos en §4.9.1.

Los Suscriptores, las Partes que Confían, los ASV, las organizaciones de antimalware y otros terceros pueden enviar los CPRs informando a la CA de una causa razonable para revocar el Certificado.

4.9.3 Procedimiento de solicitud de revocación

Un Suscriptor solicitará la revocación de su Certificado si el Suscriptor sospecha o tiene conocimiento o una base razonable para creer que cualquiera de los siguientes eventos ha ocurrido:

(i) La Clave Privada del Suscriptor ha resultado comprometida;
(ii) El conocimiento de que la solicitud del Certificado original no fue autorizada y dicha autorización no será otorgada retroactivamente;
(iii) Cambio en la información contenida en el Certificado del Suscriptor;
(iv) Cambio en las circunstancias que causan que la información contenida en el Certificado del Suscriptor se vuelva inexacta, incompleta o engañosa

Una solicitud del Suscriptor para la revocación de su Certificado puede verificarse mediante (i) Credenciales de autenticación del Suscriptor, o (ii) autorización del Suscriptor a través de un Método Confiable de Comunicación.

Si se revoca el certificado de un Suscriptor por algún motivo, se notificará al Suscriptor mediante el envío de un correo electrónico a los contactos técnicos y de seguridad listados en la Solicitud de Certificado. La revocación de un Certificado no afectará a ninguna de las obligaciones contractuales del Suscriptor en virtud de esta CPS, el Acuerdo de Suscriptor del Suscriptor o cualquier Acuerdo de Parte que Confía.

Los Suscriptores, las Partes que Confían, los ASV, las organizaciones de antimalware y otros terceros pueden enviar un CPR mediante la información de contacto especificada en §1.5.2. Si se recibe un CPR, la CA deberá:

(v) Registrar el CPR como alta gravedad en un sistema de seguimiento para tal fin;
(vi) Revisar el CPR e involucrar a las partes necesarias para verificarlo, redactar un informe de investigación de CPR y proporcionar este informe al Suscriptor y la parte que proporcionó el CPR dentro de las 24 horas posteriores a la recepción del CPR;
(vii) Determinar si hubo una emisión errónea del Certificado. En el caso de emisión errónea del Certificado, 1) el incidente debe ser escalado al equipo de Autoridad en Materia de Políticas y a la administración del servicio y 2) un informe de emisión incorrecta del Certificado debe publicarse dentro del siguiente día hábil;
(viii) Si se requiere la revocación del Certificado, se realizará de acuerdo con los requisitos de §4.9.1.1;
(ix) Actualizar el informe de emisión incorrecta del certificado dentro de los 5 días posteriores a la recepción del CPR; y
(x) Completar el informe de investigación del CPR cuando se cierre el incidente y entregarlo al Suscriptor y la parte que proporcionó el CPR.

Certificados de tipo PSD2
Las disposiciones adicionales relativas a la revocación de los Certificados de tipo PSD2 se abordan en §4.9.17.

4.9.4 Período de gracia de solicitud de revocación
En el caso de que la Clave Privada resulte comprometida, o se sospeche que pueda ser este el caso, el Suscriptor deberá solicitar la revocación del Certificado correspondiente inmediatamente después de la detección del Compromiso o supuesto Compromiso. Las solicitudes de revocación por otras razones se harán tan pronto como sea razonablemente posible.

4.9.5 Tiempo dentro del cual la CA debe procesar la solicitud de revocación
Dentro de las 24 horas posteriores a la recepción de un CPR, la CA investigará los hechos y circunstancias relacionadas con el CPR y proporcionará un informe preliminar tanto al Suscriptor como a la entidad que presentó el CPR.

Después de revisar los hechos y circunstancias, la CA trabajará con el Suscriptor y cualquier entidad que haya informado acerca del CPR u otro aviso relacionado con la revocación para establecer si el Certificado será revocado, y si es así, una fecha en la que la CA revocará el Certificado. El plazo desde la recepción del CPR o la notificación relacionada con la revocación hasta la publicación de la revocación no superará el período de tiempo establecido en §4.9.1.1. La fecha seleccionada por la CA tendrá en cuenta los siguientes criterios:

(i) La naturaleza del problema alegado (alcance, contexto, gravedad, magnitud, riesgo de daño);
(ii) Las consecuencias de la revocación (impactos directos y colaterales para los Suscriptores y Partes que Confían);
(iii) La cantidad de CPRs recibidos sobre un Certificado o Suscriptor en particular;
(iv) La entidad que presenta la queja (por ejemplo, una queja de un agente de la ley sobre un sitio web dedicado a actividades ilegales debería tener más peso que una queja de un consumidor alegando que no recibió los bienes que pidió); y
(v) La legislación aplicable.

El tiempo máximo entre la confirmación de la revocación de un Certificado para que entre en vigencia y el cambio real de la información de estado del Certificado en los servicios de revocación de Entrust será de 60 minutos como máximo. Entrust sincroniza la hora de su sistema al menos cada 24 horas utilizando un valor en tiempo real distribuido por un laboratorio UTC (k) reconocido o el Instituto Nacional de Medición.

4.9.6 Requisito de verificación de revocación para las Partes que Confían

La Parte que Confía debe comprobar si el Certificado en el que la Parte que Confía desea confiar ha sido revocado. La Parte que Confía verificará las Listas de Revocación de Certificados mantenidas en el Repositorio apropiado o realizará una verificación de estado de revocación en línea utilizando el OCSP para determinar si el Certificado en el que la Parte que Confía desea confiar ha sido revocado. En ningún caso, Entrust Group será responsable de ningún daño o perjuicio debido a (i) la falta de verificación de la Parte que Confía de la revocación o vencimiento de un Certificado, o (ii) la confianza de una Parte que Confía en un Certificado que ha sido revocado o que ha caducado.

4.9.7 CRL Frecuencia de emisión

Las CA emiten las CRL de la siguiente manera:

(i) Las CRLs para los Certificados emitidos a las CA Subordinadas se emiten al menos una vez cada doce meses o dentro de las 24 horas posteriores a la revocación de un Certificado de CA Subordinada. El intervalo de validez de la CRL no es mayor de doce meses desde la última actualización.
(ii) Las CRLs para los Certificados se emitirán dentro de los 60 minutos posteriores a la revocación de un Certificado, y al menos una vez cada 24 horas. La nextUpdate se produce no más de 24 horas después de la última actualización. El intervalo de validez de la CRL no es mayor de 10 días.
(iii) En caso de terminación de una CA subordinada, la última CRL se emitirá en el mismo cronograma y con nextUpdate igual que las CRL anteriores. El certificado de CA subordinada se revocará, por lo que ya no se confiará en todas las CRL que no hayan vencido.

(iv) La información del estado de revocación de un Certificado estará disponible más allá del período de validez del Certificado. Los Certificados revocados no se eliminarán de la CRL una vez que hayan expirado y la CRL incluirá la extensión X.509 "ExpiredCertsOnCRL".
(v) Los servicios de CRL y OCSP serán coherentes a lo largo del tiempo teniendo en cuenta diferentes demoras en la actualización de la información de estado para ambos métodos. La información del estado de revocación estará disponible pública e internacionalmente.

4.9.8 Latencia máxima para CRLs
No está estipulado.

4.9.9 Revocación en línea / disponibilidad de verificación de estado
La revocación en línea / verificación del estado de los Certificados está disponible de forma permanente mediante CRL o mediante el Protocolo en línea de Estado de Certificado (OCSP).

Las respuestas de OCSP están firmadas por la CA o un respondedor de OCSP cuyo Certificado está firmado por la CA que emitió el Certificado cuyo estado de revocación está siendo verificado. El certificado de firma OCSP contiene una extensión de tipo id-pkix-ocsp-nocheck, como se define en la RFC6960.

4.9.10 Requisitos de verificación de revocación en línea
Las CA admiten una capacidad de OCSP que utiliza los métodos GET tal como se describe en la RFC6960 para Certificados emitidos de acuerdo con esta CPS.

Las CA firman y ponen a disposición el OCSP de la siguiente manera:
(i) Las respuestas de OCSP para los Certificados emitidos a las CA Subordinadas se emiten al menos una vez cada doce meses o dentro de las 24 horas posteriores a la revocación de un Certificado de CA Subordinada. Las respuestas de OCSP tienen un intervalo de validez no mayor de 367 días.
(ii) Las respuestas de OCSP para precertificates [RFC 6962] y Certificados de Suscriptor se emitirán dentro de los 60 minutos posteriores a la revocación de un Certificado, y al menos una vez cada 24 horas. Las respuestas de OCSP tendrán un intervalo de validez mayor de 8 horas y no mayor de 10 días.

Nota: el intervalo de validez de una respuesta OCSP es la diferencia de tiempo entre el campo thisUpdate y nextUpdate, inclusive. Para efectos del cómputo de diferencias, una diferencia de 3.600 segundos será igual a una hora, y una diferencia de 86.400 segundos será igual a un día, ignorando los segundos bisiestos.

Un número de serie de certificado dentro de una solicitud OCSP se "asigna" con un Certificado o se "reserva" con un precertificado. Si no está "asignado" o "reservado",

entonces el número de serie está "sin usar". Si el respondedor de OCSP recibe una solicitud de estado de un número de serie de Certificado que no se ha usado, entonces el respondedor no responderá con un estado "bueno".

Las ubicaciones en línea de la CRL y la respuesta de OCSP se incluyen en el Certificado para respaldar las Aplicaciones de software que realizan la comprobación automática del estado del Certificado. Una Parte que Confía también puede comprobar el estado de revocación del Certificado directamente con el Repositorio en https://www.entrust.net/CPS.

4.9.11 Otras formas de revocación de anuncios disponibles
No está estipulado.

4.9.12 Requisitos Especiales de compromiso de cambio de clave
Si un Suscriptor sospecha o sabe que la Clave Privada correspondiente a la Clave Pública contenida en el certificado de Suscriptor ha resultado comprometida, el Suscriptor notificará inmediatamente a la RA que procesó la Solicitud de Certificado de Suscriptor, utilizando los procedimientos establecidos en §3.4, tales sospechas o Compromiso real. El Suscriptor deberá dejar de usar dicho Certificado inmediatamente y deberá eliminar dicho Certificado de cualquier dispositivo y / o software en el que se haya instalado dicho Certificado. El Suscriptor será responsable de investigar las circunstancias de tal Compromiso o presunto Compromiso y de notificar a las Partes que Confían que puedan haber sido afectadas por dicho Compromiso o sospecha de Compromiso.

Los Suscriptores, las Partes que Confían, los ASV, las organizaciones anti-malware y otros terceros pueden informar a Entrust de un Compromiso de Clave Privada mediante uno de los siguientes métodos de demostración:

(i) Presentación de un CSR firmado con un nombre común de "Prueba de compromiso clave para Entrust", o
(ii) Envío de una clave privada.

4.9.13 Circunstancias para la suspensión
El Repositorio no incluirá entradas que indiquen que un Certificado ha sido suspendido.

4.9.14 Quién puede solicitar la suspensión
No aplica.

4.9.15 Procedimiento de solicitud de suspensión
No aplica.

4.9.16 Límites del Período de Suspensión
No aplica.

4.9.17 Disposiciones adicionales para Certificados de tipo PSD2

Las siguientes disposiciones adicionales relativas a la revocación se aplicarán a los Certificados de tipo PSD2:

Las solicitudes de revocación de Certificados por parte de las NCAs pueden enviarse por correo electrónico a nca@entrust.com. Entrust verificará la autenticidad de todas las solicitudes de revocación de Certificados enviadas por las NCAs utilizando cualquiera de los siguientes métodos de autenticación de la solicitud de revocación de la NCAs, seleccionado por la NCA:

- Un secreto compartido si fue proporcionado por Entrust a la NCA para fines de revocación, o
- Una firma digital respaldada por un certificado emitido a la NCA por Entrust que cumple con una política de certificado cualificado.

Si Entrust recibe una notificación de una dirección de correo electrónico donde puede contactar con la NCA respectiva, Entrust informará a la NCA, utilizando esta dirección de correo electrónico, cómo la NCA puede autenticarse en las solicitudes de revocación.

Entrust permitirá a la NCA, como propietaria de la información específica de PSD2, solicitar la revocación del Certificado mediante el siguiente procedimiento. La NCA puede especificar una razón, que puede ser descriptiva en lugar de en un formulario estándar, para la revocación. Entrust procesará tales solicitudes y validará su autenticidad. Si no está claramente indicado o implícito por qué se solicita la revocación o si el motivo no está en el área de responsabilidad de la NCA, Entrust puede decidir no tomar medidas. Basándose en una solicitud auténtica de una NCA, Entrust revocará el Certificado de manera oportuna y, en cualquier caso, dentro de las 24 horas posteriores a la recepción de la solicitud de revocación aceptable, si se cumple alguna de las siguientes condiciones (además de cualquiera de los requisitos generales de la Sección 4.9 de esta CPS):

- La autorización del Suscriptor ha sido revocada, o
- Se revocó cualquier rol de PSP incluido en el certificado.

Si la NCA como propietaria de la información específica de PSD2 notifica a Entrust que dicha información ha cambiado, lo que puede afectar la validez del Certificado, pero sin una solicitud debidamente autenticada con una razón aceptable por la cual se debe revocar el Certificado, Entrust investigará esta notificación independientemente de su contenido y formato, y revocará los Certificados afectados si es necesario. Esta notificación no necesita ser procesada en 24 horas.

Las NCAs pueden enviar notificaciones sobre los cambios de información reguladora relevante de PSD2 de la PSP que pueden afectar la validez del certificado

a la siguiente dirección de correo electrónico: nca@entrust.com. El contenido y el formato de estas notificaciones pueden acordarse entre la NCA y Entrust. Sin embargo, Entrust investigará esta notificación independientemente de su formato. Si Entrust recibe una notificación de una dirección de correo electrónico donde puede informar a la NCA identificada en un Certificado revocado, Entrust enviará a esa dirección de correo electrónico información sobre la revocación del Certificado.

4.10 Servicios de estado del Certificado

4.10.1 Características operacionales

Las entradas de revocación en una respuesta de CRL u OCSP no se eliminan hasta después de la expiración de la CA Emisora.

4.10.2 Disponibilidad del servicio

La CA opera y mantiene su capacidad de CRL y OCSP con recursos suficientes para proporcionar un tiempo de respuesta de diez segundos o menos en condiciones normales de operación.

La CA mantiene un Repositorio en línea 24x7 que la aplicación software puede usar para verificar automáticamente el estado actual de todos los Certificados no caducados emitidos por la CA.

La CA mantiene una capacidad continua de 24x7 para responder internamente a un CPR de alta prioridad. Cuando sea apropiado, la CA remite dicha queja a las autoridades policiales y / o revoca el Certificado que es objeto de tal queja.

4.10.3 Características opcionales

No está estipulado.

4.11 Fin de la Suscripción

No está estipulado.

4.12 Depósito de claves y recuperación

4.12.1 Prácticas de la política de depósito y recuperación de claves

No está estipulado.

4.12.2 Política y prácticas de encapsulación y recuperación de claves de sesión

No está estipulado.

5. Controles operativos, de instalación y gestión

Los requisitos de seguridad del sistema de certificados y redes de CA / Browser Forum están incorporados por referencia como se establece en el presente documento. Entrust retiene la responsabilidad general de cumplir con los procedimientos prescritos en su política de seguridad de la información, incluso con respecto a aquellas políticas cuya funcionalidad es realizada por subcontratistas.

5.1 Controles de seguridad físicos

5.1.1 Ubicación del sitio y construcción

Las instalaciones informáticas que albergan los servicios de CA se encuentran en Ottawa, Canadá. El equipo de CA está ubicado en una zona de seguridad que está físicamente separada de los otros sistemas de Entrust para restringir el acceso al personal con roles de confianza. La zona de seguridad está construida con privacidad y asegurada bloque a bloque con malla de alambre. La zona de seguridad está protegida por sistemas de control de acceso electrónico, puertas con alarma y es supervisada a través de una cámara de seguridad de grabación 24x7 y un sistema detector de movimiento.

5.1.2 Acceso físico

La sala que contiene el software de CA se designa como una zona de dos (2) personas, y se usan controles para prevenir que una persona esté sola en la habitación. Los sistemas de alarma se utilizan para notificar al personal de seguridad de cualquier violación de las reglas de acceso a una CA.

5.1.3 Alimentación eléctrica y aire acondicionado

La zona de seguridad está equipada con:

• Potencia filtrada, condicionada, conectada a un UPS de tamaño apropiado y a un generador;

• Calefacción, ventilación y aire acondicionado adecuados para instalaciones de procesamiento de datos comerciales; e

• Iluminación de emergencia.

Los controles ambientales se ajustan a las normas locales y se aseguran de manera adecuada para evitar el acceso no autorizado y / o la manipulación del equipo. Las alarmas y alertas de control de temperatura se activan ante la detección de condiciones de temperatura amenazantes.

5.1.4 Exposiciones al agua

Las tuberías de líquido, gas, gases de escape, etc. no atraviesan el espacio controlado más que cuando se requiere directamente para el sistema HVAC del área y para el sistema de supresión de incendios de acción previa. Las tuberías de agua para el sistema de supresión de incendios de acción previa solo se llenan con la activación de múltiples alarmas de incendio.

5.1.5 Prevención y Protección contra Incendios
La instalación de la CA está completamente cableada para la detección, alarma y extinción de incendios. Se realizan inspecciones rutinarias y frecuentes de todos los sistemas para garantizar un funcionamiento adecuado.

5.1.6 Almacén de datos
Todos los datos se almacenan lejos de fuentes de calor y de fuentes obvias de agua u otros peligros obvios.

Los medios electromagnéticos (por ejemplo, las cintas) se almacenan lejos de fuentes obvias de campos magnéticos fuertes. El material archivado se almacena en una sala separada del equipo de CA hasta que se transfiere a la instalación de almacenamiento de archivos.

Entrust emplea procedimientos de gestión de datos para proteger contra la obsolescencia y el deterioro de los datos dentro del período de tiempo que se requiere conservar los registros.

5.1.7 Eliminación de residuos
Los residuos se eliminan o destruyen de acuerdo con las mejores prácticas de la industria. Los medios utilizados para almacenar datos confidenciales se destruyen antes de su eliminación, por lo que la información no se puede recuperar.

5.1.8 Copia de seguridad fuera de las instalaciones
Como se estipula en §5.5.

5.2 Controles de procedimiento

5.2.1 Roles de confianza
Las CA tienen una serie de Roles de Confianza para las operaciones confidenciales del software de CA.

5.2.2 Número de personas requeridas por tarea
Las operaciones de CA relacionadas con el cambio de la configuración de la política de CA requieren más de una persona con un Rol de Confianza para realizar la operación.

Solo el personal con Roles de Confianza que usan control dual en un lugar físicamente seguro hace copias de seguridad de las Claves Privadas de la CA, las almacena y las recupera.

5.2.3 Identificación y autenticación de cada rol

El personal con Roles de Confianza debe someterse a un examen de antecedentes y debe estar capacitado para su rol específico.

5.2.4 Roles que requieren separación de tareas

Los roles que requieren una separación de funciones incluyen aquellos que realizan:
(i) Funciones de autorización tales como la verificación de información en las solicitudes de Certificados y aprobaciones de solicitudes de Certificados y solicitudes de revocación;
(ii) Revocación del certificado;
(iii) Funciones de copias de seguridad, grabación y mantenimiento de registros;
(iv) Funciones de auditoría, revisión, supervisión o conciliación; y
(v) Tareas relacionadas con la gestión o administración de claves de CA.

5.3 Controles de personal

Al personal operativo de una CA no se le asignarán otras responsabilidades que entren en conflicto con sus responsabilidades operacionales de la CA. Los privilegios asignados al personal operativo de una CA se ajustarán al mínimo requerido para llevar a cabo sus tareas asignadas.

