ENTRUST EU S.L.

Política de Certificado (CP)
Para Certificados Cualificados de Autenticación de Sitio Web de tipo eIDAS (QWAC de tipo eIDAS)

Versión: 1.4
7 de diciembre de 2022

Historial de cambios

Versión	Fecha	Actualización
1.0	17 de junio de 2020	Versión inicial
1.1	30 de octubre de 2020	Actualizar el perfil del certificado para aclarar las claves RSA admitidas y el enlace qcStatement
1.2	7 de mayo de 2021	Actualizar la verificación de la identidad del Suscriptor
1.2.1	15 de noviembre de 2021	Cambio de Entrust Datacard Europe a Entrust EU, S.L.
1.3	30 de noviembre de 2021	Actualización de los nuevos nombres de las CA
1.4	7 de diciembre de 2022	Actualización del enlace del repositorio y referencias de política OID

CONTENIDO

1. Descripción de Certificado

1.1 Definición

Este certificado está cualificado para una persona jurídica según lo establecido en el Reglamento del Parlamento Europeo y del Consejo (UE) Núm. 910/2014 Sección 8, de fecha 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado nacional, que deroga la Directiva 1999/93/CE.

Este certificado identifica a la entidad responsable del sitio web y permite la autenticación del sitio web y permite la seguridad de las transacciones hacia y desde el sitio web.

Entrust emite los Certificados Cualificados de Autenticación de Sitio Web de tipo eIDAS (QWAC de tipo eIDAS) a personas jurídicas.

Los roles aplicables son los siguientes:
• Suscriptor: la persona jurídica responsable del sitio web.
• Representante Autorizado: la persona física con poder para actuar en nombre del Suscriptor.

Este certificado tiene una duración máxima de 825 días. A partir del 1 de septiembre de 2020, la duración máxima del certificado se reducirá a 398 días.

Los términos en mayúscula se definen en la Sección 1.6.1 de la Declaración de Prácticas de Certificación (CPS) - Definiciones, que se incorporan aquí por esta referencia.

1.2 Identificadores de objeto de política de certificado

El certificado incluirá los siguientes identificadores de objeto de política de certificados (OID) para indicar la política que cumplirán los certificados.

OID de política QWAC de tipo eIDAS

OID de política de certificado	Definición de política de certificado
0.4.0.194112.1.4	QCP-w como se define en ETSI EN 319 411-2
2.16.840.1.114028.10.1.12.4	Entrust OID para QCP-w como se define en ETSI EN 319 411-2
2.23.140.1.1	Certificado SSL de Validación Extendida (EV) SSL como definido por CA/Browser Forum
2.16.840.1.114028.10.1.2	Entrust OID para Certificado SSL de Validación Extendida (EV) SSL como definido por CA/Browser Forum

1.3 Ámbito de uso

Los certificados están destinados a permitir la autenticación de sitios web en función de un certificado cualificado definido en los artículos 3 (38) y 45 del Reglamento (UE) no 910/2014.

Los certificados se emiten sujetos a las condiciones y limitaciones definidas en los términos y condiciones de Entrust y la CPS, véase https://www.entrust.net/CPS.

1.4 Estipulaciones generales

1.4.1 Obligaciones relativas a la identificación

Entrust verifica la identidad y cualquier otra circunstancia relevante del Suscriptor con el propósito de emitir el certificado.

1.4.2 Obligaciones de los Subscriptores del Certificado

Las obligaciones del Suscriptor se estipulan en la sección 9.6.3 de la CPS - Representaciones y garantías del suscriptor.

2. Ciclo de vida del Certificado

2.1 Solicitud

Al acceder al sitio web de Entrust, el Representante del Solicitante completará el formulario de solicitud de certificado. Al firmar la solicitud, el Suscriptor acepta los términos y condiciones del certificado.

2.2 Verificación de la identidad del Subscriptor

Entrust verificará la identidad del Suscriptor de acuerdo con lo previsto en la sección 3.2.3 de la Declaración de Prácticas de Certificación.

2.3 Emisión y procedimiento de entrega

Entrust emitirá y entregará el certificado de la siguiente manera:

(i) El Representante del Solicitante firma los términos y condiciones y se inscribe para obtener una cuenta de administración de certificados. El Solicitante proporciona información del Suscriptor para ser asignada y verificada en la cuenta.
(ii) El Representante del Solicitante puede solicitar un certificado a través de su cuenta seleccionando la información que se incluirá en el certificado. El Representante del Solicitante seleccionará el período de validez y proporcionará una clave pública a través de una solicitud de firma de certificado (CSR).
(iii) La solicitud de certificado será verificada técnicamente para cumplir con la política del certificado, si es satisfactorio, se emitirá el certificado.
(iv) El certificado se proporcionará al Representante del Solicitante dentro de la cuenta o también se puede proporcionar por correo electrónico o mediante una respuesta API.

2.4 Verificación del certificado

Entrust seguirá los procedimientos de acuerdo con la sección 3 de CPS - Identificación y autenticación, para verificar la solicitud del certificado antes de emitir el certificado.

2.5 Revocación del certificado

Entrust puede revocar un certificado por razones de acuerdo con la sección 4.9.1.1 de CPS - Razones para revocar un Certificado de Suscriptor.

Un Suscriptor puede solicitar la revocación de su certificado.

Las Partes que Confían, los ASV, las organizaciones antimalware y otros terceros pueden presentar una solicitud de problema de certificado (CPR). Entrust investigará la CPR de acuerdo con la sección 4.9.3 de CPS - Procedimiento para la solicitud de revocación. Si es necesario, Entrust revocará de acuerdo con los requisitos de la sección 4.9.1.1 de la CPS.

Un Suscriptor deberá solicitar la revocación de su certificado si el Suscriptor tiene una sospecha o conocimiento o una base razonable para creer que se ha producido alguno de los siguientes eventos:

(i) Compromiso de la clave privada del Suscriptor;
(ii) Conocimiento de que la solicitud de certificado original no estaba autorizada y que dicha autorización no se otorgará retroactivamente;
(iii) Cambio en la información contenida en el certificado del Suscriptor;
(iv) Cambio en las circunstancias que hacen que la información contenida en el certificado del Suscriptor se vuelva inexacta, incompleta o engañosa.

2.6 Renovación del certificado

Los Suscriptores pueden solicitar la renovación dentro de los 90 días posteriores a la expiración de su certificado existente. Entrust reutilizará o verificará los datos antes de la emisión del certificado de acuerdo con la CPS.

3. Coste

El solicitante debe pagar la tarifa del certificado o certificados, de acuerdo con la base de pago seleccionada. Las tarifas se analizan en la sección 9.1 de la CPS - Tarifas.

4. Perfiles de certificado

Perfil de QWAC 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/ esqwac2.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

5. Cambios

Las modificaciones a este documento deberán ser aprobadas por la Autoridad en Materia de Políticas de Entrust. La modificación se enumerará en la sección Historial de cambios de este documento.