ENTRUST EU S.L.

Certificate Policy (CP)
For eIDAS and PSD2 Qualified Certificates

Version: 1.0
27 January 2025

Revision History

Issue	Date	Changes in this Revision
1.0	27 January 2025	Initial version combining all CPs

TABLE OF CONTENTS

1. Certificate Description

1.1 Definition

This certificate is qualified for a natural or legal person as established in Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework and Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC ("PSD2").

Capitalized terms are defined in Certification Practice Statement (CPS) section 1.6.1 - Definitions, which are incorporated herein by this reference.

Certificate Overview

Certificate Type	**Use**	**Subject**	**Roles**	**Validity Period (no greater than)**
eIDAS QWAC	Website authentication	Device	• Subscriber • Authorized Representative	398-days
PSD2 QWAC	Website Authentication	Device	• Subscriber • Authorized Representative	398-days
eIDAS QSealC	Electronic seal	Legal Person	• Subscriber • Authorized Representative	39 months
PSD2 QSealC	Electronic seal	Legal person	• Subscriber • Authorized Representative	39 months
eIDAS QSigC	Electronic signature	Natural person	• Subscriber	39 months
eIDAS QTSC	Time-stamps	Legal person	• Subscriber • Authorized Representative	5 years

Certificate validity period is stated in CPS section 6.3.2

1.2 Certificate Policy Object Identifiers

The certificate will include the following certificate policy object identifiers (OIDs) to indicate the policy from which the certificates will comply.

Certificate Policy OIDs

Certificate Type	Certificate Policies
eIDAS QWAC	• 0.4.0.194112.1.4 - QEVCP-w as defined in ETSI EN 319 411-2 • 2.23.140.1.1 - Extended Validation (EV) SSL Certificate as defined by CA/Browser Forum • 2.16.840.1.114028.10.1.2 - Entrust OID for Extended Validation (EV) SSL Certificate as defined by CA/Browser Forum
eIDAS QSealC	• 0.4.0.194112.1.1 - QCP-l as defined in ETSI EN 319 411-2 • 2.16.840.1.114028.10.1.12.1 - Entrust OID for QCP-l as defined in ETSI EN 319 411-2 • 2.16.840.1.114028.10.1.6 - Entrust OID for Adobe Approved Trust List (AATL) Technical Requirements version 2.0
eIDAS QSigC	• 0.4.0.194112.1.2 - QCP-n-qscd as defined in ETSI EN 319 411-2 • 2.16.840.1.114028.10.1.12.2 - Entrust OID for QCP-n-qscd as defined in ETSI EN 319 411-2 • 2.16.840.1.114028.10.1.6 - Entrust OID for Adobe Approved Trust List (AATL) Technical Requirements version 2.0
PSD2 QWAC	• 0.4.0.194112.1.4 - QEVCP-w as defined in ETSI EN 319 411-2 • 0.4.0.19495.3.1 - QCP-w-psd2 as defined in ETSI TS 119 495 • 2.23.140.1.1 - EV SSL Certificate as defined by CA/Browser Forum • 2.16.840.1.114028.10.1.2 - Entrust OID for EV SSL Certificate
PSD2 QSealC	• 0.4.0.194112.1.1 - QCP-l as defined in ETSI EN 319 411-2 • 2.16.840.1.114028.10.1.12.5 - Entrust OID for QCP-l including PSD2 as defined in ETSI EN 319 411-2 and ETSI TS 119 495
eIDAS QTSC	• 0.4.0.194112.1.1 - QCP-l as defined in ETSI EN 319 411-2 • 2.16.840.1.114028.10.1.12.7 - Entrust OID for QCP-l plus requirements to support a QTSA

1.3 Scope of Use

Certificate Scope of Use

Certificate Type	Scope of Use
eIDAS QWAC	• Regulation (EU) 2024/1183 articles 45
eIDAS QSealC	• Regulation (EU) 2024/1183 articles 36 and 37
eIDAS QSigC	• Regulation (EU) 2024/1183 articles 26 and 27
PSD2 QWAC and PSD2 QSealC	• Regulation (EU) 2024/1183), Directive (EU) 2015/2366 and ETSI TS 119 495 to meet the requirements of PSD2
eIDAS QTSC	• Regulation (EU) 2024/1183 articles 41 and 42

The certificates are issued subject to the conditions and limitations defined in Entrust's terms and conditions and the CPS, see https://www.entrust.net/CPS.

1.4 General Stipulations

1.4.1 Obligations Concerning Identification

Entrust verifies the identity and any other relevant circumstances of the Subject and/or the Subscriber for purposes of issuing the certificate.