5.3.1 Requisitos de calificación, experiencia y acreditaciones

Antes de la participación de cualquier persona en el proceso de gestión de Certificados, la CA o RA deberá verificar la identidad y fiabilidad de dicha persona.

5.3.2 Procedimientos de verificación de antecedentes

No está estipulado.

5.3.3 Requisitos de formación

El personal en Roles de Confianza y los Especialistas en Validación reciben capacitación en habilidades que se basa en los requisitos de la industria, incluidos los Requisitos de Referencia y las Guías EV SSL.

El Especialista en Validación realiza tareas de verificación de información y recibe formación en habilidades que cubren el conocimiento básico de PKI, las políticas y procedimientos de autenticación y verificación (incluido esta CPS) y amenazas comunes al proceso de verificación de la información (incluido el phishing y otras tácticas de ingeniería social).

Los Especialistas en Validación reciben formación en habilidades antes de comenzar su función laboral y se les exige que aprueben un examen sobre los requisitos de verificación de información aplicables.

La CA mantiene registros de dicha formación y garantiza que el personal encargado de las responsabilidades de Especialista en Validación mantenga un nivel de competencia apropiado.

5.3.4 Frecuencia de formación continua y requisitos
Las CA y las RA proporcionan una formación de actualización y actualizaciones informativas suficientes para garantizar que todo el personal con Roles de Confianza conserva el grado requerido de experiencia.

5.3.5 Frecuencia y secuencia de rotación de trabajos
No está estipulado.

5.3.6 Sanciones por acciones no autorizadas
No está estipulado.

5.3.7 Requisitos de contratación de terceros
El personal de terceros de las RA que participe en la emisión de un Certificado deberá cumplir con la formación y las habilidades de los requisitos de §5.3.3 y los requisitos de retención de documentos y registro de eventos de §5.4.1.

5.3.8 Documentación suministrada al personal
No está estipulado.

5.4 Procedimientos de registro de auditoría
Los eventos de seguridad significativos en las CA y en todas las RA que operan bajo una CA se marcan automáticamente en el tiempo y se registran como logs en los archivos de seguimiento de auditoría. Los archivos de seguimiento de auditoría se procesan (se revisan en busca de infracciones de políticas u otros eventos significativos) de forma regular. Los archivos de seguimiento de auditoría se archivan periódicamente. Todos los archivos, incluido el último archivo de seguimiento de auditoría, se transfieren a soportes de copias de seguridad y se almacenan en una instalación de archivo seguro. Entrust sincroniza la hora de su sistema al menos cada 24 horas utilizando un valor en tiempo real distribuido por un laboratorio UTC (k) reconocido o el Instituto Nacional de Medición.

5.4.1 Tipos de eventos registrados
Las CA y todas las RA que operan bajo una CA registran en detalle cada acción realizada para procesar una solicitud de Certificado y emitir un Certificado, incluida toda la información generada o recibida en relación con una Solicitud de Certificado, y cada acción tomada para procesar la Solicitud, incluidos la hora, la fecha y el personal involucrado en la acción.

Los requisitos de registro anteriores incluyen, entre otros, la obligación de registrar los siguientes eventos:
(i) Eventos clave del ciclo de vida del Certificado de CA, que incluyen:
    a. Generación de claves, copia de seguridad, almacenamiento, recuperación, archivo y destrucción;

b. Solicitudes de certificados, solicitudes de renovación y renovación de claves y revocación;
c. Aprobación y rechazo de solicitudes de Certificados;
d. Eventos del ciclo de vida de dispositivos criptográficos.
e. Generación de CRL y entradas OCSP; e
f. Introducción de nuevos perfiles de certificado y retiro de perfiles de certificado existentes.

(ii) Eventos de gestión del ciclo de vida de Certificado de Suscriptor, que incluyen:
g. Solicitudes de Certificado, solicitudes de renovación y cambio de claves, y revocación;
h. Todas las actividades de verificación requeridas por esta CPS;
i. Aprobación y rechazo de solicitudes de Certificado;
j. Emisión de Certificados; y
k. Generación de CRL y entradas OCSP.

(iii) Eventos de seguridad, incluyendo:
l. Intentos exitosos e infructuosos de acceso al sistema PKI;
m. PKI y acciones del sistema de seguridad realizadas;
n. Cambios en el perfil de seguridad;
o. Fallos del sistema, fallos de hardware y otras anomalías;
p. Actividades de cortafuegos y enrutadores; y
q. Entradas y salidas de la instalación de la CA.
r. Todas las evidencias de procesos de identificación por video incompletos que no se hayan completado debido a sospecha de fraude.

Las entradas de logs incluyen los siguientes elementos:
s. Fecha y hora de registro;
t. Identidad de la persona que realiza el registro en el diario; y
u. Descripción del registro.

5.4.2 Frecuencia de tratamiento de registros

No está estipulado.

5.4.3 Período de retención del registro de auditoría

La CA conservará durante al menos dos años:

(i) Certificado de CA y registros de eventos de gestión del ciclo de vida de la clave, como se establece en §5.4.1 (i), después de la destrucción de la clave de CA o la revocación o del vencimiento del Certificado de CA, lo que ocurra más tarde;

(ii) los registros de eventos de gestión del ciclo de vida del Certificado de Suscriptor, como se establece en la Sección §5.4.1 (ii), después de la revocación o vencimiento del Certificado de Suscriptor; y

(iii) Cualquier registro de eventos de seguridad, como se establece en §5.4.1 (iii), después de ocurrido el evento.

5.4.4 Protección de registro de auditoría
Solo los roles de confianza tienen acceso de lectura o para archivar los registros. Los registros de auditoría están protegidos contra su destrucción antes del final de su período de retención y se conservan de forma segura en el sitio hasta que se transfieren a una ubicación de almacenamiento fuera del sitio. La ubicación de almacenamiento fuera del sitio es segura y está separada de la ubicación donde se generaron los datos.

5.4.5 Procedimientos de copia de seguridad del registro de auditoría
No está estipulado.

5.4.6 Sistema de recogida de auditorías
No está estipulado.

5.4.7 Notificación al sujeto causante del evento
No está estipulado.

5.4.8 Análisis de vulnerabilidad
Las CA realizan anualmente un análisis de riesgos que:

(i) Identifica amenazas internas y externas previsibles que podrían resultar en un acceso no autorizado, divulgación, uso indebido, alteración o destrucción de los datos del Certificado o los procesos de gestión del Certificado;

(ii) Evalúa la probabilidad y el daño potencial de estas amenazas, teniendo en cuenta la sensibilidad de los datos del Certificado y procesos de gestión del Certificado; y

(iii) Evalúa la suficiencia de las políticas, procedimientos, sistemas de información, tecnología y otras disposiciones que la CA tiene para contrarrestar tales amenazas.

Sobre la base de la evaluación de riesgos se desarrolla, implementa y mantiene un plan de seguridad que consiste en procedimientos de seguridad, medidas y productos diseñados para lograr los objetivos establecidos anteriormente y para gestionar y controlar los riesgos identificados durante el análisis de riesgos. El plan de seguridad incluye protecciones administrativas, organizativas, técnicas y físicas apropiadas según la sensibilidad de los datos del Certificado y los procesos de gestión de Certificados. El plan de seguridad también tiene en cuenta la tecnología disponible en ese momento y el coste de implementar las medidas específicas, e implementa un nivel razonable de seguridad apropiado para el daño que podría resultar de una violación de la seguridad y la naturaleza de los datos a proteger.

5.5 Archivo

5.5.1 Tipos de registros archivados

Se archivan los archivos de seguimiento de auditoría, las bases de datos y la información de revocación de las CA y de las RA que operan bajo una CA.

5.5.2 Periodo de retención para archivo
La CA y las RA que operan bajo una CA retendrá toda la documentación relacionada con las solicitudes de Certificados y la verificación de los mismos, y con todos los Certificados y la revocación de los mismos, durante al menos 15 años después de que cualquier Certificado basado en esa documentación deje de ser válido. En el caso del evento contemplado en § 5.4.1 (r), la documentación se conservará por un período de 5 años a partir de la ejecución del proceso de identificación, especificando el motivo por el cual no se completó, de acuerdo con la política establecida para este propósito.

5.5.3 Protección de archivo
Las bases de datos para la CA y las RA que operan bajo una CA están protegidas mediante cifrado. Los soportes de archivos están protegidos mediante el almacenamiento en una instalación de acceso restringido a la que solo personal autorizado por Entrust tiene acceso. Se hace una copia de los archivos a medida que se crean. Los originales se almacenan en las instalaciones y se guardan con un sistema de CA. Los archivos de copia de seguridad se almacenan en una ubicación geográfica segura y separada.

5.5.4 Procedimientos de copia de seguridad de archivo
No está estipulado.

5.5.5 Requisitos para el sellado de tiempo de los registros
No está estipulado.

5.5.6 Sistema de recogida de archivos
No está estipulado.

5.5.7 Procedimientos para obtener y verificar información de archivo
No está estipulado.

5.6 Cambio de clave
Los Pares de Claves de las CA se retirarán del servicio al final de sus respectivas vidas, tal como se define en §6.3. Los nuevos Pares de Claves de la CA se crearán según sea necesario para dar continuidad a los servicios de CA. Cada CA continuará publicando las CRLs firmadas con el Par de Claves original hasta que todos los Certificados emitidos utilizando ese Par de Claves original hayan expirado. El proceso de cambio de clave de la CA se realizará de tal manera que cause una alteración mínima a los Suscriptores y Partes que Confían.

Concretamente, antes de la expiración de cualquier Certificado que se utilice para firmar claves de Sujeto (por ejemplo, según lo indicado por la expiración del Certificado), en caso de continuar con el servicio:

(i) Entrust genera un nuevo Certificado para firmar Pares de Claves de Sujeto y aplica todas las acciones necesarias para evitar la interrupción de las operaciones de cualquier entidad que pueda confiar en el Certificado;
(ii) El nuevo Certificado de CA también se genera y distribuye de acuerdo con el presente documento.

Las subsecciones (i) y (ii) se realizarán con un intervalo adecuado entre la fecha de expiración del Certificado y el último Certificado firmado para permitir que todas las partes que tengan relaciones con Entrust (Sujetos, Suscriptores, Partes que Confían, CA más altas en la jerarquía de CA, etc. .) sean conscientes de este cambio de claves e implementen las operaciones requeridas para evitar inconvenientes y fallos de funcionamiento. El período mínimo de cambio será de dos años antes de la fecha de expiración del Certificado. Esto no se aplica si Entrust deja de funcionar antes de la fecha de expiración de su propio Certificado de firma.

5.7 Compromiso y recuperación ante desastres

5.7.1 Procedimientos de manejo de incidencias y compromisos

5.7.1.1. Plan de recuperación ante desastres y continuidad del negocio

Las CA tienen un plan de respuesta a incidentes de seguridad, un plan de recuperación de desastres y un plan de continuidad de negocio para proporcionar una recuperación oportuna de los servicios en caso de incidente de seguridad, violación de la seguridad, pérdida de integridad del sistema o interrupción del sistema. Se aborda lo siguiente:

(i) Las condiciones para activar los planes;
(ii) Procedimientos de reanudación;
(iii) Calendario de mantenimiento para el plan;
(iv) Requisitos de sensibilización y educación;
(v) Las responsabilidades de los individuos;
(vi) Objetivo de punto de recuperación (RPO) de quince minutos;
(vii) Objetivo de tiempo de recuperación (RTO) de 72 horas para operaciones de CA esenciales que incluyen Revocación del Certificado y emisión del estado de revocación del Certificado; y
(viii) Pruebas de planes de recuperación.

Para mitigar las consecuencias de un desastre, las CA han implementado lo siguiente:

(ix) Almacenamiento seguro en las instalaciones y fuera de las instalaciones de los HSMs de copia de seguridad que contienen copias de todas las claves privadas de la CA

(X) Almacenamiento seguro en el sitio y fuera del sitio de todos los materiales de activación necesarios
(xi) Sincronización regular de datos críticos con el sitio de recuperación de desastres.
(xii) Copias de seguridad periódicas e incrementales de datos críticos dentro de las instalaciones primarias
(xiii) Controles ambientales como se describe en §5.1
(xiv) Arquitectura de alta disponibilidad para sistemas críticos.

Entrust ha implementado una instalación segura de recuperación de desastres que está a más de 250 km de las instalaciones primarias seguras de la CA.

5.7.1.2 Incidente de seguridad

En caso de cualquier violación de seguridad, pérdida de integridad del sistema o interrupción del sistema que tenga un impacto significativo en el servicio prestado o en los datos personales que se conservan en el mismo que afecte a los Suscriptores, ASV, Partes que Confían, otras entidades con las que Entrust tiene acuerdos u otra forma de relaciones establecidas, organismos de control y, en su caso, el organismo nacional de seguridad de la información o la autoridad de protección de datos, Entrust les informará dentro de las 24 horas posteriores a la identificación del problema enviando mensajes de correo electrónico, publicando mensajes en su sitio web describiendo la naturaleza del problema, o utilizando mecanismos de comunicación previamente establecidos por las autoridades competentes.

Si es necesario, Entrust notificará a todas las partes que los Certificados y la información del estado de revocación emitida con esta clave de CA pueden dejar de ser válidas, e incluirá una recomendación de que los Suscriptores reemplacen todos los Certificados afectados por el problema, y que todos los ASV, otras entidades con las que Entrust tiene acuerdos u otra forma de relaciones establecidas, y las Partes que Confían dejen de confiar en todos los Certificados afectados por el problema. Estas comunicaciones serán realizadas por el Equipo de Respuesta a Incidentes de Seguridad Informática establecido por el Plan de Respuesta a Incidentes de Seguridad de Entrust y de acuerdo con los procedimientos establecidos en dicho Plan, junto con la asistencia de cualquier otro personal de Entrust según lo requiera el Equipo de Respuesta a Incidentes de Seguridad Informática para enviar tales notificaciones. Después de cualquier desastre, incidente de seguridad, violación de la seguridad, pérdida de integridad del sistema o interrupción del sistema, Entrust deberá, cuando sea posible, tomar medidas para evitar la repetición del problema. Entrust revocará cualquier certificado de CA que se haya emitido para la CA que resulte comprometida cuando Entrust sea informado del compromiso de otra CA (por ejemplo, para Certificados Cruzados).

En caso de fallo del sistema, servicio u otros factores fuera del control de Entrust, se utilizarán esfuerzos comercialmente razonables para garantizar que el servicio esté disponible en un período máximo de 72 horas.

Entrust tiene políticas y procedimientos que se emplearán en caso de que se dé tal Compromiso. Como mínimo, todos los Suscriptores, ASVs y Partes que Confían serán informados tan pronto como sea posible de tal Compromiso y la información se publicará en el Repositorio. Para informar a estas partes en caso de Compromiso de la clave, Entrust enviará uno o más mensajes de correo electrónico a los Suscriptores y ASV en función de los registros de las direcciones de correo electrónico actuales y publicará uno o más mensajes para las Partes que Confían en su sitio web describiendo la naturaleza del Compromiso de la clave, declarando que los Certificados y la información del estado de revocación emitidos usando esta clave de CA pueden dejar de ser válidos, y recomendando que los Suscriptores reemplacen todos los Certificados emitidos por la CA cuya clave se vea comprometida, y que todos los ASV y las Partes que Confían dejen de confiar en todos los Certificados emitidos por la CA cuya clave se vea comprometida.

Los cambios de seguridad que podrían afectar a los suscriptores, ASV, partes que confían, organismos de evaluación y organismos supervisores / reguladores) se notificarán mediante publicación en el sitio web https://www.entrust.net/CPS. La seguridad de la información restringida solo se entregará a los organismos de evaluación en el caso de que se haya firmado previamente un documento de NDA y utilizando canales / herramientas encriptados que aseguren la confidencialidad de la información. Para distribuir la seguridad de la información restringida a los organismos supervisores / reguladores, se utilizarán para la distribución los procedimientos designados por el organismo específico para el motivo específico.

5.7.2 Alteración de los Recursos de Computación, Software y / o Datos
No está estipulado.

5.7.3 Procedimientos de Compromiso de la Clave Privada de la entidad
No está estipulado.

5.7.4 Capacidades de continuidad del negocio después de un desastre
No está estipulado

.

5.8 Cese de CA o RA
En caso de cese de la CA, Entrust:

(i) Proporcionará un aviso e información sobre el cese de la CA enviando un aviso a los Suscriptores con Certificados no vencidos, Proveedores de aplicaciones software y Partes que Confían, y mediante la publicación de dicha información en el Repositorio y mediante el envío de correos electrónicos informativos; y

(ii) Transferirá todas las responsabilidades a una entidad sucesora cualificada.

Si no existe una entidad sucesora cualificada, Entrust:

(iii) Transferirá aquellas funciones que puedan transferirse a un tercero fiable y realizará las gestiones necesarias para preservar todos los registros relevantes en un tercero fiable o una entidad gubernamental, regulatoria o legal con la autoridad apropiada;
(iv) Revocará todos los Certificados que aún no hayan sido revocados o hayan caducado en una fecha como se especifica en el aviso y publicará las CRLs finales;
(v) Destruirá todas las Claves Privadas de la CA; y
(vi) Realizará otras gestiones necesarias de acuerdo con esta CPS.

6. Controles técnicos de seguridad

6.1 Generación e instalación de Par de Claves

6.1.1 Generación de Pares de Claves

6.1.1.1 Generación del Par de Claves de CA

Las CA realizarán lo siguiente al generar un Par de Claves de CA:

(i) Prepararán y seguirán un guion de generación de Par de Claves;

(ii) Harán que un auditor cualificado sea testigo del proceso de generación de Par de Claves de CA;

(iii) Harán que un auditor cualificado emita un informe manifestando que la CA siguió la ceremonia de generación de Par de Claves de CA durante el proceso de generación de claves y los controles para garantizar la integridad y confidencialidad del Par de Claves de CA;

(iv) Generarán el Par de Claves de CA en un entorno físicamente seguro;

(v) Generarán el Par de Claves de CA utilizando personal con Roles de Confianza bajo los principios de control de varias personas y conocimiento dividido;

(vi) Generarán el Par de Claves de CA dentro de módulos criptográficos que cumplan con los requisitos aplicables de §6.2.11;

(vii) Registrarán sus actividades de generación de Par de Claves de CA; y

(viii) Mantendrán controles efectivos para proporcionar una seguridad razonable de que la Clave Privada se generó y se protegió de conformidad con los procedimientos descritos en esta CPS y (si corresponde) su guion de generación de Par de Claves de CA.

6.1.1.2 Generación de Par de Claves RA

No está estipulado.

6.1.1.3 Generación de Par de Claves de Suscriptor

El Solicitante o el Suscriptor debe generar o iniciar un Par de Claves nuevo, seguro y criptográficamente sólido para ser utilizado en asociación con el Certificado del Suscriptor o la Solicitud de Certificado del Solicitante.

Las CA rechazarán una solicitud de Certificado si se cumple una o más de las siguientes condiciones:

(i) El par de claves no cumple con los requisitos establecidos en §6.1.5 y / o §6.1.6;

(ii) Existe evidencia clara de que el método específico utilizado para generar la Clave Privada era defectuoso;

(iii) La CA tiene conocimiento de un método demostrado o comprobado que compromete la Clave Privada;

(iv) Se ha avisado previamente a la CA de que la Clave Privada ha sufrido un Compromiso de Clave, como a través de las disposiciones de la Sección 4.9.1.1;

(v) La CA tiene conocimiento de un método demostrado o probado para calcular fácilmente la Clave Privada basada en la Clave Pública (como por ejemplo una clave débil de Debian, véase https://wiki.debian.org/SSLkeys).

QWAC de tipo eIDAS y QWAC de tipo PSD2
La CA no generará un Par de Claves en nombre de un Suscriptor y no aceptará una solicitud de Certificado utilizando un Par de Claves previamente generado por la CA.

