ENTRUST EU S.L.

Política de Certificado (CP)
Para Certificados Cualificados de tipo eIDAS y de tipo PSD2

Versión: 1.0
27 de enero de 2025

Historial de cambios

Versión	Fecha	Actualización
1.0	27 de enero de 2025	Versión inicial

CONTENIDO

1. Descripción de Certificado

1.1. Definición

Este certificado está cualificado para una persona física según lo establecido en el Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) n.° 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital ("eIDAS") y la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) no 1093/2010 y se deroga la Directiva 2007/64/CE ("PSD2).

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.

Descripción general de los certificados

Tipo de certificado	**Uso**	**Sujeto**	**Roles**	**Periodo de validez (no más de)**
eIDAS QWAC	Autenticación de sitio web	Dispositivo	• Subscriptor • Representante Autorizado	398 días
PSD2 QWAC	Autenticación de sitio web	Dispositivo	• Subscriptor • Representante Autorizado	398 días
eIDAS QSealC	Sello electrónico	Persona Jurídica	• Subscriptor • Representante Autorizado	39 meses
PSD2 QSealC	Sello electrónico	Persona Jurídica	• Subscriptor • Representante Autorizado	39 meses
eIDAS QSigC	Firma electrónica	Persona Física	• Subscriptor	39 meses
eIDAS QTSC	Sello de tiempo	Persona Jurídica	• Subscriptor • Representante Autorizado	5 años

El período de validez del certificado se indica en la CPS sección 6.3.2

1.2. Identificadores de objetos de la política de certificados

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

OID de política de certificado

Tipo de Certificado	**Políticas de Certificado**

QWAC de tipo eIDAS	• 0.4.0.194112.1.4 - QEVCP-w como se define en ETSI EN 319 411-2 • 2.23.140.1.1 - Certificado SSL de Validación Extendida (EV) definido por el CA/Browser Forum • 2.16.840.1.114028.10.1.2 - Entrust OID para Certificado SSL de Validación Extendida (EV) definido por el CA/Browser Forum
QSealC de tipo eIDAS	• 0.4.0.194112.1.1 - QCP-l como se define en ETSI EN 319 411-2 • 2.16.840.1.114028.10.1.12.1 - Entrust OID para QCP-l como se define en ETSI EN 319 411-2 • 2.16.840.1.114028.10.1.6 - Entrust OID para Adobe Approved Trust List (AATL) Technical Requirements version 2.0
QSigC de tipo eIDAS	• 0.4.0.194112.1.2 - QCP-n-qscd como se define en 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 Adobe Approved Trust List (AATL) Technical Requirements version 2.0
QWAC de tipo PSD2	• 0.4.0.194112.1.4 - QEVCP-w como se define en ETSI EN 319 411-2 • 0.4.0.19495.3.1 - QCP-w-psd2 como se define en ETSI TS 119 495 • 2.23.140.1.1 - Certificado SSL EV definido por el CA/Browser Forum • 2.16.840.1.114028.10.1.2 - Entrust OID para Certificado SSL EV
QSealC de tipo PSD2	• 0.4.0.194112.1.1 - QCP-l como se define en ETSI EN 319 411-2 • 2.16.840.1.114028.10.1.12.5 - Entrust OID para QCP-l incluyendo PSD2 como se define en ETSI EN 319 411-2 and ETSI TS 119 495
QTSC de tipo eIDAS	• 0.4.0.194112.1.1 - QCP-l como se define en ETSI EN 319 411-2 • 2.16.840.1.114028.10.1.12.7 - Entrust OID para QCP-l más requisitos para permitir QTSA

1.3. Ámbito de uso

Ámbito de uso de los certificados

Tipo de Certificado	**Ámbito de uso**
QWAC de tipo eIDAS	• Reglamento (EU) 2024/1183 artículos 45
QSealC de tipo eIDAS	• Reglamento (EU) 2024/1183 artículos 36 y 37
QSigC de tipo eIDAS	• Reglamento (EU) 2024/1183 artículos 26 y 27

QWAC de tipo PSD2 y QSealC de tipo PSD2	• Reglamento (EU) 2024/1183), Directiva (EU) 2015/2366 y ETSI TS 119 495 para cumplir los requisitos de PSD2
QTSC de tipo eIDAS	• Reglamento (EU) 2024/1183 artículos 41 y 42

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 Sujeto y 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 Sujeto y/o del Subscriptor

Entrust verificará la identidad del Sujeto y/o del Subscriptor del Certificado de acuerdo con 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 o el Sujeto puede solicitar un certificado a través de su cuenta seleccionando la información que se incluirá en el certificado. El Representante del Solicitante o 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 Representante del Solicitante o al Sujeto 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 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.