1.4.2 Obligations of Certificate Subscribers

The Subscriber's obligations are stipulated in CPS section 9.6.3 - Subscriber Representations and Warranties.

2. Certificate Lifecycle

2.1 Application

By accessing Entrust's website, the Applicant Representative will fill out the certificate application form. By signing the application, the Subscriber agrees to the terms and conditions of the certificate.

2.2 Verification of Identity of the Subject and/or Subscriber

Entrust shall verify the identity of the Subject and/or the Subscriber in accordance with the CPS section 3.2.3.

2.3 Issue and Delivery Procedure

Entrust shall issue and deliver the certificate as follows:

(i) The Applicant Representative signs the terms and conditions and enrolls for a certificate management account. The Applicant provides Subscriber information to be assigned and verified to the account.
(ii) The Applicant Representative or the Subject can apply for a certificate through their account by selecting the information to be included in the certificate. The Applicant Representative or the Subject will select the validity period and provide the public key through a certificate signing request (CSR).

(iii) The certificate application will be technically verified to meet the certificate policy, if successful the certificate will be issued.
(iv) The certificate will be provided to the Applicant Representative or the Subject within the account or may also be provided by email or through an API response.

2.4 Certificate Verification

Entrust will follow procedures in accordance with the CPS section 3 - Identification and Authentication, to verify the certificate application before issuing the certificate.

2.5 Certificate Revocation

Entrust may revoke a certificate for reasons in accordance with CPS section 4.9.1.1 – Reasons for Revoking a Subscriber Certificate.

A Subscriber or a Subject may request their certificate to be revoked.

Relying Parties, ASVs, Anti-Malware Organizations and other third parties may submit a certificate problem request (CPR). Entrust will investigate the CPR in accordance with CPS section 4.9.3 – Procedure for Revocation Request. If required, Entrust will revoke in accordance with the requirements of CPS section 4.9.1.1.

A Subscriber or a Subject shall request revocation of their certificate if the Subscriber has a suspicion or knowledge of or a reasonable basis for believing that of any of the following events have occurred:

(i) Compromise of the private key;
(ii) Knowledge that the original certificate request was not authorized and such authorization will not be retroactively granted;
(iii) Change in the information contained in the certificate;
(iv) Change in circumstances that cause the information contained in the certificate to become inaccurate, incomplete, or misleading.

2.6 Certificate Renewal

Subscribers may request renewal within 90 days of expiry of their existing certificate. Entrust will reuse or verify data before certificate issuance in accordance with the CPS.

3. Cost

The Applicant must pay the fee for the certificate or certificates, according to the payment basis selected. Fees are discussed in CPS section 9.1 - Fees.

4. Certificate Profiles

eIDAS QWAC Profile

Field		**Value**
Attributes		
Version		V3
Serial Number		Unique number to PKI domain
Issuer Signature Algorithm		sha256WithRSAEncryption
Issuer DN		CN = Entrust Certification Authority – ES QWAC2 organizationIdentifier = VATES-B81188047 O = Entrust EU, S.L. C = ES
Validity Period		notBefore and notAfter are specified
Subject DN		CN = <DNS name of secure server> serialNumber=<registration number of subscriber> businessCategory=<EV business category> organizationIdentifier = <organization identifier> O = <full legal name of subscriber> jurisdictionOfIncorporationLocalityName (if applicable) = <jurisdiction of registration or incorporation locality of subscriber> jurisdicationOfIncorporationStateOrProvinceName (if applicable) = <jurisdiction of registration or incorporation state or province of subscriber> jurisdicationOfIncorporationCountry = <jurisdiction of registration or incorporation country of subscriber> L = <locality of subscriber> (optional) S = <state or province of subscriber> (if applicable) C = <country of subscriber>
Subject Public Key Info		2048, 3072 or 4096-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
Subject Alternative Name	No	DNS name(s) of secure server
Certificate Transparency	No	(1.3.6.1.4.1.11129.2.4.2) MAY include two or more Certificate Transparency proofs from approved CT Logs
Key Usage	Yes	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] Certificate Policy: Policy Identifier=2.23.140.1.1 [2] Certificate Policy: Policy Identifier=0.4.0.194112.1.4 [3] Certificate Policy: Policy Identifier=2.16.840.1.114028.10.1.2
Basic Constraints	Yes	Subject Type = End Entity Path Length Constraint = None
Authority Information	No	• Access Method = On-line Certificate Status Protocol