QSealC de tipo PSD2
La CA no generará un Par de Claves en nombre de un Suscriptor.

QsealC de tipo eIDAS
Los Pares de Claves de Suscriptor deben generarse de manera que se garantice que la Clave Privada no sea conocida ni accesible por nadie que no sea el Suscriptor o un representante autorizado del Suscriptor. La CA generará los Pares de Claves de Suscriptor en un módulo criptográfico seguro que cumpla o supere los requisitos definidos en §6.2.11.

QSigC de tipo eIDAS
Los pares de claves de suscriptor deben generarse de manera que se garantice que nadie que no sea el suscriptor o el representante autorizado de un suscriptor conozca ni pueda acceder a la clave privada. La CA generará los pares de claves de suscriptor en un QSCD de acuerdo con el Reglamento (UE) n.o 910/2014, que cumple o supera los requisitos definidos en §6.2.11.

Se debe monitorizar el estado del QSCD. Si hay una modificación en el estado del QSCD, como la pérdida de la certificación QCSD, entonces:

(i) Se impedirá el acceso y la activación de las Claves Privadas del Suscriptor en el QSCD afectado, y

(ii) Los Certificados Cualificados no vencidos con Claves Privadas en el QSCD afectado serán revocados.

QTSC de tipo eIDAS
Los pares de claves de QTSC de tipo eIDAS deben estar en un módulo criptográfico seguro que cumpla o supere los requisitos definidos en §6.2.11.

6.1.2 Entrega de Clave Privada al Suscriptor

Si la CA genera el Par de claves del Suscriptor, tendrá un proceso seguro para generar el Par de Claves en un dispositivo criptográfico seguro o QSCD. La CA almacenará y / o distribuirá de forma segura el dispositivo criptográfico seguro o QSCD.

Módulo criptográfico administrado y alojado

En el caso de que se utilice un dispositivo criptográfico o un QSCD administrado y alojado en una CA, la Clave Privada se generará, almacenará y administrará en un módulo criptográfico que cumpla con los requisitos definidos en §6.2.11. La CA aplica la autenticación multifactor para permitir que el Suscriptor se inscriba para generar el Par de Claves o utilizar la Clave Privada para firmar. La Clave Privada no se entrega al Suscriptor.

6.1.3 Entrega de Clave Pública al emisor del Certificado

La Clave Pública a incluir en un Certificado se entrega a la CA en una solicitud de firma de Certificado (CSR) firmada como parte del proceso de solicitud de Certificado. La firma en la CSR será verificada por la CA antes de emitir el Certificado.

6.1.4 Entrega de Claves Públicas de CA a Partes que Confían

El Certificado de Clave Pública para las CA se pone a disposición de los Suscriptores y Partes que Confían a través de la inclusión en software de terceros según lo distribuido por los fabricantes de software apropiados. El Certificado de Clave Pública para las CA Subordinadas certificadas cruzadas se proporciona al Suscriptor con el Certificado del Suscriptor.

Los Certificados de Clave Pública para las CA también están disponibles para su descarga desde el Repositorio.

6.1.5 Tamaños de clave

Para los Pares de Claves RSA, la CA se asegurará de que el tamaño del módulo, cuando se codifique, sea al menos de 2048 bits, y de que el tamaño del módulo, en bits, sea divisible por 8.

Tamaño de clave de CA
El tamaño de la clave de CA es de 2048 o 4096 bits RSA.

QWAC de tipo eIDAS y QWAC de tipo PSD2
Los tamaños de las claves de CA permitidos son 2048 y 4096 bits.

QSealC de tipo PSD2
Los tamaños de las claves de RSA permitidos son 2048, 3072 y 4096 bits.

QSealC de tipo eIDAS
Los tamaños de las claves de RSA permitidos son 2048, 3072 y 4096 bits.

QSigC de tipo eIDAS
Los tamaños de la clave RSA permitidos son 2048, 3072 y 4096 bits.

QTSC de tipo eIDAS
Los tamaños de clave RSA admitidos son de 4096 bits.

6.1.6 Generación de parámetros de Clave Pública y control de calidad

Para las Claves Públicas RSA, las CA confirman que el valor del exponente público es un número impar igual a 3 o más. Además, el exponente público debe estar en el rango entre $2^{16}+1$ y $2^{256}-1$. El módulo tendrá también las siguientes características: ser un número impar, no ser potencia de un número primo, y no tener factores menores de 752.

Si alguno de los algoritmos o parámetros asociados utilizados por la CA o sus Suscriptores se vuelven insuficientes para su uso previsto restante, la CA informará a todos los Suscriptores y Partes que Confían con quienes la CA tiene un acuerdo u otra forma de relación establecida. La CA también publicará esta información para ponerla a disposición de otras Partes que Confían. Si alguno de los algoritmos o parámetros asociados utilizados por la CA o sus Suscriptores se vuelven insuficientes para su uso previsto restante, la CA deberá programar la revocación de cualquier Certificado afectado.

Módulo criptográfico administrado y alojado
En el caso de que la CA haya generado el Par de Claves en nombre del Suscriptor, el Par de Claves se genera de acuerdo con FIPS 186.

6.1.7 Fines de uso de la clave

Las Claves Privadas de la CA raíz no se deben usar para firmar Certificados, excepto en los siguientes casos:

(i) Certificados auto-firmados para representar a la propia CA raíz;
(ii) Certificados para CA Subordinadas y Certificados Cruzados;
(iii) Certificados para fines de infraestructura (por ejemplo, ertificados de roles administrativos, certificados de dispositivos operacionales internos de la CA y Certificados de verificación de respuesta de OCSP); y
(iv) Certificados emitidos con el único fin de probar productos con Certificados emitidos por una CA Raíz.

6.2 Controles de protección de Claves Privadas y módulos criptográficos de ingeniería

Las CA han implementado medidas de seguridad físicas y lógicas para evitar la emisión no autorizada de Certificados. La protección de la Clave Privada de la CA fuera del sistema validado consiste en la seguridad física, encriptación o combinación de ambas, implementadas de una manera que impida la divulgación de la Clave Privada de la CA. La CA encripta su Clave Privada con un algoritmo y longitud de clave capaces de soportar ataques criptoanalíticos durante la vida restante de la clave encriptada.

6.2.1 Módulos criptográficos y controles

Claves Privadas de la CA

Las Claves Privadas de la CA deben almacenarse y protegerse en módulos criptográficos que cumplan o excedan los requisitos definidos en §6.2.11. Las Claves Privadas en los módulos criptográficos se guardan en instalaciones seguras bajo el control de dos personas. Las Claves Privadas de RA deben almacenarse y protegerse en módulos criptográficos que cumplan o excedan los requisitos definidos en §6.2.11.

Si la CA genera el Par de Claves en nombre del Sujeto o Suscriptor, las claves se generarán en un proceso confidencial.

QsealC de tipo eIDAS y QTSC de tipo eIDAS

Las Claves Privadas deben generarse, almacenarse y protegerse en un dispositivo criptográfico seguro que cumpla o exceda los requisitos definidos en §6.2.11.

QSigC de tipo eIDAS

Las Claves Privadas deben generarse, almacenarse y protegerse en un QSCD que cumpla o supere los requisitos definidos en §6.2.11.

6.2.2 Control Multi-persona (N de M) de la Clave Privada

Se establece un control de dos personas como mínimo en cualquier Clave Privada de CA para todos los fines, incluidos la activación y la copia de seguridad, y puede implementarse como una combinación de controles técnicos y de procedimiento.

Las personas involucradas en el manejo y uso de las Claves Privadas de la CA son designadas como autorizadas por la CA para este fin. Los nombres de las partes que realizan el control de dos personas se mantienen en una lista controlada.

6.2.3 Custodia de Clave Privada

Entrust no deposita las Claves Privadas de las CA.

6.2.4 Copia de seguridad de Clave Privada

Claves Privadas de la CA

Las Claves Privadas de la CA se guardan bajo el control de dos personas utilizado para crear la versión original de Claves Privadas. Todas las copias de la Clave Privada de la CA están protegidas de forma segura.

Módulo criptográfico administrado y alojado

En el caso de que se utilice un módulo criptográfico administrado y alojado en una CA, se realiza una copia de seguridad de las Claves Privadas cifradas con regularidad para fines de recuperación ante desastres.

6.2.5 Archivo de Clave Privada

Claves Privadas de la CA

Al retirarse una CA, las Claves Privadas se archivarán de forma segura mediante módulos criptográficos de hardware que cumplan con los requisitos §6.2.11. Los Pares de Claves no se usan a menos que la CA se haya reactivado o las Claves sean necesarias temporalmente para validar los datos históricos. Las Claves Privadas requeridas para fines temporales se podrán eliminar del archivo durante un breve período de tiempo.

Las claves privadas de la CA archivadas se revisarán anualmente. Después de un período mínimo de 5 años, las Claves Privadas de la CA pueden ser destruidas de acuerdo con los requisitos de §6.2.10. Las Claves Privadas de la CA no deben ser destruidas si aún son necesarias para fines comerciales o legales.

Los terceros no archivarán las Claves Privadas de CA.

Módulo criptográfico administrado y alojado

En el caso de que se utilice un módulo criptográfico administrado y alojado en una CA, las Claves Privadas no se guardan.

6.2.6 Transferencia de Clave Privada hacia o desde un módulo criptográfico

Las Claves Privadas de CA se deben generar y proteger en un módulo criptográfico. En el caso de que una Clave Privada sea transportada de un módulo criptográfico a otro, la Clave Privada se debe migrar usando la metodología segura soportada por el módulo criptográfico.

Si la Clave Privada de una CA Subordinada se comunica a un tercero no autorizado, entonces la CA Subordinada revocará todos los Certificados correspondientes a la Clave Privada.

QSigC de tipo eIDAS y QsealC de tipo eIDAS

En el caso de que se utilice un dispositivo criptográfico seguro o QSCD administrado y alojado en una CA, la Clave Privada se cifrará mediante la función de envoltura de claves AES 256 del módulo criptográfico y se almacenará en una base de datos segura.

6.2.7 Almacenamiento de Claves Privadas en módulo criptográfico

Las Claves Privadas de la CA se almacenan en un módulo criptográfico, y se protegen en un módulo criptográfico tal como se define en §6.2.11.

6.2.8 Método de activación de la Clave Privada

Claves Privadas de la CA

Las Claves Privadas de la CA se activan bajo el control de dos personas utilizando la metodología proporcionada con el módulo criptográfico.

Claves Privadas del Suscriptor
Las Claves Privadas del Suscriptor deberían ser activadas por el Suscriptor para cumplir con los requisitos del software de seguridad utilizado por sus aplicaciones. Los Suscriptores protegerán sus Claves Privadas de acuerdo con los requisitos de §9.6.3.

QSigC de tipo eIDAS y QsealC de tipo eIDAS
En el caso de que se utilice un dispositivo criptográfico seguro o un QSCD administrado y alojado en una CA, la activación de la Clave Privada se realiza con la autenticación multifactor del Sujeto. El Sujeto protegerá las credenciales de acceso a la Clave Privada de acuerdo con §9.6.3.

6.2.9 Método de desactivación de la Clave Privada
Claves Privadas de la CA
Las Claves Privadas de la CA se desactivarán cuando la CA no sea necesaria para el uso. La desactivación de las Claves Privadas se realiza de acuerdo con la metodología proporcionada con el módulo criptográfico.

Claves Privadas del Suscriptor
Se considera que las Claves Privadas del Suscriptor están desactivadas cuando la Clave Privada ya no es necesaria o cuando todos los Certificados asociados con la Clave Privada han expirado o han sido revocados.

6.2.10 Método de Destrucción de la Clave Privada
Claves Privadas de la CA
La destrucción de las Claves Privadas de la CA se controlará por dos personas y se puede lograr ejecutando un comando de "puesta a cero" o por la destrucción del módulo criptográfico. La destrucción de las Claves Privadas de la CA debe ser autorizada por la Autoridad en Materia de Políticas.

Si la CA está eliminando un módulo criptográfico del servicio, todas las Claves Privadas deben eliminarse del módulo. Si el módulo criptográfico de la CA que se elimina está destinado a proporcionar características de evidencia de manipulación indebida, el dispositivo será destruido.

QSigC de tipo eIDAS y QsealC de tipo eIDAS
En el caso de que se utilice un QSCD o un dispositivo criptográfico seguro administrado y alojado en una CA, el Sujeto del Certificado puede destruir la Clave Privada mediante la autenticación multifactor. La CA está autorizada a destruir la Clave Privada cuando finaliza la suscripción al servicio.

6.2.11 Clasificación del módulo criptográfico
Pares de Claves de la CA

Los Pares de Claves de la CA deben generarse y protegerse en un módulo criptográfico que cumpla con al menos FIPS 140-2 de Nivel 3, FIPS 140-3 Nivel 3, o un Perfil de Protección de Criterios Comunes apropiado u Objetivo de Seguridad, EAL 4 (o superior), que incluye requisitos para proteger la Clave Privada y otros activos contra amenazas conocidas.

QsealC de tipo eIDAS
Los Pares de Claves deben generarse y protegerse en un dispositivo criptográfico seguro que cumpla al menos con los estándares de certificación FIPS 140-2 Nivel 2 o Common Criteria EAL 4+.

QTSC de tipo eIDAS
Los pares de claves deben generarse y protegerse en un dispositivo criptográfico seguro que cumpla al menos con los estándares de certificación FIPS 140-2 Nivel 2 o Common Criteria EAL 4+.

QSigC de tipo eIDAS
Los Pares de Claves deben generarse y protegerse en un QSCD que cumpla al menos con los estándares de certificación FIPS 140-2 Nivel 2, Common Criteria EAL 4+ o equivalente.

6.3 Otros aspectos de la gestión del Par de Claves

6.3.1 Archivo de Clave Pública

No está estipulado.

6.3.2 Períodos operativos de Certificados y períodos de uso de Pares de Claves

Pares de Claves de CA
Los pares de Claves RSA de CA de 2048 bits pueden tener un período de validez que expire a más tardar el 31 de diciembre de 2030.

QWAC de tipo eIDAS y QWAC de tipo PSD2
Los QWAC de tipo eIDAS y los QWAC de tipo PSD2 pueden tener un período de validez de 398 días,como máximo.

QSealC de tipo eIDAS, QSealC de tipo PSD2 y QSigC de tipo eIDAS
Los QSealC de tipo eIDAS, QSealC de tipo PSD2 y QSigC de tipo eIDAS pueden tener un período de validez de 3 años como máximo.

QTSC de tipo eIDAS
Los QTSC de tipo eIDAS pueden tener un período de validez de hasta, pero no más de 5 años. El período de uso de la Clave Privada no es superior a 15 meses, después de lo cual la Clave Privada será reemplazada y posteriormente destruida.

6.4 Datos de activación

6.4.1 Generación e instalación de datos de activación.
No está estipulado.

6.4.2 Protección de datos de activación
No está estipulado.

6.4.3 Otros aspectos de los datos de activación
No está estipulado.

6.5 Controles de seguridad informática
6.5.1 Requisitos técnicos específicos de seguridad informática
Las estaciones de trabajo en las que operan las CA están protegidas físicamente como se describe en §5.1. Los sistemas operativos en las estaciones de trabajo en las que las CA operan requieren la identificación y autenticación de los usuarios. El acceso a las bases de datos de software de CA y los registros de auditoría está restringido como se describe en esta CPS. Todo el personal operacional que está autorizado para tener acceso a las CA debe usar tokens de hardware junto con un PIN para tener acceso a la sala física que contiene el software de CA que se está utilizando para dichas CA.

La CA requiere autenticación de múltiples factores para todas las cuentas RA y Empresa RA capaces de emitir directamente el Certificado de Suscriptor.

Para las cuentas de Suscriptor, la CA ha implementado controles técnicos para restringir la emisión de Certificados a un conjunto limitado de dominios aprobados previamente.

6.5.2 Clasificación de seguridad informática
No está estipulado.

6.6 Controles de seguridad del ciclo de vida
6.6.1 Controles de desarrollo del sistema
La CA utiliza productos "Commercial Off The Shelf" (COTS) para el hardware, el software y los componentes de red. Los sistemas desarrollados por la CA se implementan de acuerdo con los estándares de desarrollo del ciclo de vida del software de Entrust.

6.6.2 Controles de gestión de seguridad
La configuración del sistema de la CA, así como cualquiera de las modificaciones y actualizaciones están documentadas y controladas. Los métodos para detectar modificaciones no autorizadas en el equipo y la configuración de CA garantizan la integridad del software de seguridad, el firmware y el hardware para su correcto funcionamiento. La metodología de gestión de configuración formal se utiliza para la instalación y el mantenimiento continuo de los servicios de confianza de Entrust

y del sistema de CA. Se realizan revisiones trimestrales para confirmar el cumplimiento de las políticas de seguridad.

Cuando se carga por primera vez, se verifica que el software de CA haya sido suministrado por el proveedor, sin modificaciones, y que la versión sea la prevista para su uso.

6.6.3 Controles de seguridad del ciclo de vida

En el caso de que se utilice un módulo criptográfico administrado y alojado en una CA, el Sujeto del Certificado controla el ciclo de vida del Par de Claves. El Sujeto puede destruir la Clave Privada de acuerdo con §6.2.10.

6.7 Controles de seguridad de red

La CA ha implementado controles de seguridad para cumplir con los requisitos del sistema de seguridad de red y certificado del CA / Browser Forum.

6.8 Sellado de tiempo

Entrust proporciona una Autoridad de Sellado de Tiempo Cualificada, que funciona de acuerdo con la Declaración de prácticas de la Autoridad de Sellado de Tiempo Cualificada eIDAS de EEU.

7. Perfiles de Certificado, CRL y OCSP

El perfil de los Certificados y la Lista de revocación de certificados (CRL) emitidos por una CA se ajustan a las especificaciones contenidas en el documento IETF RFC 5280 Certificado de PKI X.509 de Internet y Perfil de Lista de Certificados Revocados (CRL).

7.1 Perfil de Certificado

Las CA emiten Certificados de acuerdo con la versión 3 X.509. Los perfiles de Certificación para el Certificado de CA Raíz, los Certificados de CA Subordinadas y los Certificados de Suscriptor se describen en el Apéndice A y en las secciones posteriores.

Los Certificados tienen un número de serie mayor que cero (0) que contiene al menos 64 bits impredecibles.

Los Certificados de Suscriptor se emiten desde CA subordinadas dedicadas según los identificadores de política enumerados en §7.1.6.4.

7.1.1 Número de versión

Todos los Certificados emitidos por las CA son certificados de la versión 3 de X.509.

7.1.2 Extensiones del Certificado

7.1.2.1 Certificado de CA Raíz

Las extensiones de certificado se establecen según lo estipulado en IETF RFC 5280 y de acuerdo con el Apéndice A.

Si la CA raíz firma las respuestas de OCSP, el uso de la clave de digitalSignature se establecerá en el certificado de la CA raíz.

7.1.2.2 Certificado de CA Subordinada

Las extensiones de Certificado se establecen según lo estipulado en IETF RFC 5280 y de acuerdo con el Apéndice A.

Si la CA subordinada firma las respuestas de OCSP, el uso de la clave de digitalSignature se establecerá en el certificado de la CA subordinada.

Los requisitos de extensión para el uso extendido de claves son:

(i) Debe contener una extensión EKU,
(ii) No debe incluir el EKU anyExtendedKeyUsage, y
(iii) No debe incluir las EKUs id-kep-serverAuth, id-kp-emailProtection ni id-kp-timeStamping en el mismo certificado.

7.1.2.3 Certificado de Suscriptor

Las extensiones de Certificado se establecen según lo estipulado en IETF RFC 5280 y de acuerdo con el Apéndice A.

Certificados Cualificados
Los Certificados Cualificados incluirán qcStatement según lo exige ETSI EN 319 412-5.
Los certificados de suscriptor contienen la URL HTTP de la respuesta OCSP de la CA en la extensión accessMethod.