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 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.

4. Perfiles de certificado

Perfil de QWAC de tipo eIDAS

Campo		**Contenido**
Attributes		
Version		V3
Serial Number		Número único para el dominio PKI
Issuer Signature Algorithm		sha256WithRSAEncryption
Issuer DN		CN = Entrust Certification Authority – ES QWAC2 organizationIdentifier = VATES-B81188047 O = Entrust EU, S.L. C = ES
Validity Period		Se especifica notBefore y notAfter
Subject DN		CN = <DNS nombre de servidor seguro> serialNumber=<número de registro del subscriptor > businessCategory=<EV categoría de negocio> organizationIdentifier = <identificador de organización> O = <nombre legal complete del subscriptor> 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 subscriptor> (opcional) S = <estado o provincial del subscriptor> (si aplica) C = <país del subscriptor >
Subject Public Key Info		Módulo clave RSA de 2048, 3072 o 4096-bit rsaEncryption {1.2.840.113549.1.1.1}
Extensión	**Crítico**	**Contenido**
Authority Key Identifier	No	Hash de la Clave Pública de CA
Subject Key Identifier	No	Hash del subjectPublicKey en este certificado
Subject Alternative Name	No	DNS nombre(s) de servidor seguro
Certificate Transparency	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
Key Usage	Sí	Digital Signature Key Encipherment
Extended Key Usage	No	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)
Certificate Policies	No	[1] Política de certificado: Identificador de política = 2.23.140.1.1 [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
Basic Constraints	Sí	Tipo de Sujeto = entidad final Restricción de longitud de ruta = Ninguna

Authority Information Access	No	• Access Method = On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.entrust.net • Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://aia.entrust.net/esqwac2-chain.cer
CRL Distribution Points	No	uri: http://crl.entrust.net/esqwac2ca.crl
cabfOrganizationIdentifier	No	2.23.140.3.1 = organizationIdentifier codificado en cumplimiento de las Guías EV SSL de CAB Forum
qcStatements	**Crítico**	**Contenido**
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 cualificado 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 de 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 Language = en

Perfil de QSealC de tipo eIDAS (dispositivo criptográfico seguro)

Campo		**Contenido**
Attributes		
Version		V3
Serial Number		Número único para el dominio PKI
Issuer Signature Algorithm		sha512WithRSAEncryption
Issuer DN		CN = Entrust Certification Authority – ES QSeal2 organizationIdentifier = VATES-B81188047 O = Entrust EU, S.L. C = ES
Validity Period		Se especifica notBefore y notAfter
Subject DN		CN = < nombre común usado habitualmente por el sujeto para representarse a sí mismo > OU = < unidad organizativa del suscriptor > (opcional) organizationIdentifier = < 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 >
Subject Public Key Info		RSA de 2048 o 4096-bit key modulus rsaEncryption {1.2.840.113549.1.1.1}
Extensión	**Crítico**	**Contenido**
Authority Key Identifier	No	Hash de la Clave Pública de CA
Subject Key Identifier	No	Hash del subjectPublicKey en este certificado
Key Usage	Sí	Non Repudiation
Extended Key Usage	No	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] 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 Qualifier: 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
Basic Constraints	Sí	Tipo de Sujeto = entidad final Restricción de longitud de ruta = Ninguna
Authority Information Access	No	[1]Authority Info Access Método de Acceso = 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 Método de Acceso = Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://aia.entrust.net/esqseal2-chain.p7c
CRL Distribution Points	No	uri: http://crl.entrust.net/esqseal2ca.crl
qcStatements	**Crítico**	**Contenido**

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-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 Language = en

Perfil de QSigC de tipo eIDAS (QCP-n-qscd)

