ENTRUST EU S.L.

Política de Certificado (CP)

Para Certificados Cualificados de Firma Electrónica de tipo eIDAS (QSigC de tipo eIDAS)

Versión: 1.7
1 de diciembre de 2023

Historial de cambios

Versión	Fecha	Actualización
1.0	17 de junio de 2020	Versión inicial
1.1	19 de junio de 2020	OID política de certificado 2.16.840.1.114028.10.1.6 añadida al perfil de certificado
1.2	22 de julio de 2020	Añadir extensiones AATL al perfil de certificado
1.3	30 de octubre de 2020	Actualizar el perfil del certificado para aclarar las claves RSA admitidas
1.4	7 de mayo de 2021	Actualizar la verificación de la identidad del Sujeto
1.4.1	15 de noviembre de 2021	Cambiar Entrust Datacard Europe por Entrust EU, S.L.
1.5	30 de noviembre de 2021	Actualización de los nuevos nombres de CA, actualización del perfil de certificado QCP-n-qscd
1.6	7 de diciembre de 2022	Actualización del enlace del repositorio, QCP-n, actualización del tamaño de la clave y referencias de la política OID
1.7	1 de diciembre de 2023	Actualización del enlace TSA y eliminación de la extensión Archive Rev Info Certificado de Corto Plazo

CONTENIDO

Descripción de Certificado

Definición

Este certificado está cualificado para una persona física 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 de la firma electrónica. Los certificados permiten la validación para demostrar que el documento electrónico fue emitido por la entidad, lo que proporciona certeza en cuanto al origen y la integridad del documento.

Entrust emite certificados cualificados de firma electrónica de tipo eIDAs (QSigC de tipo eIDAS) a personas físicas. Una persona física o jurídica puede ser descrita como el Suscriptor. Una persona física será descrita como el Sujeto del certificado.

Este certificado tiene una duración máxima de 3 años.

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.

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 QSigC de tipo eIDAS

OID de política de certificado	Definición de politica de certificado
0.4.0.194112.1.2	QCP-n-qscd como se define en in ETSI EN 319 411-2
2.16.840.1.114028.10.1.12.2	Entrust OID para QCP-n-qscd como se define en ETSI EN 319 411-2
2.16.840.1.114028.10.1.6	Entrust OID para Requisitos Técnicos de Adobe Approved Trust List (AATL) versión 2.0

Ámbito de uso

Los certificados están destinados a respaldar las firmas electrónicas avanzadas en función de un certificado cualificado definido en los artículos 26 y 27 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.

Estipulaciones generales

1.1.1 Obligaciones relativas a la identificación

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

1.1.2 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.

Ciclo de vida del Certificado

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.

Verificación de la identidad del Sujeto

Entrust verificará la identidad del Sujeto del Certificado de acuerdo con la sección 3.2.3 de la Declaración de Prácticas de Certificación.

El Sujeto se identificará de forma única con un atributo de número de identidad único incluido en el nombre de Sujeto del Certificado. El número de identidad único se determinará de acuerdo con la sección 3.1.5 de la Declaración de Prácticas de Certificación.

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 Sujeto puede solicitar un certificado a través de su cuenta seleccionando la información que se incluirá en el certificado. El Sujeto 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 satisfactoria, se emitirá el certificado.
(iv) El certificado se proporcionará al Sujeto mediante una respuesta API

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.

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 Sujeto o 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 Sujeto o Suscriptor deberá solicitar la revocación de su certificado si 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;
(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;
(iv) Cambio en las circunstancias que hacen que la información contenida en el certificado del Suscriptor se vuelva inexacta, incompleta o engañosa.

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.

Coste

El Suscriptor 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.

Perfiles de certificado

Perfil de QSigC 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 =0.4.0.194112.1.0 [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
Time-stamp (1.2.840.113583.1.1.9.1)	No	https://timestamp.entrust.net/qtsa1
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 cualificado 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 Firma Electrónica de tipo eIDAS de Corto Plazo (QCP-n-qscd)

Campo		**Contenido**
Attributes		
Version		V3
Serial Number		Número único con entropía de 64 bits
Issuer Signature Algorithm		sha-512
Issuer DN		CN = Entrust Certification Authority – ES QSig2 OrganizationIdentifier = VATES-B81188047 O = Entrust EU, S.L. C = ES
Validity Period		Se especifica notBefore and notAfter < 24 hours
Subject DN		CN = <givenName + surname> serialNumber (2.5.4.5) = <unique identity number> givenName (2.5.4.42) = <validated first name> surname (2.5.4.4) = <validated surname> C = <country of subscriber>
Subject Public Key Info		2048, 3072 or 4096-bit RSA key modulus rsaEncryption {1.2.840.113549.1.1.1}

Extensión	**Crítico**	**Valor**
Authority Key Identifier	No	Hash of the CA public key
Subject Key Identifier	No	Hash of the subjectPublicKey in this certificate
Key Usage	Yes	nonRepudiation
Extended Key Usage	No	Document Signing (1.3.6.1.5.5.7.3.3.6) Document Signing (1.3.6.1.4.1.311.10.3.12) Adobe Authentic Documents Trust (1.2.840.113583.1.1.5)
Certificate Policies	No	[1]Certificate Policy: Policy Identifier= 2.16.840.1.114028.10.1.12.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.entrust.net/rpa [2]Certificate Policy: Policy Identifier=0.4.0.194112.1.2
Basic Constraints	Yes	Subject Type = End Entity Path Length Constraint = None
Authority Information Access		[1]Authority Info Access Access Method = On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: uri=http://ocsp.entrust.net [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://aia.entrust.net/esqsig2-chain.p7c
CRL Distribution Points	No	http://crl.entrust.net/esqsig2ca.crl
Short term certificate (0.4.0.194121.2.1)	No	
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 Cualificado 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 púlica 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 firmas electrónicas 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

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.