Certificados de tipo PSD2
Los Certificados Cualificados de Autenticación de Sitio Web de tipo PSD2 incluirán qcStatement de PSD2 según lo exige la norma ETSI EN 319 495 e incluirán la función del proveedor de servicios de pago, que puede ser uno o más de los siguientes:
(i) servicio de cuenta (PSP_AS);
(ii) inicio de pago (PSP_PI);
(iii) información de la cuenta (PSP_AI);
(iv) emisión de instrumentos de pago con tarjeta (PSP_IC).

7.1.2.4 Todos los certificados
Todos los demás campos y extensiones DEBEN establecerse de acuerdo con RFC 5280.

7.1.2.5 Aplicación de RFC 5280
A modo de aclaración, un pre-certificado, como se describe en RFC 6962 (Certificado de Transparencia), no deberá ser considerado como un "certificado" sujeto a los requisitos de RFC 5280.

7.1.3 Identificadores de objeto de algoritmo
7.1.3.1 SubjectPublicKeyInfo
Para RSA, la CA indicará una clave RSA utilizando el identificador de algoritmo rsaEncryption (OID: 1.2.840.113549.1.1.1). Los parámetros deben estar presentes y deben ser NULL explícitamente.

7.1.3.2 SignatureAlgorithmIdentifier
Todos los objetos firmados por una clave privada de CA deben cumplir estos requisitos sobre el uso del AlgorithmIdentifier o del tipo derivado de AlgorithmIdentifier en el contexto de las firmas.

Para RSA, la CA debe utilizar uno de los siguientes algoritmos de firma y codificaciones.

(i) RSASSA-PKCS1-v1_5 con SHA-256
(ii) RSASSA-PKCS1-v1_5 con SHA-384
(iii) RSASSA-PKCS1-v1_5 con SHA-512

7.1.4 Formatos de nombre

7.1.4.1 Codificación de nombre

Para cada ruta de certificación válida (según definición en RFC 5280, Sección 6) para todos los Certificados y Certificados de CA Subordinada, se debe cumplir lo siguiente:

(i) Para cada Certificado en la Ruta de Certificación, el contenido codificado del campo nombre distinguido del emisor de un Certificado será byte por byte idéntico a la forma codificada del campo nombre distinguido del Sujeto del Certificado de la CA emisora.

(ii) Para cada Certificado de CA en la Ruta de Certificación, el contenido codificado del campo de nombre distinguido del Sujeto de un Certificado será byte por byte idéntico en todos los Certificados cuyos nombres distinguidos de Sujeto se puedan comparar como iguales de acuerdo con RFC 5280, sección 7.1, e incluyendo Certificados caducados y revocados.

7.1.4.2 Información del sujeto - Certificados de Suscriptor

La información del sujeto debe cumplir con los requisitos establecidos en el Apéndice A.

Los formatos de nombre para los Certificados de Suscriptor son los estipulados en §3.1.1. Todos los demás atributos opcionales deben contener información que haya sido verificada por la CA o la RA. Los atributos opcionales no contendrán solo metadatos como '.', '-' y " (es decir, espacio), y / o cualquier otra indicación de que el valor está ausente, incompleto o no aplica.

Las entradas en dNSName están en la "sintaxis de nombre preferido" como se especifica en IETF RFC 5280 y, por lo tanto, no contienen caracteres de subrayado.

QWAC de tipo eIDAS y QWAC de tipo PSD2

Las CA no emitirán un Certificado con un Nombre de Dominio que contenga una Dirección IP Reservada o un Nombre Interno.

7.1.4.3 Información del sujeto: certificados de CA Raíz y certificados de CA Subordinada

La información del Sujeto debe cumplir con los requisitos establecidos en el Apéndice A.

7.1.5 Restricciones de nombre

Las CA no admiten la emisión de Certificados de CA Subordinadas técnicamente restringidos.

7.1.6 Identificador de objeto de política de Certificado

7.1.6.1 Identificadores de política de Certificado reservados

Los Certificados de Suscriptor deben incluir uno o más de los siguientes identificadores de política de Certificado reservados, si la CA afirma que el Certificado cumple con la política asociada:

Certificados Extended Validation (EV) SSL	2.23.140.1.1
Certificados Cualificados de Firma Electrónica	0.4.0.194112.1.0
Certificados Cualificados de Sello Electrónico y Certificados Cualificados de Sello de Tiempo	0.4.0.194112.1.1
Certificados Cualificados de Autenticación de Sitio Web	0.4.0.194112.1.4
Certificados Cualificados de Autenticación de Sitio Web de tipo PSD2	0.4.0.19495.3.1

La CA declara que todos los Certificados que contienen un identificador de política de certificado reservado indican el cumplimiento de los requisitos asociados y se emiten y gestionan de acuerdo con dichos requisitos.

7.1.6.2 Certificados de CA Raíz

Los Certificados de CA Raíz no contienen los identificadores de objeto de política de certificado.

7.1.6.3 Certificados de CA Subordinadas

CA Subordinada

Los Certificados de CA Subordinadas deben incluir el identificador de objeto de política de Certificado de "cualquier política" o uno o más identificadores explícitos de objeto de política de Certificado que indiquen el cumplimiento de una política de Certificado específica. Los identificadores de objeto de política de certificado se enumeran en §7.1.6.4.

7.1.6.4 Certificados de Suscriptor

Los Certificados pueden incluir uno o más de los siguientes identificadores de política de certificado:

Certificates Extended Validation (EV) SSL
2.16.840.1.114028.10.1.2
Document Signing Certificates (AATL)
2.16.840.1.114028.10.1.6
Certificados Cualificados de Sello Electrónico (QCP-l)
2.16.840.1.114028.10.1.12.1
Certificados Cualificados de Firma Electrónica (QCP-n-qscd)
2.16.840.1.114028.10.1.12.2
Certificados Cualificados de Autenticación de Sitio Web (QCP-w)
2.16.840.1.114028.10.1.12.4
Certificados Cualificados de Sello Electrónico de tipo PSD2 (QCP-l-psd2)
2.16.840.1.114028.10.1.12.5

Certificados Cualificados de Autenticación de Sitio Web de tipo PSD2 (QCP-w-psd2)
2.16.840.1.114028.10.1.12.6
Certificados Cualificados de Sello de Tiempo (QCP-l para sellado de tiempo)
2.16.840.1.114028.10.1.12.7

7.1.7 Uso de la extensión de restricciones de políticas
No está estipulado.

7.1.8 Sintaxis y semántica de los Calificadores de política
Las CA incluyen calificadores de políticas en todos los Certificados de Suscriptor como se estipula en el Apéndice A.

7.1.9 Tratamiento semántico para la extensión crítica de política de Certificado
La extensión de las políticas de Certificado está marcada como no crítica.

7.2 Perfil de CRL
Las CA utilizan los siguientes campos del formato CRL de la versión 2 de X.509:
• Versión: configurada en v2
• Firma: identificador del algoritmo utilizado para firmar la CRL
• Emisor: el nombre equivalente byte por byte al distinguido de la CA que emite la CRL
• Esta actualización: hora de emisión de la CRL
• Próxima actualización: hora prevista de la próxima actualización de CRL
• Certificados revocados: lista de información de Certificados revocados

7.2.1 Número de versión
Las CRL emitidas por las CA son X.509 versión 2.

7.2.2 CRL y extensiones de entrada de CRL
reasonCode (OID 2.5.29.21)
La extensión del código CRLReason se utiliza para todos los Certificados revocados. La CRLReason indicada no debe ser sin especificar (0) y si se utiliza reasonCode no especificado (0), la CA omitirá la entrada de reasonCode en la CRL.

Esta extensión no debe marcarse como crítica. El Suscriptor o la CA deben seleccionar el motivo más apropiado de uno de los siguientes:

(i) keyCompromise (1), si la clave del certificado ha sido o se sospecha que está comprometida;
(ii) cACompromise (2), si la CA ha sido o se sospecha que está comprometida
(iii) affiliationChange (3), si la información verificada en el Certificado ha cambiado y, como tal, las Partes que Confían ya no deberían confiar en el Certificado;

(iv) superseded (4), si el Certificado se ha vuelto a emitir, se ha cambiado de clave o se ha renovado por otro Certificado, la CA tiene evidencia de que no se debe confiar en la validación del dominio o la dirección IP o el Certificado no se emitió de acuerdo con los requisitos de §1.1 o de esta CPS;
(v) cessationOfOperation (5), si el sitio web o el dispositivo ya no está en servicio o el Suscriptor ya no controla el Nombre de Dominio; o
(vi) privilegeWithdrawn (9), si la CA determina que el privilegio del Certificado emitido por el Suscriptor ya no existe.

El motivo de revocación predeterminado no se especifica (0), lo que hace que no se proporcione ningún reasonCode en la CRL. La CA no utilizará reasonCode certificateHold (6). El código de motivo de privilegeWithdrawn (9) no se pone a disposición del Suscriptor.

Si la CA obtiene evidencia de Compromiso de clave o la Clave privada ha firmado un código sospechoso para un Certificado cuya entrada de CRL no contiene una extensión de reasonCode o tiene una extensión de reasonCode con un motivo que es non-keyCompromise (1), la CA puede actualizar el reasonCode de CRL a keyCompromise (1).

7.3 Perfil OCSP

El perfil para los mensajes del Protocolo en línea de estado de certificado (OCSP) emitidos por una CA se ajusta a la especificaciones contenidas en el perfil del protocolo en línea de estado de certificado (OCSP) PKI Internet X.509 PKI de IETF.

Si una respuesta de OCSP es para un certificado de CA raíz o CA subordinada, incluidos los certificados cruzados, y ese certificado ha sido revocado, entonces el campo revocationReason dentro de RevokedInfo del CertStatus estará presente.

El CRLReason indicado contendrá un valor permitido para las CRL, como se especifica en §7.2.2.

7.3.1 Número de versión

No está estipulado.

7.3.2 Extensiones OCSP

Las extensiones singleExtensions de una respuesta OCSP no contienen la extensión de entrada de CRL reasonCode (OID 2.5.29.21).

8. Auditoría de conformidad y otras evaluaciones

La CA cumple con los requisitos establecidos en §1.1, que incluye los requisitos básicos, las Guías EV SSL y el Reglamento (UE) n.º 910/2014. La CA cumple con los requisitos de auditoría de cumplimiento de esta sección. La CA tiene licencia, si corresponde, para cada jurisdicción donde emite Certificados.

8.1 Frecuencia o Circunstancias de Auditoría

Las claves privadas raíz y subordinada y la CA se auditan continuamente desde la generación de la clave hasta que ya no se confía en la CA desde el vencimiento o la revocación del certificado de CA. Las CA son auditadas para verificar que cumplan con las prácticas y procedimientos establecidos en la CPS con la que opera la CA. El período durante el cual la CA emite Certificados se dividirá en una secuencia ininterrumpida de periodos de auditoría. Un período de auditoría no excederá un año de duración.

Ya no será necesario auditar la implementación de una CA si todos los Certificados de CA para la CA han expirado o han sido revocados antes del comienzo del período de auditoría.

8.2 Identidad / Acreditaciones del Auditor

La auditoría de conformidad de las CA se realiza por un auditor que posea las siguientes cualificaciones y habilidades:

i. Independencia del sujeto de la auditoria;

ii. Capacidad para realizar una auditoría que aborde los criterios de los esquemas de auditoría especificados en §8.4;

iii. Emplear a personas que tienen competencia en el examen de la tecnología PKI, herramientas y técnicas de seguridad de la información, auditoría de seguridad y tecnología de la información, y la función de certificación de terceros

iv. Realizado por un organismo de evaluación de conformidad con licencia y acreditado de acuerdo con ISO 17065 que aplica los requisitos especificados en ETSI EN 319 403;

v. Limitado por la ley, la regulación gubernamental o el código de ética profesional; y

vi. Mantener los límites de la póliza del seguro de responsabilidad profesional / errores y omisiones de al menos un millón de dólares estadounidenses de cobertura.

8.3 Relación del auditor con la entidad auditada

La firma de contabilidad pública certificada seleccionada para realizar la auditoría de conformidad para las CA y RA deberá ser independiente de la entidad que está siendo auditada.

8.4 Temas cubiertos por la auditoría

La auditoría de conformidad probará el cumplimiento por parte de las CA y RA de las políticas y procedimientos establecidos, según sean aplicables en:

i. Esta CPS;
ii. ETSI EN 319 411-2 y documentos de normas relacionadas;
iii. ETSI TS 119 495 y documentos de normas relacionadas.

8.5 Acciones tomadas como resultado de las deficiencias

Al recibir una auditoría de conformidad que identifique cualquier incidencia, la CA auditada informará de la misma a los ASV.

8.6 Comunicación de resultados

El informe de auditoría indicará que cubre los sistemas y procesos relevantes utilizados en la emisión de todos los Certificados que afirman uno o más de los identificadores de política enumerados en §7.1.6.1.

Los resultados de todas las auditorías de conformidad se comunicarán a la Autoridad en Materia de Políticas y a cualquier tercero que tenga derecho por ley o reglamento a recibir una copia de los resultados de la auditoría.

Los resultados de la auditoría de conformidad más reciente se publicarán en el Repositorio dentro de los tres meses posteriores al final del período de la auditoría y, si aplica, en la CCADB. En caso de un retraso superior a tres meses, la CA proporcionará una carta explicativa firmada por el auditor cualificado.

El informe de auditoría contendrá al menos la siguiente información:
(i) nombre de la organización que se audita;
(ii) nombre y dirección de la organización que realiza la auditoría;
(iii) la huella digital SHA-256 de todos los Certificados de CA Raíz y Subordinada, incluidos los Certificados Cruzados, que estaban dentro del alcance de la auditoría, donde la huella digital usa letras mayúsculas y no contiene dos puntos, espacios ni saltos de línea;
(iv) criterios de auditoría, con número (s) de versión, que se utilizaron para auditar cada uno de los certificados (y claves asociadas);
(v) una lista de los documentos de política de la CA, con números de versión, referenciados durante la auditoría;
(vi) si la auditoría evaluó un período de tiempo o un momento determinado;
(vii) la fecha de inicio y la fecha de finalización del Período de Auditoría, para aquellas que abarquen un período de tiempo;
(viii) la fecha puntual, para aquellas que sean para un momento puntual;
(ix) la fecha de emisión del informe, que será necesariamente posterior a la fecha de finalización o fecha del momento;
(x) (para auditorías realizadas de acuerdo con cualquiera de las normas ETSI) una declaración para indicar si la auditoría fue una auditoría completa o una auditoría de seguimiento, y qué partes de los criterios se aplicaron y evaluaron, p. DVCP, OVCP,

NCP, NCP +, LCP, EVCP, EVCP +, QCP-w, Parte 1 (Requisitos generales) y / o Parte 2 (Requisitos para proveedores de servicios de confianza);
(xi) (para auditorías realizadas de acuerdo con cualquiera de los estándares ETSI) una declaración para indicar que el auditor hizo referencia a los criterios aplicables de CA / Browser Forum, como este documento, y la versión utilizada;
(xii) todos los incidentes revelados por la CA, o informados por un tercero, y todos los hallazgos informados por un auditor calificado, que, en cualquier momento durante el período de auditoría, ocurrieron, estuvieron abiertos en Bugzilla o se informaron a una tienda; y
(xiii) una declaración explícita que indique que la auditoría cubre los sistemas y procesos relevantes utilizados en la emisión de todos los Certificados que afirman los identificadores de póliza en §7.1.6.1.

La versión autorizada del informe de auditoría debe estar en inglés, disponible en formato PDF y con texto que permita buscar toda la información requerida.

8.7 Auditorías internas

Los Certificados de Suscriptor son auto-auditados utilizando un software de linting posterior a la emisión para monitorizar el cumplimiento de los elementos aplicables de esta CPS, limitado a la cobertura de linter.

QWAC de tipo eIDAS y QWAC de tipo PSD2

Los QWAC de tipo eIDAS y QWAC de tipo PSD2 se auto-auditan utilizando un software de linting previo a la emisión para monitorear las adherencias a esta CPS, los Requisitos de Referencia y las Guías EV SSL limitadas a la cobertura de linter.

9. Otros asuntos comerciales y legales

9.1 Tarifas

A menos que se especifique lo contrario en un Acuerdo de Suscriptor, las tarifas por los servicios prestados por Entrust con respecto a los Certificados se establecen en los sitios web (incluidos los sitios de comercio electrónico) manejados por Entrust. A menos que se indique lo contrario en un Acuerdo de Suscriptor, estas tarifas están sujetas a cambios, y dichos cambios entrarán en vigor inmediatamente después de su publicación en dichos sitios web (incluidos los sitios de comercio electrónico). Las tarifas por los servicios proporcionados por RA independientes de terceros, Revendedores y Comerciales con respecto a los Certificados se establecen en los sitios web operados por dichas RA, Revendedores y Comerciales. Estas tarifas están sujetas a cambios, y dichos cambios entrarán en vigor inmediatamente después de su publicación en tales sitios web.

9.1.1 Tarifas de emisión o renovación de Certificados

No está estipulado.

9.1.2 Tarifas de acceso al Certificado

No está estipulado.

9.1.3 Tarifas de Revocación o de acceso a la información de estado

No está estipulado.

9.1.4 Tarifas por otros servicios

No está estipulado.

9.1.5 Política de reembolso

Excepto en el caso de una política formal de reembolso por escrito de Entrust, si la hay, ni Entrust ni ninguna RA que opera bajo las CA proporcionan reembolsos por Certificados o servicios en relación a los Certificados.

9.2 Responsabilidad financiera

Los Suscriptores y las Partes que Confían serán responsables de las consecuencias financieras para dichos Suscriptores, Partes que Confían, y cualquier otra persona, entidad u organización para cualquier transacción en la cual tales Suscriptores o Partes que Confían participen y utilicen Certificados o cualquier servicio provisto con respecto a Certificados.

9.2.1 Cobertura del seguro

Entrust mantiene (a) un seguro de responsabilidad civil comercial con límites de póliza de al menos dos millones de dólares estadounidenses (US $ 2.000.000,00) de cobertura; y (b) seguro de responsabilidad profesional / errores y omisiones, con límites de póliza de al menos cinco millones de dólares estadounidenses (US $ 5.000.000,00) de cobertura. Tales pólizas de seguro se llevarán a cabo con

compañías calificadas con no menos de A- en cuanto a la calificación del titular de la póliza en la edición actual de Best's Insurance Guide.

9.2.2 Otros activos
No está estipulado.

9.2.3 Cobertura de seguro o garantía para entidades finales
No está estipulado.

9.3 Confidencialidad de la información comercial

9.3.1 Alcance de la información confidencial

La siguiente información se considera información confidencial de Entrust y está protegida contra la divulgación con un grado razonable de cuidado:

- Claves Privadas;
- Datos de activación utilizados para acceder a las Claves Privadas o para acceder al sistema de CA;
- Planes de continuidad del negocio, respuesta a incidentes, contingencia y recuperación ante desastres;
- Otras prácticas de seguridad utilizadas para proteger la confidencialidad, integridad o disponibilidad de la información;
- Información mantenida por Entrust como información privada de acuerdo con 9.4;
- Registros de auditoría y registros de archivo; y
- Registros de transacciones, registros de auditoría financiera y registros de seguimiento de auditoría externa o interna y cualquier informe de auditoría (con la excepción de una carta del auditor que confirme la efectividad de los controles establecidos en esta CPS).

9.3.2 Información fuera del alcance de la información confidencial

La información que se incluye en un Certificado o en una Lista de revocación de certificados se considera pública.

9.3.3 Responsabilidad de proteger la información confidencial
Los empleados, agentes y contratistas de Entrust son responsables de proteger la información confidencialidad y están obligados contractualmente a hacerlo. Los sistemas Entrust están configurados para proteger información confidencial.