Access		(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 encoded in compliance with the CAB Forum EV SSL Guidelines
qcStatements	**Critical**	**Value**
id-etsi-qcs-QcCompliance	No	id-etsi-qcs-1 (0.4.0.1862.1.1) esi4-qcStatement-1: Claim that the certificate is an EU Qualified Certificate in accordance with Regulation EU 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 = Certificate for website authentication as defined in Regulation EU 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

eIDAS QSealC Profile (secure crypto device)

Field		**Value**
Attributes		
Version		V3
Serial Number		Unique number to PKI domain
Issuer Signature Algorithm		sha512WithRSAEncryption
Issuer DN		CN = Entrust Certification Authority – ES QSeal2 organizationIdentifier = VATES-B81188047 O = Entrust EU, S.L. C = ES
Validity Period		notBefore and notAfter are specified
Subject DN		CN = <common name which is commonly used by the subject to represent itself> OU = <organization unit of subscriber> (optional) organizationIdentifier = <organization identifier> O = <full legal name of subscriber> L = <locality of subscriber> (optional) S = <state or province of subscriber> (optional) C = <country of subscriber>
Subject Public Key Info		2048 or 4096-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	Yes	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]Certificate Policy: Policy Identifier= 2.16.840.1.114028.10.1.12.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.entrust.net/rpa [2]Certificate Policy: Policy Identifier=0.4.0.194112.1.1 [3]Certificate Policy: Policy Identifier=2.16.840.1.114028.10.1.6
Basic Constraints	Yes	Subject Type = End Entity Path Length Constraint = None
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	**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: Claim that the certificate is an EU Qualified Certificate in accordance with Regulation EU 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 2 = Certificate for electronic Seals as defined in Regulation 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

eIDAS QSigC Profile (QCP-n-qscd)

Field		**Value**
Attributes		
Version		V3
Serial Number		Unique number with 64-bit entropy
Issuer Signature Algorithm		sha512WithRSAEncryption
Issuer DN		CN = Entrust Certification Authority – ES QSig2 organizationIdentifier = VATES-B81188047 O = Entrust EU, S.L. C = ES
Validity Period		notBefore and notAfter are specified
Subject DN		CN = <common name which is commonly used by the subject to represent itself> serialNumber (2.5.4.5) = <unique identity number> givenName (2.5.4.42) = <validated first name> surname (2.5.4.4) = <validated surname> OU = <organization unit of subscriber> (optional) O = <full legal name of subscriber> L = <locality of subscriber> (optional) S = <state or province of subscriber> (optional) 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	Yes	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]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 [3]Certificate Policy: Policy Identifier=2.16.840.1.114028.10.1.6
Basic Constraints	Yes	Subject Type = End Entity Path Length Constraint = None
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/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	**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: Claim that the certificate is an EU Qualified Certificate in accordance with Regulation EU 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: The private key related to the certified public key resides on a QSCD in accordance with Regulation EU 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 = Certificate for electronic signatures as defined in Regulation 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

eIDAS Qualified Signature Short -term Certificate (QCP-n-qscd)

Field		**Value**
Attributes		
Version		V3
Serial Number		Unique number with 64-bit entropy
Issuer Signature Algorithm		sha512WithRSAEncryption
Issuer DN		CN = Entrust Certification Authority – ES QSig2 organizationIdentifier = VATES-B81188047 O = Entrust EU, S.L. C = ES
Validity Period		notBefore and notAfter are specified
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	Yes	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]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	**Critical**	**Value**
id-etsi-qcs-	No	id-etsi-qcs-1 (0.4.0.1862.1.1)

QcCompliance (0.4.0.1862.1.1)		esi4-qcStatement-1: Claim that the certificate is an EU Qualified Certificate in accordance with Regulation EU 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: The private key related to the certified public key resides on a QSCD in accordance with Regulation EU 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 = Certificate for electronic signatures as defined in Regulation 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