Campo		**Contenido**
Attributes		
Version		V3
Serial Number		Número único con entropía de 64 bits
Issuer Signature Algorithm		sha512WithRSAEncryption
Issuer DN		CN = Entrust Certification Authority – ES QSig2 organizationIdentifier = VATES-B81188047 O = Entrust EU, S.L. C = ES
Validity Period		Se especifica notBefore y notAfter
Subject DN		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 >
Subject Public Key Info		2048-bit RSA key modulus rsaEncryption {1.2.840.113549.1.1.1}
Extensión	**Crítico**	**Contenido**
Authority Key Identifier	No	Hash de la Clave Pública de CA
Subject Key Identifier	No	Hash del subjectPublicKey en este certificado
Key Usage	Sí	nonRepudiation, digitalSignature
Extended Key Usage	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)
Certificate Policies	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
Basic Constraints	Sí	Tipo de Sujeto = entidad final Restricción de longitud de ruta = Ninguna
Authority Information Access	No	[1] Acceso a la información de la autoridad Método de acceso = On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: uri=http://ocsp.entrust.net [2] Acceso a la información de la autoridad Método de acceso = 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	uri: http://crl.entrust.net/esqsig2ca.crl

Time-stamp (1.2.840.113583.1.1.9.1)	No	https://timestamp.entrust.net/qtsa1 Authentication = Not Required
qcStatements	**Crítico**	**Contenido**
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-4: 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 : Tipo de certificado 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 Language = 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		sha512WithRSAEncryption
Issuer DN		CN = Entrust Certification Authority – ES QSig2 organizationIdentifier = VATES-B81188047 O = Entrust EU, S.L. C = ES
Validity Period		Se especifica notBefore y notAfter
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-bit RSA key modulus rsaEncryption {1.2.840.113549.1.1.1}
Extension	**Critical**	**Value**
Authority Key Identifier	No	Hash of the CA public key
Subject Key Identifier	No	Hash of the subjectPublicKey in this certificate
Key Usage	Sí	nonRepudiation
Extended Key Usage	No	Document Signing (1.3.6.1.5.5.7.3.36) 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] Política de Certificado: Identificador de Política = 2.16.840.1.114028.10.1.12.2 [1,1]Información del calificador de política: Id del calificador de política=CPS Qualifier: https://www.entrust.net/rpa [2] Política de Certificado: Identificador de Política = 0.4.0.194112.1.2
Basic Constraints	Sí	Tipo de Sujeto = entidad final Restricción de longitud de ruta = Ninguna
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	**Critical**	**Value**

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-4: 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 : Tipo de certificado 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 Language = en

Perfil de QWAC de tipo PSD2

Campo		**Contenido**
Attributes		
Version		V3
Serial Number		Número único para el dominio PKI
Issuer Signature Algorithm		sha256WithRSAEncryption
Issuer DN		CN = Entrust Certification Authority – ES QWAC2 organizationIdentifier = VATES-B81188047 O = Entrust EU, S.L. C = ES
Validity Period		Se especifica notBefore y notAfter
Subject DN		CN = < DNS nombre del servidor seguro > serialNumber=< número de registro del subscriptor > businessCategory=<EV categoría de negocio > organizationIdentifier = < identificador de organización asignado por la NCA aplicable > O = < nombre legal completo del subscriptor > jurisdictionOfIncorporationLocalityName (if applicable) = < jurisdicción o localidad de registro del subscriptor > jurisdicationOfIncorporationStateOrProvinceName (si aplica) = < jurisdicción o estado o provincia de registro del Suscriptor > jurisdicationOfIncorporationCountry = <jurisdicción o país de registro del subscriptor> L = <localidad del subscriptor > (opcional) S = <estado o provincia del subscriptor> (si aplica) C = <país del subscriptor>
Subject Public Key Info		2048, 3072 or 4096 RSA key modulus rsaEncryption {1.2.840.113549.1.1.1}
Extensión	**Crítico**	**Contenido**
Authority Key Identifier	No	Hash de la Clave Pública de CA
Subject Key Identifier	No	Hash del subjectPublicKey en este certificado
Subject Alternative Name	No	Nombre(s) DNS de servidor seguro
Certificate Transparency	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
Key Usage	Sí	Digital Signature Key Encipherment
Extended Key Usage	No	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)
Certificate Policies	No	[1] Política de certificado: Identificador de política = 2.23.140.1.1 [2] Política de certificado: Identificador de política = 0.4.0.194112.1.4 [3] Política de certificado: Identificador de política = 0.4.0.19495.3.1 [4] Política de certificado: Identificador de política = 2.16.840.1.114028.10.1.2
Basic Constraints	Sí	Tipo de Sujeto = entidad final Restricción de longitud de ruta = Ninguna
Authority Information Access	No	• Access Method = On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.entrust.net

		• Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://aia.entrust.net/esqwac2-chain.cer
CRL Distribution Points	No	uri: http://crl.entrust.net/esqwac2.crl
cabfOrganizationIdentifier	No	2.23.140.3.1 = organizationIdentifier codificado de conformidad con las Guías EV SSL del CAB Forum
qcStatements	**Crítico**	**Contenido**
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 Cualificado 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 : Type of certificate Id-etsi-qct-web (0.4.0.1862.1.6.3) id-etsi-qcs-QcType 3 = Certificado de autenticación de 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 Language = en
id-etsi-psd2-qcStatement	No	Id-etsi-psd2-qcStatement (0.4.0.19495.2) PSD2QcType ::= SEQUENCE{ rolesOfPSP RolesOfPSP, nCAName NCAName, nCAId NCAId }

Perfil de QSealC de tipo PSD2

Campo		**Contenido**
Attributes		
Version		V3
Serial Number		Número único para el dominio PKI
Issuer Signature Algorithm		sha512WithRSAEncryption
Issuer DN		CN = Entrust Certification Authority – ES QSeal2 organizationIdentifier = VATES-B81188047 O = Entrust EU, S.L. C = ES
Validity Period		Se especifica notBefore y notAfter
Subject DN		CN = < nombre común usado habitualmente por el sujeto para representarse a sí mismo > OU = < unidad organizativa del suscriptor > (opcional) organizationIdentifier = < identificador de la organización > O = < nombre legal completo del subscriptor > L = <localidad del suscriptor > (opcional) S = <estado o provincia del suscriptor > (opcional) C = <país del suscriptor>
Subject Public Key Info		2048-bit RSA
Extensión	**Crítico**	**Contenido**
Authority Key Identifier	No	Hash de la Clave Pública de CA
Subject Key Identifier	No	Hash del subjectPublicKey en este certificado
Key Usage	Sí	Non Repudiation
Extended Key Usage	No	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] 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
Basic Constraints	Sí	Tipo de Sujeto = entidad final Restricción de longitud de ruta = Ninguna
Authority Information Access	No	[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/esqseal2-chain.p7c
CRL Distribution Points	No	uri: http://crl.entrust.net/esqseal2ca.crl
qcStatements	**Crítico**	**Contenido**
id-etsi-qcs-QcCompliance	No	id-etsi-qcs-1 (0.4.0.1862.1.1)

(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-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 Language = EN
id-etsi-psd2-qcStatement (0.4.0.19495.2)	No	(ONLY for PSD2 per ETSI TS 119 495, 5.1) PSD2QcType ::= SEQUENCE{ rolesOfPSP RolesOfPSO, nCAName NCAName, nCAId NCAId}

Certificado Cualificado de Sellado de Tiempo de tipo eIDAS

Campo		**Contenido**
Attributes		
Version		V3
Serial Number		Número único para el dominio PKI
Issuer Signature Algorithm		sha256WithRSAEncryption
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
Subject DN		CN = < nombre común de la TSA > organizationIdentifier = <organization identifier> O = < nombre legal completo del subscriptor > C = < país del subscriptor >
Subject Public Key Info		4096-bit RSA key modulus rsaEncryption {1.2.840.113549.1.1.1}
Extensión	**Crítico**	**Contenido**
Authority Key Identifier	No	Hash de la Clave Pública de CA
Subject Key Identifier	No	Hash del subjectPublicKey en este certificado
Key Usage	Sí	Digital Signature
Extended Key Usage	Sí	Timestamping (1.3.6.1.5.5.7.3.8)
Certificate Policies	No	[1] Política de certificado: Identificador de política = 2.23.140.1.4.2 [2] Política de certificado: Identificador de política = 2.16.840.1.114028.10.1.12.7 [2,1] Información de calificadores de política: Id. del calificador de política =CPS Calificador: https://www.entrust.net/rpa [3] Política de certificado: Identificador de política = 0.4.0.194112.1.1
Basic Constraints	Sí	Tipo de Sujeto = entidad final Restricción de longitud de ruta = Ninguna
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/esqts1-chain.p7c
CRL Distribution Points	No	uri: http://crl.entrust.net/esqts1ca.crl
privateKeyUsagePeriod	No	No mayor de 15 meses
qcStatements	**Crítico**	**Contenido**
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-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 Language = 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.