9.4 Privacidad de la información personal

9.4.1 Plan de Privacidad

Entrust sigue las políticas, declaraciones y prácticas disponibles en www.entrust.com/legal-compliance/privacy ("Privacy Plan") cuando se trata de información personal.

9.4.2 Información considerada privada
Entrust trata toda la información personal sobre un individuo como información personal de acuerdo con el Plan de Privacidad.

9.4.3 Información no considerada privada
Los Certificados, CRL y OCSP y la información personal o corporativa que aparece en ellos no se consideran información confidencial.

9.4.4 Responsabilidad de proteger la información privada
El personal de Entrust debe proteger la información personal de acuerdo con la Política de protección de datos.

9.4.5 Aviso y consentimiento para utilizar información privada
A menos que se indique lo contrario en la CPS, el Plan de Privacidad u otro acuerdo (como un Acuerdo de Suscriptor o un Acuerdo de Parte que Confía), la información personal no se utilizará sin el consentimiento del sujeto de
tal información personal. No obstante lo anterior, la información personal contenida en un Certificado puede publicarse en repositorios públicos en línea y todos los Suscriptores aceptan la transferencia global de cualquiera de los datos personales contenidos en el Certificado.

9.4.6 Divulgación de conformidad con el proceso judicial o administrativo
Entrust, RA de terceros independientes bajo una CA, Revendedores y Comerciales tienen derecho a divulgar información que se considera personal y/o confidencial a los funcionarios encargados de hacer cumplir la ley en cumplimiento de la legislación aplicable.

Entrust, RA de terceros independientes bajo una CA, Revendedores y Comerciales pueden divulgar información que se considera confidencial durante el curso de cualquier arbitraje, litigio o cualquier otro procedimiento legal, judicial o administrativo relacionado con dicha información. Cualquier divulgación de este tipo será permisible siempre que Entrust, la RA de tercero independiente, el Revendedor o el Comercial utilice esfuerzos comercialmente razonables para obtener una orden de protección presentada por un tribunal que restrinja el uso y divulgación de dicha información en la medida en que sea razonablemente necesaria para los fines de dicho arbitraje, litigio o cualquier otro procedimiento legal, judicial o administrativo.

9.4.7 Otras circunstancias de divulgación de información

Entrust, RA de terceros independientes bajo una CA, Revendedores y Comerciales pueden divulgar la información proporcionada a Entrust, la RA, Revendedor o Comercial, por un Solicitante, un Suscriptor, o una Parte que Confía a petición de dicho Solicitante, Suscriptor o Parte que Confía.

Si un Certificado es revocado por una CA, se proporcionará el estado del Certificado mediante la Lista de revocación de certificados y la respuesta del OCSP.

9.5 Derechos de propiedad intelectual

Entrust retiene todos los derechos, títulos e intereses (incluidos todos los derechos de propiedad intelectual), de la CPS y de todos los Certificados, a excepción de cualquier información que proporcione un Solicitante o un Suscriptor y que sea incluida en un Certificado, cuya información será propiedad del Solicitante o del Suscriptor. Sujeto a disponibilidad, Entrust puede, a su discreción, poner a disposición de los Suscriptores copias de uno o más Certificados de CA Subordinadas, para uso exclusivo con el Certificado emitido para tales Suscriptores. Entrust se reserva todos los derechos, títulos e intereses (incluidos todos los derechos de propiedad intelectual), sobre los Certificados de CA Subordinadas. Salvo que se establezca expresamente en el Acuerdo de Suscriptor, no se otorga ni se considerará otorgado ningún derecho, ya sea implícitamente o por exclusión, inferencia o de otro modo.

9.6 Representación y garantías

9.6.1 Representaciones y garantías de la CA

Entrust ofrece las siguientes garantías limitadas con respecto al funcionamiento de las CA. Una CA deberá:

(i) proporcionar servicios de CA de acuerdo con la CPS;
(ii) al recibir una solicitud de una RA que opera bajo dicha CA, emitir un Certificado de acuerdo con las prácticas y procedimientos de la CPS;
(iii) poner a disposición la información de revocación del Certificado emitiendo Certificados y emitiendo y poniendo a disposición las CRL de los certificados y las respuestas OCSP en un Repositorio de acuerdo con la CPS;
(iv) emitir y publicar las CRL de los Certificados y las respuestas OCSP regularmente de acuerdo con la CPS;
(v) proporcionar servicios de revocación de acuerdo con los procedimientos establecidos en la CPS; y
(vi) proporcionar servicios de Repositorio de acuerdo con las prácticas y procedimientos de la CPS.

Al operar las CA, Entrust puede usar uno o más representantes o agentes para realizar sus obligaciones en virtud de la CPS, cualquier Acuerdo de Suscriptor o cualquier Acuerdo de Parte que Confía, siempre que Entrust sea responsable de su desempeño.

En ningún caso Entrust Group actúa como representante, o proporciona garantías o condiciones a los Solicitantes, Suscriptores, Partes que Confían o cualquier otra persona, entidades u organizaciones con respecto a (i) las técnicas utilizadas por cualquier parte que no sea Entrust en la generación y el almacenamiento de la Clave Privada correspondiente a la Clave Pública en un Certificado, incluso si dicha Clave Privada se halla comprometida o haya sido generada utilizando técnicas criptográficas de sonido, (ii) la confiabilidad de cualquier técnica de criptografía o métodos utilizados para realizar cualquier acto, transacción o proceso que involucre o utilice un Certificado, o (iii) no repudio de cualquier Certificado o transacción facilitada a través del uso de un Certificado, ya que dicha determinación es una cuestión de ley aplicable.

9.6.2 Representaciones y Garantías de la RA

Las RA que operan bajo una CA deben:

(i) recibir Solicitudes de Certificado de acuerdo con la CPS;

(ii) realizar, registrar y asegurar la verificación de la información presentada por los Solicitantes al solicitar Certificados, y si dicha verificación es satisfactoria, enviar una Solicitud a una CA para la emisión de un Certificado, siempre de acuerdo con la CPS;

(iii) recibir y verificar las solicitudes de los Suscriptores para la revocación de Certificados, y si la verificación de una Solicitud de Revocación es satisfactoria, enviar una solicitud a una CA para la revocación de dicho Certificado, siempre de acuerdo con la CPS;

(iv) notificar a los Suscriptores, de acuerdo con la CPS, que un Certificado se les ha expedido; y

(v) notificar a los Suscriptores, de acuerdo con la CPS, que el Certificado que se les ha emitido ha sido revocado o caducará pronto.

Entrust puede utilizar uno o más representantes o agentes para cumplir con sus obligaciones con respecto a una RA de Entrust bajo la CPS, cualquier Acuerdo de Suscriptor o cualquier Acuerdo de Parte que Confía, siempre que Entrust siga siendo responsable del desempeño de dichos representantes o agentes bajo la CPS, cualquier Acuerdo de Suscriptor o cualquier Acuerdo de Parte que Confía. Entrust puede designar a terceros independientes para que actúen como RA bajo una CA. Dichas RA de terceros independientes serán responsables de su desempeño bajo la CPS, cualquier Acuerdo de Suscriptor o cualquier Acuerdo de Parte que Confía. Entrust no será responsable del rendimiento de dichas RA de terceros independientes. Las RA de terceros independientes pueden usar uno o más representantes o agentes para cumplir con sus obligaciones cuando actúan como una RA bajo una CA. Las RA de terceros independientes seguirán siendo responsables del rendimiento de dichos representantes o agentes bajo la CPS, cualquier Acuerdo de Suscriptor, o cualquier Acuerdo de Parte que Confía. Entrust puede nombrar Revendedores y Comerciales para (i) Certificados y (ii) servicios proporcionados con respecto a los Certificados. Dichos Revendedores y Comerciales serán

responsables de su desempeño bajo la CPS, cualquier Acuerdo de Suscriptor o cualquier Acuerdo de Parte que Confía. Entrust no será responsable del rendimiento de ninguno de dichos Revendedores ni Comerciales. Los Revendedores y Comerciales pueden usar uno o más representantes o agentes para cumplir con sus obligaciones bajo la CPS, cualquier Acuerdo de Suscriptor, o cualquier Acuerdo de Parte que Confía. Los Revendedores y Comerciales permanecerán como responsables del desempeño de dichos representantes o agentes bajo la CPS, cualquier Acuerdo de Suscriptor, o cualquier Acuerdo de Parte que Confía. Las RA de terceros independientes, Revendedores y Comerciales tendrán derecho a beneficiarse de (i) las exenciones de responsabilidad de representaciones, garantías y condiciones, (ii) limitaciones de responsabilidad, (iii) declaraciones y garantías de los Solicitantes, Suscriptores y Partes que Confían, e (iv) indemnizaciones de los Solicitantes, Suscriptores y Partes que Confían, establecidas en esta CPS, cualquier Acuerdo de Suscriptor, y cualquier Acuerdo de Parte que Confía.

9.6.3 Representaciones y garantías de los Suscriptores

Como condición para tener un Certificado emitido a o para el Suscriptor, cada Suscriptor (en esta sección, "Suscriptor" incluye "Solicitante" cuando se hace referencia a cualquier momento antes de la emisión del Certificado) hace, en su propio nombre y si corresponde en nombre de su principal o agente bajo una relación de subcontratista o servicio de hospedaje, las siguientes representaciones, compromisos, afirmaciones y garantías en beneficio de los Beneficiarios del Certificado, Entrust y cualquiera de los Afiliados de Entrust que emitirán Certificados a o para el Suscriptor:

9.6.3.1 Para todos los Certificados:

(i) Si el Suscriptor solicita la emisión de un Certificado a nombre de otra Persona, dicha Persona ha autorizado al Suscriptor para actuar en su nombre, incluso para solicitar Certificados en nombre de dicha Persona, y para hacer las declaraciones, compromisos, afirmaciones y garantías en este §9.6.3 en nombre de dicha Persona, así como en el propio nombre del Suscriptor.
(ii) Toda la información proporcionada y todas las representaciones realizadas, en todo momento, por el Suscriptor en relación con cualquier Servicio de Certificado, incluso en la solicitud de Certificado y de otro modo en relación con la emisión del Certificado, son y serán completas, correctas y precisas, incluyendo que cualquier entidad legal Sujeto existe legalmente como una entidad válida en la jurisdicción de incorporación o registro especificada en el Certificado (y dicha información y representaciones se actualizarán oportunamente de vez en cuando según sea necesario para mantener dicha integridad, corrección y precisión), y no infringe, se apropia indebidamente, diluye, compite injustamente o viola de otro modo la propiedad intelectual u otros derechos de cualquier persona, entidad u organización en cualquier jurisdicción. Para mayor claridad, al enviar

cualquier solicitud de un Certificado utilizando información pre-cualificada, se considera que un Suscriptor está haciendo de nuevo las declaraciones, compromisos, afirmaciones y garantías establecidas en este §9.6.3, y Entrust no tendrá la obligación de emitir ningún Certificado que contenga información pre-cualificada si posteriormente se descubre que dicha información ha cambiado o es de alguna manera inexacta, incorrecta o engañosa.

(iii) La Clave Privada correspondiente a la Clave Pública enviada a Entrust con la solicitud de Certificado fue creada utilizando técnicas criptográficas sólidas (en un módulo criptográfico si y según lo requiera la CPS) y se han tomado todas las medidas razonables para, en todo momento, asegurar el control, mantener la confidencialidad, proteger adecuadamente y prohibir los uso de la clave privada (y cualquier acceso asociado o datos de activación o dispositivo, por ejemplo, contraseña o token).

(iv) Cualquier dispositivo que almacene Claves Privadas será operado y mantenido de manera segura.

(v) No se instalará ni utilizará un Certificado hasta que el Suscriptor haya revisado y verificado que el contenido del Certificado es exacto y correcto.

(vi) En el caso de los QWAC de tipo eIDAS y los QWAC de tipo PSD2, el Certificado se instalará solo en los servidores a los que se puede acceder en el Nombre de Dominio (subjectAltName (s)) que figura en el Certificado.

(vii) Los Certificados y la Clave Privada correspondiente a la Clave Pública enumerada en dicho Certificado solo se utilizarán de conformidad con todas las leyes aplicables y únicamente de conformidad con el Acuerdo, y solo se utilizarán en nombre de la organización indicada. como Sujeto en dichos Certificados.

(viii) El contenido de los Certificados no se modificará indebidamente.

(ix) El Suscriptor notificará a Entrust, dejará de usar el Certificado y la Clave Privada correspondiente a la Clave Pública en el Certificado y solicitará la revocación del Certificado.

a) con prontitud, si cualquier información incluida en el Certificado o la solicitud de un Certificado cambia, es o se vuelve incorrecta o inexacta, o si cualquier cambio en cualquier circunstancia pudiera hacer que la información del Certificado sea engañosa.

b) inmediatamente, si existe de forma real o sospechada un Compromiso de Clave, si la Clave Privada se ha extraviado o ha sido robada, o si el control sobre la Clave Privada se ha perdido por otras razones.

(x) El Suscriptor cesará de inmediato todo uso del Certificado y la Clave Privada correspondiente a la Clave Pública en dicho Certificado al vencimiento o revocación. de dicho Certificado.

(xi) El Suscriptor responderá inmediatamente a las instrucciones de Entrust con respecto a cualquier Compromiso de Clave o mal uso o sospecha de mal uso de un Certificado.

(xii) El Suscriptor reconoce y acepta que Entrust tiene derecho a revocar un Certificado de inmediato si:

a) El Subscriptor incumple el Acuerdo de Suscriptor.

b) Entrust descubre que ha habido un Compromiso de Clave de la Clave Privada del Certificado.

c) La revocación es obligatoria según la CPS o los Estándares de la Industria. Entrust descubre que el Certificado se ha visto comprometido o se está utilizando para Código Sospechoso.

d) La Clave Privada correspondiente a la Clave Pública en el Certificado ha sido utilizada para firmar digitalmente el Código sospechoso.

(xiii) Cuando el Sujeto nombrado en el Certificado (s) es una entidad separada del Suscriptor, el Sujeto ha autorizado la inclusión de la información del Sujeto en el Certificado.

(xiv) El Suscriptor posee, controla o tiene el derecho exclusivo de usar el Nombre de Dominio o la dirección de correo electrónico que figuran en el Certificado.

(xv) El Suscriptor reconoce y acepta que Entrust tiene derecho a modificar el Acuerdo cuando sea necesario para cumplir con cualquier cambio en los Estándares de la Industria.

(xvi) El Suscriptor utilizará el juicio apropiado sobre si es apropiado, dado el nivel de seguridad y confianza que proporciona el Certificado, utilizar el Certificado en cualquier circunstancia dada.

9.6.3.2 Además, en el caso de Certificados Cualificados y Certificados de tipo PSD2,

(i) El suscriptor cumplirá con todos los requisitos de la CPS para poder utilizar un tipo específico de dispositivo criptográfico (incluyendo un dispositivo criptográfico seguro o QSCD) y, si es necesario:

a) la (s) Clave (s) Privada (s) del Sujeto solo se utilizarán para funciones criptográficas dentro del dispositivo criptográfico seguro.

Si las claves del Sujeto se generan bajo el control del Suscriptor o del Sujeto, las claves del Sujeto se generarán dentro del dispositivo criptográfico seguro especificado.

b) Para mayor claridad, el dispositivo criptográfico especificado para la generación y uso de las Claves Privadas de QSealC de tipo eIDAS es un dispositivo criptográfico seguro, y el dispositivo criptográfico especificado para la generación y uso de la(s) Clave(s) Privada(s) QSigC de tipo eIDAS es un QSCD.

(ii) El Suscriptor consiente que Entrust mantenga un registro de la información utilizada en el registro, la provisión del dispositivo sujeto, incluso si se trata del Suscriptor o del Sujeto donde difieren, y cualquier revocación posterior, la identidad y cualquier atributo específico colocado en el Certificado, y la transmisión de esta información a terceros en las mismas

condiciones requeridas por los Estándares de la Industria en el caso de que Entrust cancele sus servicios.
(iii) El Suscriptor requiere la publicación del Certificado en la forma y de acuerdo con las condiciones establecidas en la CPS y obtendrá, en su caso, el consentimiento del Sujeto para dicha publicación.
(iv) La Clave Privada y la Clave Pública correspondiente asociada con el Certificado solo se utilizarán de acuerdo con las limitaciones notificadas al Suscriptor, incluso en la CPS.
(v) Si el Suscriptor o el Sujeto genera las claves del Sujeto:

a) las claves de Sujeto se generarán utilizando un algoritmo como se especifica en los estándares de la industria para los usos de la clave certificada como se identifica en la CPS.
b) la longitud de la clave y el algoritmo serán los especificados en los Estándares de la Industria para los usos de la clave certificada identificada en la CPS durante el tiempo de validez del Certificado.
c) la Clave Privada del Sujeto se mantendrá bajo el control del Sujeto y, si el Sujeto es un individuo, la Clave Privada del Sujeto se mantendrá bajo el control exclusivo del Sujeto.

(vi) La Clave Privada del Sujeto se utilizará bajo el control del Sujeto y, si el Sujeto es un individuo, el control exclusivo del Sujeto.
(vii) Al ser informado de que el Certificado del Sujeto ha sido revocado, o que la CA emisora se ha visto comprometida, el Suscriptor se asegurará de que el Sujeto ya no utilice la Clave Privada correspondiente a la Clave Pública en el Certificado.
(viii) Con respecto a QSigC de tipo eIDAS, los Pares de Claves solo se utilizarán para firmas electrónicas.
(ix) Con respecto a QSealC de tipo eIDAS y QSealC de tipo PSD2, los Pares de Claves solo se utilizarán para sellos electrónicos.

9.6.4 Representaciones y garantías de las Partes que Confían

Todas las Partes que Confían realizan las siguientes declaraciones, compromisos, afirmaciones y garantías:

(i) La Parte que Confía debe comprender y, si es necesario, recibir una educación adecuada en el uso de la criptografía de Clave Pública y Certificados incluyendo los Certificados.
(ii) La Parte que Confía debe leer y aceptar todos los términos y condiciones de la CPS y el Acuerdo de Parte que Confía.
(iii) La Parte que Confía debe verificar los Certificados, incluido el uso de CRL, de acuerdo con el procedimiento de validación del camino de certificación especificado en la Rec. UIT-T X.509: 2005 | ISO / IEC 9594-8 (2005), teniendo en cuenta cualquier extensión crítica y correcciones técnicas aprobadas, según corresponda.

(iv) La Parte que Confía debe confiar y hacer uso de un Certificado solo si el Certificado no ha caducado ni ha sido revocado y si se puede establecer una cadena de confianza adecuada a una CA Raíz fiable.
(v) La Parte que Confía deberá validar adecuadamente un Certificado antes de tomar una decisión sobre si confiar en dicho Certificado, incluida la confirmación de que el Certificado no ha expirado o ha sido revocado y que se puede establecer una cadena de confianza adecuada hasta una CA Raíz fiable.
(vi) La Parte que Confía no se basará en un Certificado que no pueda validarse con un ancla de confianza, que se encuentre en la lista de confianza de la UE en el siguiente sitio: https://webgate.ec.europa.eu/tl-browser/#/tl/ES/37.
(vii) La Parte que Confía deberá emitir su propio juicio y confiar en un Certificado solo si dicha confianza es razonable en las circunstancias dadas, incluida la determinación de si tal confianza es razonable dada la naturaleza de la seguridad y la confianza proporcionadas por un Certificado y el valor de cualquier transacción que pueda implicar el uso de un Certificado.
(viii) La Parte que Confía ejercerá su propio juicio para determinar si es razonable, dadas las circunstancias, confiar en un Certificado, incluida la determinación de si dicha confianza es razonable dada la naturaleza de la seguridad y la confianza que proporciona un Certificado y el valor de cualquier transacción que puede implicar el uso de un Certificado.
(ix) La Parte que Confía no utilizará un Certificado para actividades peligrosas o ilegales (incluidas las delictivas).
(x) La Parte que Confía deberá confiar y hacer uso de un Certificado solo si el Certificado no ha caducado o ha sido revocado y si se puede establecer una cadena de confianza adecuada hasta una CA Raíz fiable, y la Parte que Confía no se basará en un Certificado revocado o caducado.

