ENTRUST EU, S.L.

Certificate Policy (CP)
For PSD2 Certificates

Version: 1.5
October 31, 2023

Revision History

Issue	Date	Changes in this Revision
1.0	June 17, 2020	Initial version.
1.1	October 30, 2020	Update certificate profile to clarify RSA keys supported and qcStatement link.
1.2	May 7, 2021	Update verification of identity of Subscriber
1.2.1	November 15, 2021	Change Entrust Datacard Europe to Entrust EU, S.L.
1.3	November 30, 2021	Update for new CA names
1.4	December 7, 2022	Update repository link
1.5	October 31, 2023	Certificate policy OID changes

TABLE OF CONTENTS

1. Certificate Description

1.1 Definition

This certificate is qualified for a legal person as established in European Parliament and Council Regulation (EU) Num. 910/2014 dated 23 July 2014, on electronic identification and trust services for electronic transactions on the domestic market, repealing Directive 1999/93/EC, including its Annex IV ("eIDAS"); and to Directive (EU) 2015/2366 [i.2] 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").

This certificate identifies the entity responsible for PSD2 communication and who is either responsible for the website or the electronic seal.

Entrust issues the PSD2 Qualified Web Authentication Certificates (QWACs) and PSD2 Qualified Seal Certificates (QSealC) to legal persons.

The following are the applicable roles:

- Subscriber: the legal person who is responsible for the website or the electronic seal.
- Authorized Representative: the natural person with power to act on behalf of the Subscriber.

PSD2 QWAC has a maximum 825-day duration and effective 1 September 2020, the certificate maximum duration will be reduced to 398-days. PSD2 QSealC has a maximum 3 year duration.

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

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.

PSD2 QWAC Policy OIDs

Certificate Policy OID	**Certificate Policy Definition**
0.4.0.194112.1.4	QCP-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	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

PSD2 QSealC Policy OIDs

Certificate Policy OID	**Certificate Policy Definition**
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-psd2 as defined in ETSI EN 319 411-2

	and ETSI TS 119 495

1.3 Scope of Use

The certificates are aimed to support the PSD2 Regulatory Technical Standards for use of qualified certificates as defined in eIDAS (Regulation (EU) No 910/2014), including Annex IV to meet the regulatory requirements of PSD2 (Directive (EU) 2015/2366), including the requirements of ETSI TS 119 495 and related ETSI Guidelines.

The certificates are 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 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 Subscriber

Entrust shall verify the identity of 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 can apply for a certificate through their account by selecting the information to be included in the certificate. The Applicant Representative will select the validity period and provide a 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 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 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 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 Subscriber's 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 Subscriber's certificate;
(iv) Change in circumstances that cause the information contained in Subscriber's 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

PSD2 QWAC Profile

Field		**Value**
Attributes		
Version		V3
Serial Number		Unique number to PKI domain
Issuer Signature Algorithm		sha-256
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> OU = <organization unit of subscriber> (optional) OrgID (2.23.140.3.1)= <Organization ID> O = <full legal name of subscriber> organizationIdentifier = <organization identifier assigned by applicable NCA> <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	No	Subject Type = End Entity Path Length Constraint = None
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 = Organization ID 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{

Commented [BM1]: To be approved in CPS 2.0

		rolesOfPSP RolesOfPSP, nCAName NCAName, nCAId NCAId }

PSD2 QSealC profile

Field		**Value**
Attributes		
Version		V3
Serial Number		Unique number to PKI domain
Issuer Signature Algorithm		sha-256
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 <= 3 years
Subject DN		CN = <common name which is commonly used by the subject to represent itself> OU = <organization unit of subscriber> (optional) OrgID = <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	No	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
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}

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.