PSD2 QWAC Profile

Field		**Value**
Attributes		
Version		V3
Serial Number		Unique number to PKI domain
Issuer Signature Algorithm		sha256WithRSAEncryption
Issuer DN		CN = Entrust Certification Authority – ES QWAC2 organizationIdentifier = VATES-B81188047 O = Entrust EU, S.L. C = ES
Validity Period		notBefore and notAfter are specified
Subject DN		CN = <DNS name of secure server> serialNumber=<registration number of subscriber> businessCategory=<EV business category> organizationIdentifier = <organization identifier assigned by applicable NCA> O = <full legal name of subscriber> <jurisdiction of registration or incorporation locality of subscriber> jurisdictionOfIncorporationLocalityName (if applicable) = jurisdicationOfIncorporationStateOrProvinceName (if applicable) = <jurisdiction of registration or incorporation state or province of subscriber> jurisdicationOfIncorporationCountry = <jurisdiction of registration or incorporation country of subscriber> L = <locality of subscriber> (optional) S = <state or province of subscriber> (if applicable) C = <country of subscriber>
Subject Public Key Info		2048, 3072 or 4096 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
Subject Alternative Name	No	DNS name(s) of secure server
Certificate Transparency	No	(1.3.6.1.4.1.11129.2.4.2) MAY include two or more Certificate Transparency proofs from approved CT Logs
Key Usage	Yes	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] Certificate Policy: Policy Identifier=2.23.140.1.1 [2] Certificate Policy: Policy Identifier=0.4.0.194112.1.4 [3] Certificate Policy Policy Identifier=0.4.0.19495.3.1 [4] Certificate Policy Policy identifier=2.16.840.1.114028.10.1.2
Basic Constraints	Yes	Subject Type = End Entity Path Length Constraint = None
Authority Information	No	• Access Method = On-line Certificate Status Protocol

Access		(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 encoded in compliance with the CAB Forum EV SSL Guidelines
qcStatements	**Critical**	**Value**
id-etsi-qcs-QcCompliance	No	id-etsi-qcs-1 (0.4.0.1862.1.1) esi4-qcStatement-1: Claim that the certificate is an EU Qualified Certificate in accordance with Regulation EU 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 = Certificate for website authentication as defined in Regulation EU 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 }

PSD2 QSealC profile

Field		**Value**
Attributes		
Version		V3
Serial Number		Unique number to PKI domain
Issuer Signature Algorithm		sha512WithRSAEncryption
Issuer DN		CN = Entrust Certification Authority – ES QSeal2 organizationIdentifier = VATES-B81188047 O = Entrust EU, S.L. C = ES
Validity Period		notBefore and notAfter are specified
Subject DN		CN = <common name which is commonly used by the subject to represent itself> OU = <organization unit of subscriber> (optional) organizationIdentifier = <organization identifier> O = <full legal name of subscriber> L = <locality of subscriber> (optional) S = <state or province of subscriber> (optional) C = <country of subscriber>
Subject Public Key Info		2048-bit RSA
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	Yes	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]Certificate Policy: Policy Identifier= 2.16.840.1.114028.10.1.12.5 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.entrust.net/rpa [2]Certificate Policy: Policy Identifier=0.4.0.194112.1.1
Basic Constraints	Yes	Subject Type = End Entity Path Length Constraint = None
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	**Critical**	**Value**
id-etsi-qcs-	No	id-etsi-qcs-1 (0.4.0.1862.1.1)

QcCompliance (0.4.0.1862.1.1)		esi4-qcStatement-1: Claim that the certificate is an EU Qualified Certificate in accordance with Regulation EU 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 2 = Certificate for electronic Seals as defined in Regulation 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
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}

eIDAS Qualified Time-stamp Certificate

Field		**Value**
Attributes		
Version		V3
Serial Number		Unique number to PKI domain
Issuer Signature Algorithm		sha256WithRSAEncryption
Issuer DN		CN = Entrust Certification Authority – ES QTS1 organizationIdentifier = VATES-B81188047 O = Entrust EU, S.L. C = ES
Validity Period		notBefore and notAfter are specified
Subject DN		CN = <common name for the TSA> organizationIdentifier = <organization identifier> O = <full legal name of subscriber> C = <country of subscriber>
Subject Public Key Info		4096-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	Yes	Digital Signature
Extended Key Usage	Yes	Timestamping (1.3.6.1.5.5.7.3.8)
Certificate Policies	No	[1]Certificate Policy: Policy Identifier= 2.23.140.1.4.2 [2]Certificate Policy: Policy Identifier= 2.16.840.1.114028.10.1.12.7 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.entrust.net/rpa [3]Certificate Policy: Policy Identifier=0.4.0.194112.1.1
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/esqts1-chain.p7c
CRL Distribution Points	No	uri: http://crl.entrust.net/esqts1ca.crl
privateKeyUsagePeriod	No	No greater than 15 months
qcStatements	**Critical**	**Value**
id-etsi-qcs-	No	id-etsi-qcs-1 (0.4.0.1862.1.1)

QcCompliance (0.4.0.1862.1.1)		esi4-qcStatement-1: Claim that the certificate is an EU Qualified Certificate in accordance with Regulation EU 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 2 = Certificate for electronic Seals as defined in Regulation 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. Changes

Modifications to this document shall be approved by the Entrust Policy Authority. Modification will be listed in the Revision History section of this document.