9.6.5 Representaciones y garantías de otros participantes

Los terceros que realicen servicios de Certificado deberán proporcionar dichos servicios de acuerdo con los requisitos de la CPS.

9.7 Exención de garantías

Excepto por la garantía limitada descrita en §9.6.1 arriba, y salvo que se indique lo contrario en el Acuerdo de Suscriptor, los Afiliados de Entrust y de Entrust Group renuncian expresamente y no representan, u ofrecen garantía o pacto de ningún tipo, sea expreso o implícito, ya sea de hecho o por aplicación de la ley, con respecto a esta CPS o cualquier certificado publicado aquí, incluyendo sin limitación alguna, todas las garantías de calidad, comerciabilidad, no infracción, título y adecuación a un propósito particular, y todas las garantías, representaciones, condiciones, compromisos, términos y obligaciones que implique el derecho estatutario o consuetudinario, uso comercial, negociación u otros están excluidos en la extensión máxima permitida por la ley. Excepto por la garantía limitada descrita arriba, los Afiliados de Entrust y de Entrust Group renuncian además y no representan, u

ofrecen garantía o pacto de ningún tipo, ya sea expreso o implícito, ya sea de hecho o por aplicación de la ley, a ningún Solicitante, Suscriptor o cualquier Parte que Confía, de que (a) el Suscriptor al que se ha emitido un Certificado es la persona, entidad u organización que declara que le ha sido emitido este Certificado (b) un Suscriptor es de hecho la persona, entidad u organización que aparece en el Certificado, o (c) la información contenida en los Certificados o en cualquier mecanismo de estado del Certificado recopilado, publicado o de otra manera difundido por Entrust, o los resultados de cualquier método criptográfico implementado en conexión con los Certificados es exacto, auténtico, completo o fiable.

Se acuerda y reconoce que los Solicitantes y sus Suscriptores son responsables de cualquier representación falsificada hecha a Entrust y en la que una Parte que Confía ha confiado. Los Afiliados de Entrust y de Entrust Group no garantizan bajo ninguna circunstancia la "no repudiación" por un Suscriptor y / o una Parte que Confía de ninguna transacción iniciada por el Suscriptor y / o Parte que Confía que involucre el uso o la confianza en un Certificado.

Se entiende y es aceptado por los Suscriptores y las Partes que Confían que, al usar y / o confiar en un Certificado, son los únicos responsables de su confianza, y que tales partes deben considerar hechos, circunstancias y contexto de la transacción en la que el Certificado se utiliza para determinar dicha confianza.

Los Suscriptores y las Partes que Confían aceptan y reconocen que los Certificados tienen un período operativo limitado y se pueden revocar en cualquier momento. Los Suscriptores y las Partes que Confían están obligados a verificar si un Certificado expiró o se ha revocado. Los Afiliados de Entrust y de Entrust Group rechazan cualquier y toda responsabilidad frente a los Suscriptores y Partes que Confían que no sigan dichos procedimientos. Se puede encontrar más información sobre las situaciones en que puede revocarse un Certificado en la sección 4.9.9 de esta CPS.

9.8 Limitaciones de responsabilidad

9.8.1 La entera responsabilidad de Entrust Group bajo esta CPS para con: (i) un Solicitante o Suscriptor está establecida en el Acuerdo de Suscriptor entre Entrust (o un Afiliado de Entrust Group) y dicho Suscriptor; y (ii) una Parte que Confía está establecida en el acuerdo publicado en el repositorio en la fecha en la que la Parte que Confía confía en dicho Certificado. La responsabilidad total de Entrust Gruop ante cualquier otra parte está establecida en el (los) acuerdo (s) entre Entrust y dicha otra parte.

9.8.2 Sujeto a lo anterior y si el §9.8.1 anterior no aplica:
9.8.2.1 En la medida en que Entrust haya expedido el Certificado en cumplimiento con la CPS, Entrust Group no será responsable frente a cualquier persona de

cualquier reclamación, daños o pérdidas sufridas como resultado del uso o la confianza en dicho Certificado.

En ningún caso, Entrust group será responsable y todo posible demandante renuncia a cualquier derecho que pueda tener a cualquier daño consecuente, indirecto, especial, incidental, pena disciplinaria o ejemplar o por cualquier pérdida de negocios, oportunidades, contratos, ingresos, beneficios, ahorros buena voluntad, reputación, uso o datos, o costos de recuperación o interrupción comercial, o cualquier pérdida o daño que no sea atribuible directamente al uso o la confianza en un certificado o los servicios de certificados proporcionados bajo esta CPS incluyendo cualquier pérdida o daño resultante de la combinación o integración del Certificado o servicios del Certificado con cualquier software o hardware no proporcionado por Entrust si la pérdida o daño no habría ocurrido como resultado del uso del certificado o servicios del certificado solo.

9.8.2.2 En ningún caso la responsabilidad total agregada de entrust group que surja o esté relacionada con esta CPS y el uso y rendimiento de cualquier producto y servicio proporcionado excederá de mil dólares de estados unidos (US$ 1.000,00), o las cuotas pagadas por la parte reclamante a Entrust bajo esta CPS durante los doce meses antes del inicio de la reclamación, la cantidad que sea mayor, hasta un máximo de cien mil dólares americanos (US$ 100.000,00) (excepto que para cualquier Certificado cualificado de autenticación de sitio web de tipo eIDAS o Certificado Cualificado de Autenticación de Sitio Web de tipo PSD2 emitidos bajo esta CPS, la responsabilidad agregada de Entrust hacia cualquier Suscriptor o Parte que Confía y sus entidades está limitada a dos mil dólares de Estados Unidos (US$ 2.000,00) por Certificado, hasta un máximo de cien mil dólares de estados unidos (US$ 100.000,00)).

9.8.2.3 Las exclusiones y límites de esta sección (Limitaciones de Responsabilidad) se aplican: (a) independientemente de la forma de acción, ya sea en el contrato (incluyendo incumplimiento fundamental), agravio (incluyendo negligencia), garantía, incumplimiento de deberes legales, responsabilidad, responsabilidad estricta del producto, o de otro modo; (b) sobre una base agregada, independientemente del número de reclamaciones, transacciones, firmas digitales o Certificados; (c) incluso si la posibilidad de los daños en cuestión fue conocida o comunicada con anticipación e incluso si dichos daños fueron previsibles; y (d) incluso si los recursos no cumplen con su propósito esencial. Entrust ha fijado sus precios y proporciona certificados en función de las exclusiones y límites de esta sección (Limitaciones de Responsabilidad), que forman una base esencial de la provisión de los servicios descritos en esta CPS.

9.8.2.4 En ningún caso Entrust o sus Afiliadas serán responsables ante los Suscriptores, las Partes que Confían o cualquier otra persona, entidad u organización por pérdidas, costos, gastos, responsabilidades, daños, reclamaciones o

liquidaciones que surjan o estén relacionados con el uso o uso indebido o dependencia de cualquier Certificado emitido bajo esta CPS que: (i) haya vencido o haya sido revocado; (ii) se haya utilizado para cualquier otro propósito que no sea el establecido en esta CPS o un Acuerdo de Suscriptor aplicable; (iii) haya sido manipulado; (iv) con respecto al cual el Par de Claves subyacente a dicho Certificado o el algoritmo criptográfico utilizado para generar el Par de Claves de dicho Certificado, se ha visto comprometido por la acción de cualquier parte que no sea Entrust o sus Afiliados (incluido, entre otros, el Suscriptor o la Parte que Confía) ; o (v) es objeto de tergiversaciones u otros actos u omisiones engañosos de cualquier otra parte, incluidos, entre otros, los Suscriptores y las Partes que Confían. Excepto en la medida en que se disponga expresamente en esta CPS o en un Acuerdo de Suscriptor o Acuerdo de Parte que Confía, en ningún caso Entrust o sus Afiliados serán responsables ante el Suscriptor, la Parte que Confía u otra parte por los daños que surjan de cualquier reclamación de que el contenido de un Certificado infringe cualquier patente, marca comercial, derecho de autor, secreto comercial u otro derecho de propiedad intelectual de cualquier parte.

9.8.2.5 Sin perjuicio de cualquier disposición en contrario en esta Sección (Limitación de Responsabilidad) o en otra parte del Acuerdo, en la medida en que lo requiera la ley aplicable, Entrust no excluye ni limita su responsabilidad por: (i) muerte o lesiones corporales causadas por su propia negligencia; (ii) su propio fraude o tergiversación fraudulenta; o (iii) otros asuntos por los cuales la responsabilidad no puede ser excluida o limitada bajo la ley aplicable.

9.9 Indemnizaciones

9.9.1 Indemnización de las CA.

Entrust defenderá, indemnizará y mantendrá indemne a todo Proveedor de Aplicaciones de Software de cualquier y todas las reclamaciones, daños y pérdidas de terceros sufridos por dicho Proveedor de Aplicaciones de Software relacionados con un Certificado emitido por la CA que no cumpla con los Requisitos de Referencia vigentes en el momento en el que el Certificado fue emitido, independientemente de la causa de la acción o la jurisprudencia involucrada. Esto no se aplica, sin embargo, ante cualquier reclamación, daño o pérdida sufrida por dicho Proveedor de Aplicaciones de Software relacionado con un Certificado emitido por la CA cuando dicha reclamación, daño o pérdida fuese directa o indirectamente causada por el software de dicho Proveedor de Aplicaciones de Software al mostrar como no fiable un Certificado que aún es válido, o al mostrar como fiable: (1) un Certificado que ha caducado, o (2) un Certificado que ha sido revocado (pero solo en casos en que el estado de revocación está disponible en ese momento en línea desde la CA, y el software de la aplicación no pudo verificar dicho estado o ignoró una indicación de estado revocado).

9.9.2 Indemnización de las Partes que Confían

Las Partes que Confían deben indemnizar y mantener indemnes a Entrust Group y a todas las autoridades de registro de terceros independientes que funcionan bajo una autoridad de certificación, y a todos los proveedores de aplicaciones de software, (colectivamente, las "partes indemnizadas") ante cualquier y todas las cargas, pérdidas, costos, gastos, daños, reclamaciones y liquidaciones (incluidas cuotas razonables de abogado, costas de tribunal y cuotas de expertos) que surjan o estén relacionados con cualquier uso o confianza de una Parte que Confía en cualquier Certificado o cualquier servicio proporcionado con respecto a los Certificados, incluyendo (i) falta de validación apropiada de un Certificado por una Parte que Confía, (ii) confianza por parte de una Parte que Confía en un Certificado expirado o revocado, (iii) uso de un Certificado distinto al que se permite por la CPS, el Acuerdo de Suscriptor, cualquier acuerdo de Parte que Confía y ley aplicable, (iv) falta de una Parte que Confía al ejercer una interpretación razonable de las circunstancias en relación con un Certificado, o (v) cualquier reclamación o alegación de que la confianza por parte de una Parte que Confía en el Certificado o la información contenida en un Certificado infringe, malversa, diluye, o compite de forma desleal, o de otra manera viola los derechos incluyendo derechos de propiedad intelectual o cualquier otro derecho de cualquiera en cualquier jurisdicción. Sin perjuicio de lo anterior, las Partes que Confían no estarán obligadas a proporcionar indemnización alguna a una parte indemnizada respecto a cualquier responsabilidad, pérdidas, costos, gastos, daños, reclamaciones, y liquidaciones (incluyendo cuotas razonables de abogado, costas de tribunal y cuotas de expertos) en la medida en que tales responsabilidades, pérdidas, costos, gastos, daños, reclamaciones y liquidaciones (incluyendo cuotas razonables de abogados, costas de tribunal y cuotas de expertos) se deriven o se relacionen con cualquier mala praxis deliberada de dicha parte indemnizada.

9.9.3 Indemnización de los Suscriptores

A menos que se indique lo contrario en un Acuerdo de Suscriptor, los Suscriptores deberán indemnizar y mantener indemne a Entrust Group y a todas las autoridades de registro de terceros independientes que funcionan bajo una autoridad de certificación, y a todos los proveedores de aplicaciones de software, (colectivamente, las "partes indemnizadas") ante cualquier y todas las responsabilidades, pérdidas, costos, gastos, daños, reclamaciones y liquidaciones (incluidas cuotas razonables de abogado, costas de tribunal y cuotas de expertos) que surjan o estén relacionados con cualquier Parte que Confía en cualquier Certificado o cualquier servicio proporcionado con respecto a los Certificados, incluyendo cualquier (i) error, falta de representación o de omisión realizada por un Suscriptor al usar o solicitar un Certificado, (ii) modificación realizada por un Suscriptor de la información contenida en un Certificado, (iii) uso de un Certificado para otro propósito que no sea permitido por la CPS, por el Acuerdo de Suscriptor, o por cualquier acuerdo de Parte que Confía, y por la ley aplicable, (iv) fallo de un Suscriptor al tomar las necesarias precauciones para evitar la pérdida, divulgación, compromiso o uso no autorizado de la clave privada correspondiente a la clave

pública del Certificado de dicho Suscriptor, o (v) alegación de que el uso del Certificado de Suscriptor o la información contenida en el Certificado de Suscriptor infringe, malversa, diluye, compite de forma desleal o de otra manera viola los derechos, incluyendo derechos de propiedad intelectual o cualquier otro derecho de cualquiera en cualquier jurisdicción. Sin perjuicio de lo anterior, un Suscriptor no estará obligado a proporcionar indemnización alguna a una parte indemnizada respecto de ninguna responsabilidad, pérdidas, costos, gastos, daños, reclamaciones, y liquidaciones (incluyendo cuotas razonables de abogado, costas de tribunal y cuotas de expertos) en la medida en que tales responsabilidades, pérdidas, costos, gastos, daños, reclamaciones y liquidaciones (incluyendo cuotas razonables de abogado, costas de tribunal y cuotas de expertos) se deriven o se relacionen con cualquier mala praxis deliberada de tal parte indemnizada.

9.10 Período de validez y derogación

9.10.1 Período de validez
Esta CPS entrará en vigor en la fecha en que esta CPS se publique en el Repositorio y continuará vigente hasta que se publique una nueva versión de la CPS.

9.10.2 Derogación
Esta CPS permanecerá vigente hasta que sea reemplazada por una nueva versión.

9.10.3 Efecto de la derogación y supervivencia
Las disposiciones de las secciones 1.6, 3.1.6, 5.5, 9.1, 9.3, 9.4, 9.5, 9.7, 9.8, 9.9.2, 9.9.3, 9.10.3, 9.13, 9.14 y 9.16 seguirán vigentes tras la derogación o vencimiento de la CPS, cualquier Acuerdo de Suscriptor y cualquier Acuerdo de Parte que Confía. Todas las referencias a las secciones que sigan vigentes tras la finalización de la CPS, cualquier Acuerdo de Suscriptor y cualquier Acuerdo de Parte que Confía deberán incluir todas las subsecciones de dichas secciones. Todas las obligaciones de pago seguirán vigentes tras cualquier derogación o vencimiento de la CPS, cualquier Acuerdo de Suscriptor y cualquier Acuerdo de Parte que Confía.

9.11 Avisos individuales y comunicaciones con los participantes.
A menos que se establezca lo contrario en un Acuerdo de Suscriptor o un Acuerdo de Parte que Confía, cualquier notificación que se envíe a Entrust en virtud de esta CPS, un Acuerdo de Suscriptor o un Acuerdo de Parte que Confía se realizará por escrito a la dirección especificada en §1.5.2 por correo con acuse de recibo, mensajería o correo electrónico, y se hará efectiva de la siguiente manera (i) en caso de mensajería o correo electrónico, al siguiente día hábil, y (ii) en caso de correo con acuse de recibo, al quinto día hábil posterior a la fecha de envío. Cualquier notificación que realice Entrust en virtud de la CPS, o un Acuerdo de Suscriptor deberá enviarse por correo electrónico o mensajería a la última dirección o dirección de correo electrónico del Suscriptor que figure en el archivo de Entrust.

9.12 Enmiendas

9.12.1 Procedimiento de enmienda
Entrust puede, de forma discrecional, modificar la CPS y los términos y condiciones contenidos en este documento periódicamente. Entrust modificará la CPS para mantenerla coincidente con la última versión de los Requisitos de Referencia, Guías EV SSL y Guías ETSI.

9.12.2 Mecanismo de notificación y período
Las modificaciones de la CPS se publicarán en el Repositorio. Dichas notificaciones causarán efecto en el mismo momento de su publicación en el Repositorio, y seguirán siendo válidas mientras dure dicha publicación. En el caso de que Entrust realice una modificación significativa de la CPS, se actualizará el número de versión de la CPS. A menos que un Suscriptor deje de usar, elimine y solicite la revocación de dicho(s) Certificado(s) de Suscriptor(es) antes de la fecha en que una versión actualizada de la CPS entre en vigor, se considerará que dicho Suscriptor ha dado su consentimiento a los términos y condiciones de dicha versión actualizada de la CPS y estará sujeto a los términos y condiciones de dicha versión actualizada de la CPS.

9.12.3 Circunstancias bajo las cuales se debe cambiar el OID
No está estipulado.

9.13 Disposiciones de resolución de conflictos
A menos que se establezca lo contrario en un Acuerdo de Suscriptor o Acuerdo de Parte que Confía, y excepto por el derecho de cualquiera de las Partes a solicitar a un tribunal de jurisdicción competente una medida cautelar u otra reparación equitativa, cualquier conflicto o reclamación entre un Suscriptor o un Solicitante y Entrust o cualquier RA de terceros que opere bajo las CA, o una Parte que Confía y Entrust o cualquier RA de terceros que opere bajo las CA, deberá enviarse a la Corte Internacional de Arbitraje de la Cámara de Comercio Internacional y será finalmente resuelto bajo el Reglamento de Arbitraje de la Cámara de Comercio Internacional por uno o más árbitros designados de acuerdo con dicho Reglamento. El idioma que se utilizará en el arbitraje será el español. La sede del arbitraje será España. El árbitro tendrá derecho a decidir todas las cuestiones de arbitrabilidad. El conflicto se resolverá finalmente mediante arbitraje de acuerdo con el Reglamento de Arbitraje de la Cámara de Comercio Internacional. El árbitro deberá presentar una decisión escrita dentro de los treinta (30) días a partir de la fecha de cierre de la audiencia de arbitraje, pero dentro del año a partir de la fecha en la que el asunto fue sometido a arbitraje. La decisión del árbitro será vinculante y concluyente y podrá ser registrada en cualquier tribunal de jurisdicción competente. En cada arbitraje, la parte ganadora tendrá derecho a la adjudicación de la totalidad o una parte de sus costos en dicho arbitraje, incluyendo los honorarios de abogados incurridos y razonables. Nada en la CPS, ni en ningún Acuerdo de Suscriptor, ni en ningún Acuerdo de Parte que Confía impedirá a Entrust o cualquier RA de terceros que opere bajo las CA solicitar

a cualquier tribunal de la jurisdicción competente un recurso cautelar temporal o permanente, sin infracción de esta §9.13 y sin ninguna restricción de los poderes del árbitro, con respecto a cualquier (i) presunto Compromiso que afecte la integridad de un Certificado, o (ii) presunto incumplimiento de los términos y condiciones de la CPS, cualquier Acuerdo de Suscriptor o cualquier Acuerdo de Parte que Confía. La institución de cualquier arbitraje o cualquier acción no eximirá a un Solicitante, Suscriptor o Parte que Confía de sus obligaciones según la CPS, cualquier Acuerdo de Suscriptor, o cualquier Acuerdo de Parte que Confía.

Todos y cada uno de los arbitrajes o acciones legales con respecto a un conflicto relacionado con un Certificado o cualquier servicio proporcionado con respecto a un Certificado se iniciará antes del final de un (1) año después de (i) el vencimiento o revocación del Certificado en conflicto, o (ii) la fecha de prestación del servicio o servicios en conflicto con respecto al Certificado en conflicto, lo que ocurra primero. Si cualquier arbitraje o acción con respecto a un conflicto relacionado con un Certificado o cualquier servicio o servicios proporcionados con respecto a un Certificado no ha comenzado antes de ese tiempo, se impedirá a cualquier parte que busque instituir tal arbitraje o acción iniciar o proceder con dicho arbitraje o acción.

9.14 Ley aplicable

Cualquier conflicto relacionado con los Certificados emitidos bajo esta CPS y los servicios prestados con respecto a dichos Certificados, así como la construcción, validez, interpretación, exigibilidad y desempeño de la CPS, todos los Acuerdos de Suscriptor y todos los Acuerdos de Parte que Confía, si no se resuelve mediante una resolución alternativa de conflictos, se regirán por las leyes y se llevarán a los tribunales indicados en la sección Elección de la Ley del Acuerdo de Suscriptor o Acuerdo de la Parte que Confía correspondiente, y cada persona, entidad u organización acuerda que dichos tribunales tendrán jurisdicción personal y exclusiva sobre tales conflictos. En el caso de que cualquier asunto sea llevado ante un tribunal, los Solicitantes, Suscriptores y Partes que Confían renuncian a cualquier derecho que tales Solicitantes, Suscriptores y Partes que Confían pudiesen tener a un juicio con jurado. Se excluye expresamente la aplicación de la Convención de las Naciones Unidas sobre Contratos para la Venta Internacional de Bienes a la CPS, los Acuerdos de Suscriptor y los Acuerdos de Parte que Confía. Sin perjuicio de todo lo anterior, cualquier conflicto relacionado con los Certificados en virtud de esta CPS y los servicios prestados con respecto a dichos Certificados, si no se resuelve mediante una resolución alternativa de conflictos, se regirá por las leyes de España.

9.15 Cumplimiento de la ley aplicable

Entrust operará de manera legal y fiable. En particular, Entrust deberá cumplir con todos los requisitos legales aplicables (como el Reglamento General de Protección de Datos (GDPR)) manteniendo un departamento legal con personal competente y autorizado, que conozca todas las leyes y regulaciones aplicables, realice formación

legal continua sobre las nuevas leyes y reglamentos, actualice las políticas y prácticas internas de Entrust (incluida esta CPS) para cumplir con las leyes y reglamentos aplicables, y forme a otros empleados de Entrust (según corresponda) en todas las nuevas leyes y reglamentos relacionados con sus funciones y deberes.

Los certificados y la información relacionada pueden estar sujetos a restricciones de exportación, importación y / o uso. Los Suscriptores y las Partes que Confían cumplirán en todos los aspectos con todas y cada una de las leyes, normas y reglamentos aplicables y obtendrán todos los permisos, licencias y autorizaciones o certificados que puedan ser necesarios en relación con el ejercicio de sus derechos y obligaciones en virtud de cualquier parte de la CPS, Acuerdo de Suscriptor y / o Acuerdo de la Parte que Confía, incluido el uso o acceso por parte de cualquiera de los usuarios del Suscriptor o de la Parte que Confía. Sin limitar lo anterior, los Suscriptores y las Partes que Confían cumplirán con todas las leyes de control comercial aplicables, incluidas, entre otras, las sanciones o controles comerciales de la Unión Europea ("UE"), Canadá, el Reino Unido ("UK") y Naciones Unidas ("ONU"); las Regulaciones de la Administración de Exportaciones administradas por la Oficina de Industria y Seguridad del Departamento de Comercio de los Estados Unidos; Regulaciones de sanciones de EE. UU. Administradas por la Oficina de Control de Activos Extranjeros del Departamento del Tesoro de EE. UU. ("OFAC"); o en la Lista de entidades del Departamento de Comercio de EE. UU. ("Lista de entidades"); y cualquier licencia de importación o exportación requerida de conformidad con cualquiera de los anteriores; y todas las leyes aplicables contra el lavado de dinero, incluida la Ley de Secreto Bancario de EE. UU., la Ley de Control de Lavado de Dinero y la Ley Patriota, la Ley Canadiense de Activos del Crimen (Lavado de Dinero) y Financiamiento del Terrorismo, la Ley de Activos del Crimen del Reino Unido y la legislación que implementa el Convenio internacional para la represión de la financiación del terrorismo o las disposiciones sobre blanqueo de capitales de la Convención contra la Delincuencia Organizada transnacional de las Naciones Unidas. Cada Suscriptor y Parte que Confía declara y garantiza que: (a) ni él ni ninguno de sus usuarios está ubicado en, bajo el control de, o es un nacional o residente de cualquier país al que la exportación de cualquier software o tecnología con licencia bajo el Acuerdo , o información relacionada, estaría prohibida por las leyes, reglas o regulaciones aplicables de los EE. UU., Canadá, Reino Unido, UE u otra jurisdicción aplicable; (b) ni él ni ninguno de sus usuarios es una Persona a la que la exportación de cualquier software o tecnología con licencia en virtud del Acuerdo, o información relacionada, estaría prohibida por las leyes de los EE. UU., Canadá, Reino Unido, UE u otros aplicables jurisdicción; (c) él y cada uno de sus usuarios ha cumplido y cumplirá con las leyes, reglas y regulaciones aplicables de los EE. UU., Canadá, el Reino Unido, la UE u otras jurisdicciones aplicables y de cualquier estado, provincia o localidad o jurisdicción aplicable que gobierne exportaciones de cualquier producto o servicio proporcionado por Entrust o a través de él; (d) ni él ni todos sus usuarios utilizarán ningún producto o servicio para ningún propósito prohibido por las leyes, normas o

reglamentos aplicables sobre controles comerciales, incluidos los relacionados con la proliferación de armas nucleares, químicas o biológicas, el comercio de armas o el fomento de financiación terrorista; (e) ni él ni ninguno de sus usuarios ni ninguno de sus afiliados, funcionarios, directores o empleados es (i) una persona que figura en la lista, o que sea propiedad o esté controlada directa o indirectamente por una persona (ya sea legal o física) que figure en , o actuando en nombre de una Persona incluida en cualquier lista de sanciones de los EE. UU., Canadá, la UE, el Reino Unido o la ONU, incluida la lista de Nacionales Especialmente Designados de la OFAC o la Lista de Entidades; o (ii) ubicado en, incorporado bajo las leyes de, o que sea propiedad (es decir, 50% o más de participación en la propiedad) o que sea de otra manera, directa o indirectamente, controlado por, o actuando en nombre de, una persona ubicada en, residente u organizada según las leyes de cualquiera de los países enumerados en https://www.entrust.com/legal-compliance/denied-parties (cada uno de (i) y (ii), una "Parte Denegada"); y (f) él y cada uno de sus usuarios es legalmente distinto y no un agente de cualquier Parte Denegada. En el caso de que cualquiera de las declaraciones y garantías anteriores sea incorrecta o el Suscriptor, la Parte que Confía o cualquiera de sus usuarios se involucre en cualquier conducta que sea contraria a las sanciones o controles comerciales u otras leyes, regulaciones o reglas aplicables, cualquier acuerdo, orden de compra, la prestación de servicios u otras obligaciones contractuales de Entrust se rescinden de inmediato.

9.16 Otras disposiciones

9.16.1 Acuerdo completo
No está estipulado.

9.16.2 Asignación
Los Certificados y los derechos otorgados en virtud de la CPS, cualquier Acuerdo de Suscriptor o cualquier Acuerdo de Parte que Confía son personales del Solicitante, el Suscriptor o la Parte que Confía que entró en el Acuerdo de Suscriptor o Acuerdo de Parte que Confía y no pueden ser asignados, vendidos, transferidos o de otra manera eliminados, ya sea voluntariamente, involuntariamente, por ley o de otra manera, sin el consentimiento previo por escrito de Entrust o de la pertinente RA bajo una CA. Cualquier intento de asignación o transferencia sin dicho consentimiento será nulo y automáticamente se rescindirán los derechos de dicho Solicitante, Suscriptor o Parte que Confía de acuerdo con la CPS, cualquier Acuerdo de Suscriptor, o cualquier Acuerdo de Parte que Confía. Entrust puede ceder, vender, transferir o deshacerse de cualquier otro modo de la CPS, los Acuerdos de Suscriptor o los Acuerdos de Parte que Confía, junto con todos sus derechos y obligaciones según la CPS, cualquier Acuerdo de Suscriptor y cualquier Acuerdo de Parte que Confía (i) a un Afiliado, o (ii) como parte de una venta, fusión u otra transferencia de todos los activos o una parte sustancial de los activos o acciones del negocio de Entrust relacionados con la CPS, los Acuerdos de Suscriptor y la Parte que Confía. Sujeto a los límites anteriores, esta CPS y los términos y condiciones de

cualquier Acuerdo de Suscriptor, o cualquier Acuerdo de la Parte que Confía serán vinculantes y se aplicarán en beneficio de los sucesores y cesionarios permitidos de Entrust, cualquier RA de terceros que opere bajo las CA, Solicitantes, Suscriptores y Partes que Confían, según sea el caso.

La CPS, los Acuerdos de Suscriptor y los Acuerdos de Parte que Confía establecen todos los derechos y obligaciones de Entrust Group, cualquier Solicitante, Suscriptor o Parte que Confía y cualquier otra persona, entidades u organizaciones con respecto a la materia objeto del presente documento y tales derechos y obligaciones no serán aumentados o derogados por ningún acuerdo previo, comunicación o entendimiento de cualquier naturaleza ya sea oral o escrito. Los derechos y obligaciones de Entrust Group no pueden ser modificados o renunciados oralmente y solo pueden ser modificados en un escrito firmado o autenticado por un representante autorizado de Entrust.

9.16.3 Divisibilidad

Siempre que sea posible, cada disposición de la CPS, los Acuerdos de Suscriptor y cualquier Acuerdo de Parte que Confía, se interpretarán de manera tal que sean efectivos y válidos según la ley aplicable. Si un árbitro o tribunal de jurisdicción competente considera que la aplicación de cualquier disposición de la CPS, Acuerdo de Suscriptor o Acuerdo de Parte que Confía o cualquier parte de la misma ante cualquier hecho o circunstancia particular es inválida o inaplicable, entonces (i) la validez y exigibilidad de tal disposición aplicada a cualquier otro hecho o circunstancia particular y la validez de otras disposiciones de la CPS, cualquier Acuerdo de Suscriptor o cualquier Acuerdo de Parte que Confía no se verán afectadas ni deterioradas de ninguna manera, y (ii) dicha disposición se aplicará en la mayor medida de lo posible a fin de lograr su propósito y se reformará sin más acciones en la medida necesaria para que dicha disposición sea válida y ejecutable.

9.16.4 Cumplimiento

No está estipulado.

9.16.5 Fuerza mayor

En ningún caso se considerará a Entrust Group en incumplimiento o responsable de cualquier pérdida o daño resultante del incumplimiento o demora en el cumplimiento de sus obligaciones en virtud de la CPS, cualquier Acuerdo de Suscriptor o cualquier Acuerdo de Parte que Confía, que surja o sea causado por , directa o indirectamente, un Evento de Fuerza Mayor. "Evento de fuerza mayor" significa cualquier evento o circunstancia más allá del control razonable de Entrust Group, incluidos, entre otros, inundaciones, incendios, huracanes, terremotos, tornados, epidemias, pandemias, otros actos fortuitos o de la naturaleza, huelgas y otras disputas laborales, fallos de infraestructura de servicios públicos, transporte o comunicaciones, disturbios u otros actos de desorden civil, actos de guerra, terrorismo (incluido el terrorismo cibernético), daño malicioso, acción judicial, falta o incapacidad para obtener

permisos o aprobaciones de exportación, actos de gobierno como la expropiación, condena, embargo, cambios en las leyes o regulaciones aplicables y órdenes de quedarse en casa o similares, y actos o incumplimientos de proveedores externos o proveedores de servicios.

9.17 Otras provisiones

9.17.1 Conflicto de disposiciones

En caso de cualquier inconsistencia entre las disposiciones de esta CPS y las disposiciones de cualquier Acuerdo de Suscriptor o cualquier Acuerdo de Parte que Confía, regirán los términos y condiciones de esta CPS.

9.17.2 Relaciones fiduciarias

Nada de lo contenido en esta CPS, ni en ningún Acuerdo de Suscriptor, ni en ningún Acuerdo de Parte que Confía, se considerará que constituye a Entrust Group como fiduciario, socio, agente, administrador o representante legal de ningún Solicitante, Suscriptor, Parte que Confía o cualquier otra persona, entidad u organización, o que crea relación fiduciaria alguna entre Entrust Group y cualquier Suscriptor, Solicitante, Parte que Confía o cualquier otra persona, entidad u organización, para cualquier propósito. Nada en la CPS, ni en ningún Acuerdo de Suscriptor o Acuerdo de Parte que Confía confiere a ningún Suscriptor, Solicitante, Parte que Confía, o cualquier otro tercero, ninguna autoridad para actuar, vincular, crear o asumir cualquier obligación o responsabilidad, o hacer representación alguna en nombre de Entrust Group.

9.17.3 Exención

La falta de exigencia por parte de Entrust del cumplimiento, en cualquier momento, de cualquiera de las disposiciones de esta CPS, un Acuerdo de Subscriptor con Entrust, o un Acuerdo de Parte que Confía con Entrust o en caso de que Entrust no requiera, en cualquier momento, el cumplimiento por parte de cualquier Solicitante, Suscriptor, Parte que Confía o cualquier otra persona, entidad u organización de cualquiera de las disposiciones de esta CPS, un Acuerdo de Suscriptor con Entrust, o una Parte que Confía con Entrust, no se interpretará en modo alguno como una presente o futura exención de tales disposiciones, ni afectará de ninguna manera a la capacidad de Entrust de hacer cumplir todas y cada una de esas disposiciones a partir de entonces. La exención expresa por parte de Entrust de cualquier disposición, condición o requisito de esta CPS, un Acuerdo de Suscriptor con Entrust o un Acuerdo de Parte que Confía con Entrust no constituirá una exención de ninguna obligación futura de cumplir con tal disposición, condición o requisito.

9.17.4 Interpretación

Todas las referencias en esta CPS a "sección" o "§" se refieren a las secciones de esta CPS a menos que se indique lo contrario. En esta CPS, los pronombres masculinos o neutros y cualquier variación de los mismos se considerará que

incluyen el femenino y masculino y todos los términos utilizados en singular se considerará que incluyen el plural, y viceversa, según el contexto. Las palabras "aquí", "aquí", y "a continuación" y otras palabras de relevancia similar se refieren a esta CPS en su conjunto, ya que la misma puede ser enmendada o complementada periódicamente, y no a ninguna subdivisión contenida en esta CPS. La palabra "incluido" tal como se usa en este documento no pretende ser exclusiva y significa "incluido, sin limitación".

Apéndice A - Perfiles de Certificados

Certificado de CA Raíz

Campo de Certificado CA Raíz	Crítico	Contenido
Emisor		Debe coincidir con el Sujeto
Sujeto		Debe contener nombre de país, nombre de organización y nombre común
Extensión: subjectKeyIdentifier	No crítico	hash SHA-1 de 160 bits de subjectPublicKey según RFC 5280
Extensión: basicConstraints	Crítico	cA es VERDADERO; pathLenConstraint no está presente
Extensión: keyUsage	Crítico	Los bits keyCertsign y cRLSign están configurados digitalSignature si Raíz firma respuestas OCSP

Certificado Cruzado o Certificado de CA Subordinada

Campo	Crítico	Contenido
Validez: notAfter		No más tarde que la fecha "notAfter" (no después) del certificado de firma
Sujeto		Debe contener countryName, organizationName y commonName y puede contener organizationIdentifier
Extensión: subjectKeyIdentifier	No crítico	hash SHA-1 de 160 bits de subjectPublicKey según RFC 5280
Extensión: authorityKeyIdentifier	No crítico	Coincide con subjectKeyIdentifier del certificado de firma
Extensión: CertificatePolicies	No crítico	Debe contener al menos un conjunto de policyInformation que contenga al menos un policyIdentifier
Extensión: basicConstraints	Crítico	cA es VERDADERO
Extensión: keyUsage	Crítico	Los bits keyCertsign y cRLSign están configurados digitalSignature si CA firma respuestas OCSP
Extensión: extKeyUsage	No crítico	Debe estar presente cuando se asocia con raíces públicas de confianza
Extensión: authorityInfoAccess	No crítico	Debe contener una AccessDescription con un accessMethod of caIssuers y una ubicación de tipo UniformResourceIdentifier y una AccessDescription con un accessMethod de ocsp y una ubicación de tipo uniformResourceIdentifier
Extensión: cRLDistributionPoints	No crítico	Debe tener al menos un DistributionPoint que contenga un fullName de tipo uniformResourceIdentifier

Certificado Cualificado de Firma Electrónica de tipo eIDAS (QCP-n-qscd)

Campo		**Contenido**
Atributos		
Versión		V3
Número de Serie		Número único con entropía de 64 bits
Algoritmo de firma del emisor		sha-512
DN del emisor		CN = Entrust Certification Authority – ES QSig2 OrganizationIdentifier = VATES-B81188047 O = Entrust EU, S.L. C = ES
Validez: Período		Se especifica notBefore y notAfter <= 3 años
DN de Sujeto		CN = <nombre común que el sujeto usa habitualmente para representarse a sí mismo> serialNumber (2.5.4.5) = <número de identidad unívoco> givenName (2.5.4.42) = <nombre de pila validado> surname (2.5.4.4) = <apellido validado> OU = <unidad organizativa del suscriptor > (opcional) O = <Nombre legal completo del suscriptor > L = <localidad del suscriptor > (opcional) S = <estado o provincia del suscriptor > (opcional) C = <país del Suscriptor >
Información de Clave Pública del Sujeto		2048-bit RSA key modulus rsaEncryption {1.2.840.113549.1.1.1}
Extensión	**Crítico**	**Valor**
Identificador de clave de autoridad	No	Hash de la Clave Pública de CA
Identificador de clave de Sujeto	No	Hash del subjectPublicKey en este certificado
Uso de clave	Yes	nonRepudiation, digitalSignature
Uso de clave extendida	No	Document Signing (1.3.6.1.4.1.311.10.3.12) Adobe Authentic Documents Trust (1.2.840.113583.1.1.5) Client Authentication (1.3.6.1.5.5.7.3.2)
Políticas de certificado	No	[1] Política de certificado: Identificador de política = 2.16.840.1.114028.10.1.12.2 [1,1] Información de calificadores de política Id. del calificador de política =CPS Calificador: https://www.entrust.net/rpa [2] Política de certificado: Identificador de política =0.4.0.194112.1.2 [3] Política de certificado: Identificador de política =2.16.840.1.114028.10.1.6
Restricciones Básicas	Sí	Tipo de Sujeto = entidad final Restricción de longitud de ruta = Ninguna
Acceso a la información de la autoridad		[1] Acceso a la información de la autoridad Método de acceso = Protocolo de estado del certificado en línea (1.3.6.1.5.5.7.48.1) Nombre alternativo: uri = http: //ocsp.entrust.net [2] Acceso a la información de la autoridad

		Método de acceso = Emisor de la autoridad de certificación (1.3.6.1.5.5.7.48.2) Nombre alternativo: URL = http://aia.entrust.net/esqsig2-chain.p7c
Puntos de distribución de CRL	No	uri: http://crl.entrust.net/esqsig2ca.crl
Archive Rev Info (1.2.840.113583.1.1.9.2)	No	30 03 02 01 01
Time-stamp (1.2.840.113583.1.1.9.1)	No	URI = http://timestamp.entrust.net/TSS/RFC3161sha2TS Authentication = Not Required
qcStatements	**Crítico**	**Valor**
id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)	No	id-etsi-qcs-1 (0.4.0.1862.1.1) esi4-qcStatement-1: Afirma que el certificado es un certificado calificado de la UE de acuerdo con el Reglamento UE no 910/2014
id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)	No	id-etsi-qcs-4 (0.4.0.1862.1.4) esi4-qcStatement-1: La clave privada relacionada con la clave pública certificada reside en un QSCD de acuerdo con el Reglamento UE No 910/2014
id-etsi-qcs-QcType (0.4.0.1862.1.6)	No	id-etsi-qcs-6 (0.4.0.1862.1.6) esi4-qcStatement-6 : Type of certificate id-etsi-qcs-QcType 1 = Certificado para firma electrónica tal como se define en el Reglamento UE No 910/2014
id-etsi-qcs-QcPDS (0.4.0.1862.1.5)	No	id-etsi-qcs-5 (0.4.0.1862.1.5) URL= https://www.entrust.net/rpa Idioma = en

Certificado Cualificado de Sello Electrónico de tipo eIDAS (dispositivo criptográfico seguro)

Campo		**Contenido**
Atributos		
Versión		V3
Número de Serie		Número único para el dominio PKI
Algoritmo de firma del emisor		sha-512
DN del emisor		CN = Entrust Certification Authority – ES QSeal2 OrganizationIdentifier = VATES-B81188047 O = Entrust EU, S.L. C = ES
Validez: Período		Se especifica notBefore y notAfter <= 3 years
DN de Sujeto		CN = <nombre común usado habitualmente por el sujeto para representarse a sí mismo> OU = <unidad organizativa del suscriptor > (opcional) OrgID = < identificador de la organización> O = <Nombre legal completo del suscriptor > L = <localidad del suscriptor > (opcional) S = <estado o provincia del suscriptor > (opcional) C = <país del suscriptor>
Información de clave pública del Sujeto		2048 o 4096-bit RSA key modulus rsaEncryption {1.2.840.113549.1.1.1}
Extensión:	**Crítico**	**Valor**
Identificador de clave de autoridad	No	Hash de la Clave Pública de CA

Identificador de clave de Sujeto	No	Hash del subjectPublicKey en este certificado
Uso de clave	Yes	Non Repudiation
Uso de clave extendida	No	Document Signing (1.3.6.1.4.1.311.10.3.12) Adobe Authentic Documents Trust (1.2.840.113583.1.1.5)
Políticas de certificado	No	[1] Política de certificado: Identificador de política = 2.16.840.1.114028.10.1.12.1 [1.1] Información de calificadores de política Id. del calificador de política = CPS Calificador: https://www.entrust.net/rpa [2] Política de certificado: Identificador de política =0.4.0.194112.1.1 [3] Política de certificado: Identificador de política =2.16.840.1.114028.10.1.6
Restricciones Básicas	No	Tipo de Sujeto = entidad final Restricción de longitud de ruta = Ninguna
Acceso a la información de la autoridad	No	[1] Acceso a la información de la autoridad Método de acceso = Protocolo de estado del certificado en línea (1.3.6.1.5.5.7.48.1) Nombre alternativo: uri = http: //ocsp.entrust.net [2] Acceso a la información de la autoridad Método de acceso = Emisor de la autoridad de certificación (1.3.6.1.5.5.7.48.2) Nombre alternativo: URL = http://aia.entrust.net/esqseal2-chain.p7c
Puntos de distribución de CRL	No	uri: http://crl.entrust.net/esqseal2ca.crl
qcStatements	**Crítico**	**Valor**
id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)	No	id-etsi-qcs-1 (0.4.0.1862.1.1) esi4-qcStatement-1: afirma que el certificado es un certificado calificado de la UE de acuerdo con el Reglamento UE no 910/2014
id-etsi-qcs-QcType (0.4.0.1862.1.6)	No	id-etsi-qcs-6 (0.4.0.1862.1.6) esi4-qcStatement-6: Tipo de certificado id-etsi-qcs-QcType 2 = Certificado para sello electrónico tal como se define en el Reglamento UE No 910/2014
id-etsi-qcs-QcPDS (0.4.0.1862.1.5)	No	id-etsi-qcs-5 (0.4.0.1862.1.5) URL= https://www.entrust.net/rpa Idioma = en

Certificado Cualificado de Sello Electrónico de tipo PSD2

Campo		**Contenido**
Atributos		
Versión		V3
Número de Serie		Número único para el dominio PKI
Algoritmo de firma del emisor		sha-512
DN del emisor		CN = Entrust Certification Authority – ES QSeal2 OrganizationIdentifier = VATES-B81188047 O = Entrust EU, S.L. C = ES
Validez: Período		Se especifica notBefore y notAfter <= 3 years
DN de Sujeto		CN = <nombre común usado habitualmente por el sujeto para representarse a sí mismo> OU = <unidad organizativa del suscriptor > (opcional) OrgID = < identificador de la organización> O = <Nombre legal completo del suscriptor > L = <localidad del suscriptor > (opcional) S = <estado o provincia del suscriptor > (opcional) C = <país del suscriptor>
Información de clave pública del Sujeto		2048, 3072 o 4096 bits RSA key modulus rsaEncryption {1.2.840.113549.1.1.1}
Extensión:	**Crítico**	**Valor**
Identificador de clave de autoridad	No	Hash de la Clave Pública de CA
Identificador de clave de Sujeto	No	Hash del subjectPublicKey en este certificado
Uso de clave	Yes	Non Repudiation
Uso de clave extendida	No	Document Signing (1.3.6.1.4.1.311.10.3.12) Adobe Authentic Documents Trust (1.2.840.113583.1.1.5)
Políticas de certificado	No	[1] Política de certificado: Identificador de política = 2.16.840.1.114028.10.1.12.5 [1.1] Información de calificadores de política Id. del calificador de política = CPS Calificador: https://www.entrust.net/rpa [2] Política de certificado: Identificador de política =0.4.0.194112.1.1
Restricciones Básicas	No	Tipo de Sujeto = entidad final Restricción de longitud de ruta = Ninguna
Acceso a la información de la autoridad	No	[1] Acceso a la información de la autoridad Método de acceso = Protocolo de estado del certificado en línea (1.3.6.1.5.5.7.48.1) Nombre alternativo: uri = http: //ocsp.entrust.net [2] Acceso a la información de la autoridad Método de acceso = Emisor de la autoridad de certificación (1.3.6.1.5.5.7.48.2) Nombre alternativo: URL = http://aia.entrust.net/esqseal2-chain.p7c
Puntos de distribución de CRL	No	uri: http://crl.entrust.net/esqseal2ca.crl
qcStatements	**Crítico**	**Valor**
id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)	No	id-etsi-qcs-1 (0.4.0.1862.1.1) esi4-qcStatement-1: afirma que el certificado es un certificado calificado de la UE de acuerdo con el Reglamento UE no 910/2014

id-etsi-qcs-QcType (0.4.0.1862.1.6)	No	id-etsi-qcs-6 (0.4.0.1862.1.6) esi4-qcStatement-6: Tipo de certificado id-etsi-qcs-QcType 2 = Certificado para sello electrónico tal como se define en el Reglamento UE No 910/2014
id-etsi-qcs-QcPDS (0.4.0.1862.1.5)	No	id-etsi-qcs-5 (0.4.0.1862.1.5) URL= https://www.entrust.net/rpa Idioma = en
id-etsi-psd2-qcStatement (0.4.0.19495.2)	No	(SOLO para PSD2 según ETSI TS 119 495, 5.1) PSD2QcType ::= SEQUENCE{ rolesOfPSP RolesOfPSO, nCAName NCAName, nCAId NCAId}

Certificado Cualificado de Autenticación de Sitio Web de tipo eIDAS

Campo		**Contenido**
Atributos		
Versión		V3
Número de Serie		Número único para el dominio PKI
Algoritmo de firma del emisor		sha-256
DN del emisor		CN = Entrust Certification Authority – ES QWAC2 OrganizationIdentifier = VATES-B81188047 O = Entrust EU, S.L. C = ES
Validez: Período		Se especifica notBefore y notAfter
DN de Sujeto		CN = <DNS nombre del servidor seguro> serialNumber=<número de registro del Suscriptor > businessCategory=<EV categoría de negocio> OU = <unidad organizativa del Suscriptor > (opcional) O = <Nombre legal completo del Suscriptor > jurisdictionOfIncorporationLocalityName (si aplica) = <jurisdicción o localidad de registro del Suscriptor > jurisdicationOfIncorporationStateOrProvinceName (si aplica) = < jurisdicción o estado o provincia de registro del Suscriptor > jurisdicationOfIncorporationCountry = < jurisdicción o país de registro del Suscriptor> L = <localidad del Sujeto > (opcional) S = <estado o provincia del Sujeto > (si aplica) C = <país del Sujeto>
Información de clave pública del Sujeto		Módulo clave RSA de 2048, 3072 o 4096 bits rsaEncryption {1.2.840.113549.1.1.1}
Extensión:	**Crítico**	**Valor**
Identificador de clave de autoridad	No	Hash de la Clave Pública de CA
Identificador de clave de Sujeto	No	Hash del subjectPublicKey en este certificado
Nombre alternativo de sujeto	No	Nombre(s) DNS del servidor seguro
Transparencia de certificado	No	(1.3.6.1.4.1.11129.2.4.2) PUEDE incluir dos o más pruebas de Transparencia de Certificado de logs CT aprobados
Uso de clave	Yes	Digital Signature Key encipherment
Uso de clave extendida	No	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)
Políticas de certificado	No	[1] Política de certificado: Identificador de política = 2.16.840.1.114028.10.1.12.4 [1,1] Información de calificadores de política Id. del calificador de política = CPS Calificador: https://www.entrust.net/rpa [2] Política de certificado: Identificador de política =0.4.0.194112.1.4 [3] Política de certificado: Identificador de política =2.16.840.1.114028.10.1.2 [4] Política de certificado: Identificador de política = 2.23.140.1.1
Restricciones Básicas	No	Tipo de Sujeto = entidad final Restricción de longitud de ruta = Ninguna

Acceso a la información de la autoridad	No	• Método de acceso = Protocolo de estado del certificado en línea (1.3.6.1.5.5.7.48.1) Nombre alternativo: URL = http: //ocsp.entrust.net • Método de acceso = Emisor de la autoridad de certificación (1.3.6.1.5.5.7.48.2) Nombre alternativo: URL = http://aia.entrust.net/ esqwac2-chain.cer
Puntos de distribución de CRL	No	uri: http://crl.entrust.net/ esqwac2ca.crl
qcStatements	**Crítico**	**Valor**
id-etsi-qcs-QcCompliance	No	id-etsi-qcs-1 (0.4.0.1862.1.1) esi4-qcStatement-1: afirma que el certificado es un certificado calificado de la UE de acuerdo con el Reglamento UE no 910/2014
id-etsi-qcs-QcType	No	id-etsi-qcs-6 (0.4.0.1862.1.6) esi4-qcStatement-6: Tipo de certificado Id-etsi-qct-web (0.4.0.1862.1.6.3) id-etsi-qcs-QcType 3 = Certificado de autenticación del sitio web tal como se define en el Reglamento UE No 910/2014
id-etsi-qcs-QcPDS	No	id-etsi-qcs-5 (0.4.0.1862.1.5) URL = https://www.entrust.net/rpa Idioma = en

Certificado Cualificado de Autenticación de Sitio Web de tipo PSD2

Campo	Crítico	Contenido
Atributos		
Versión		V3
Número de Serie		Número único para el dominio PKI
Algoritmo de firma del emisor		sha-256
DN del emisor		CN = Entrust Certification Authority – ES QWAC2 OrganizationIdentifier = VATES-B81188047 O = Entrust EU, S.L. C = ES
Validez: Período		Se especifica notBefore y notAfter
DN de Sujeto		CN = <DNS nombre del servidor seguro> serialNumber=<número de registro del Suscriptor > businessCategory=<EV categoría de negocio> OU = <unidad organizativa del Suscriptor > (opcional) OrgID (2.23.140.3.1)= <Organization ID> O = <Nombre legal completo del Suscriptor > organizationIdentifier = <identificador de organización asignado por la NCA aplicable> jurisdictionOfIncorporationLocalityName (si aplica) = <jurisdicción o localidad de registro del Suscriptor > jurisdicationOfIncorporationStateOrProvinceName (si aplica) = < jurisdicción o estado o provincia de registro del Suscriptor > jurisdicationOfIncorporationCountry = < jurisdicción o país de registro del Suscriptor> L = <localidad del Sujeto > (opcional) S = <estado o provincia del Sujeto > (si aplica) C = <país del Sujeto>
Información de clave pública del Sujeto		Módulo clave RSA de 2048, 3072 o 4096 bits rsaEncryption {1.2.840.113549.1.1.1}
Extensión:	**Crítico**	**Valor**
Identificador de clave de autoridad	No	Hash de la Clave Pública de CA
Identificador de clave de Sujeto	No	Hash del subjectPublicKey en este certificado
Nombre alternativo de sujeto	No	Nombre(s) DNS del servidor seguro
Transparencia de certificado	No	(1.3.6.1.4.1.11129.2.4.2) PUEDE incluir dos o más pruebas de Transparencia de Certificado de logs CT aprobados
Uso de clave	Yes	Digital Signature Key Encipherment
Uso de clave extendida	No	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)
Políticas de certificado	No	[1] Política de certificado: Identificador de política = 2.16.840.1.114028.10.1.12.6 [1,1] Información de calificadores de política Id. del calificador de política = CPS Calificador: https://www.entrust.net/rpa [2] Política de certificado: Identificador de política =0.4.0.194112.1.4 [3] Política de certificado: Identificador de política =2.16.840.1.114028.10.1.2 [4] Política de certificado: Identificador de política = 2.23.140.1.1 [5] Política de certificado Identificador de política =0.4.0.19495.3.1

Restricciones Básicas	No	Tipo de Sujeto = entidad final Restricción de longitud de ruta = Ninguna
Acceso a la información de la autoridad	No	• Método de acceso = Protocolo de estado del certificado en línea (1.3.6.1.5.5.7.48.1) Nombre alternativo: URL = http: //ocsp.entrust.net • Método de acceso = Emisor de la autoridad de certificación (1.3.6.1.5.5.7.48.2) Nombre alternativo: URL = http://aia.entrust.net/ esqwac2-chain.cer
Puntos de distribución de CRL	No	uri: http://crl.entrust.net/ esqwac2ca.crl
cabfOrganizationIdentifier	No	2.23.140.3.1 = ID de la organización codificada de conformidad con las Guías EV SSL del CAB Forum
qcStatements	**Crítico**	**Valor**
id-etsi-qcs-QcCompliance	No	id-etsi-qcs-1 (0.4.0.1862.1.1) esi4-qcStatement-1: afirma que el certificado es un certificado calificado de la UE de acuerdo con el Reglamento UE no 910/2014
id-etsi-qcs-QcType	No	id-etsi-qcs-6 (0.4.0.1862.1.6) esi4-qcStatement-6: Tipo de certificado Id-etsi-qct-web (0.4.0.1862.1.6.3) id-etsi-qcs-QcType 3 = Certificado de autenticación del sitio web tal como se define en el Reglamento UE No 910/2014
id-etsi-qcs-QcPDS	No	id-etsi-qcs-5 (0.4.0.1862.1.5) URL = https://www.entrust.net/rpa Idioma = en
id-etsi-psd2-qcStatement	No	Id-etsi-psd2-qcStatement (0.4.0.19495.2) PSD2QcType ::= SEQUENCE{ rolesOfPSP RolesOfPSP, nCAName NCAName, nCAId NCAId }

Certificado Cualificado de Sello de Tiempo de tipo eIDAS

Campo		**Valor**
Attributes		
Version		V3
Serial Number		Número único para el dominio PKI
Issuer Signature Algorithm		sha-256
Issuer DN		CN = Entrust Certification Authority – ES QTS1 OrganizationIdentifier = VATES-B81188047 O = Entrust EU, S.L. C = ES
Validity Period		Se especifica notBefore y notAfter <= 5 years
Subject DN		CN = <nombre común de la TSA> OrgID = <identificador de la organización> O = < Nombre legal completo del Suscriptor > C = <país del Suscriptor>
Subject Public Key Info		Módulo clave RSA de 4096 bits rsaEncryption {1.2.840.113549.1.1.1}
Extensión	**Crítico**	**Valor**
Authority Key Identifier	No	Hash de la Clave Pública de CA
Subject Key Identifier	No	Hash del subjectPublicKey en este certificado
Key Usage	Yes	Digital Signature
Extended Key Usage	Yes	Timestamping (1.3.6.1.5.5.7.3.8)
Certificate Policies	No	[1] Política de certificado: Identificador de política = 2.16.840.1.114028.10.1.12.7 [1,1] Información de calificadores de política: Id. del calificador de política =CPS Calificador: https://www.entrust.net/rpa [2] Política de certificado: Identificador de política =0.4.0.194112.1.1
Basic Constraints	No	Tipo de Sujeto = entidad final Restricción de longitud de ruta = Ninguna
Authority Information Access		[1] Información de Acceso de Autoridad Método de Acceso = On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Nombre Alternativo: uri=http://ocsp.entrust.net [2] Información de Acceso de Autoridad Método de Acceso =Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Nombre Alternativo: URL= http://aia.entrust.net/esqts1-chain.p7c
CRL Distribution Points	No	uri: http://crl.entrust.net/esqts1ca.crl
qcStatements	**Crítico**	**Valor**
id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)	No	id-etsi-qcs-1 (0.4.0.1862.1.1) esi4-qcStatement-1: afirma que el certificado es un certificado calificado de la UE de acuerdo con el Reglamento UE no 910/2014
id-etsi-qcs-QcType (0.4.0.1862.1.6)	No	id-etsi-qcs-6 (0.4.0.1862.1.6) esi4-qcStatement-6 : Tipo de certificado id-etsi-qcs-QcType 2 = Certificado para Sellos electrónicos tal como se define en el Reglamento EU No 910/2014
id-etsi-qcs-QcPDS (0.4.0.1862.1.5)	No	id-etsi-qcs-5 (0.4.0.1862.1.5) URL= https://www.entrust.net/rpa Idioma = en

Apéndice B - Esquemas de registro

Los siguientes esquemas de registro se reconocen actualmente como válidos bajo estas pautas:

NTR: La información contenida en este campo debe ser la misma que se encuentra en el número de registro del Sujeto, como se especifica en §3.2.2.1, y el código de país utilizado en el identificador del esquema de registro debe coincidir con el de la jurisdicción del Sujeto, como se especifica en §3.2.2.1.

Cuando la jurisdicción de registro del Sujeto o el campo de registro en §3.2.2.1 incluya más datos que el código de país, la información de localidad adicional se incluirá como se especifica en §3.2.2.10.

IVA: Referencia asignada por las autoridades fiscales nacionales a una entidad jurídica. Esta información se validará utilizando la información proporcionada por la autoridad fiscal nacional comparándola con la organización identificada por el nombre de la organización del sujeto y el número de registro del sujeto dentro del contexto de la jurisdicción del sujeto, como se especifica en §3.2.2.1.

PSD: Número de autorización especificado en ETSI TS 119 495 cláusula 4.4 asignado a un proveedor de servicios de pago y que contiene la información especificada en ETSI TS 119 495 cláusula 5.2.1. Esta información se obtendrá directamente del registro de la autoridad nacional competente para los servicios de pago o de una fuente de información aprobada por una agencia gubernamental, organismo regulador o legislación para este propósito. Esta información se validará comparándola directa o indirectamente (por ejemplo, haciendo coincidir un número de registro globalmente único) con la organización identificada por el nombre de la organización del sujeto y el número de registro del sujeto dentro del contexto de la jurisdicción del sujeto, como se especifica en §3.2. 2.1. La dirección indicada de la organización combinada con el nombre de la organización no será la única información utilizada para desambiguar la organización.