ENTRUST EU, S.L.

Certificate Policy (CP)
For Qualified Signature Certificates (QSigC)

Version: 1.4.1
November 15, 2021

Revision History

Issue	Date	Changes in this Revision
1.0	June 17, 2020	Initial version.
1.1	June 19, 2020	Certificate policy OID 2.16.840.1.114028.10.1.6 added to certificate profile
1.2	July 22, 2020	Add AATL extensions to certificate profile.
1.3	October 30, 2020	Update certificate profile to clarify RSA keys supported.
1.4	May 7, 2021	Update verification of subject identity
1.4.1	November 15, 2021	Change Entrust Datacard Europe to Entrust EU, S.L.

TABLE OF CONTENTS

1. Certificate Description

1.1 Definition

This certificate is qualified for a natural person as established in European Parliament and Council Regulation (EU) Num. 910/2014 Section 4 dated 23 July 2014, on electronic identification and trust services for electronic transactions on the domestic market, repealing Directive 1999/93/EC.

This certificate identifies the entity responsible for the electronic signature. The certificates supports validation to prove that the electronic document was issued by the identity, providing certainty as to the origin and integrity of the document.

Entrust issues the Qualified Signature Certificates (QSigCs) to natural persons. A natural person or a legal person may be described as the Subscriber. A natural person will be described as the Subject of the certificate.

This certificate 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.

QSigC Policy OIDs

Certificate Policy OID	Certificate Policy Definition
0.4.0.194112.1.0	QCP-n as defined in ETSI EN 319 411-2
2.16.840.1.114028.10.1.12.0	QCP-n as defined in ETSI EN 319 411-2
2.16.840.1.114028.10.1.6	Adobe Approved Trust List (AATL) Technical Requirements version 2.0

1.3 Scope of Use

The certificates are aimed to support the advanced electronic signatures based on a qualified certificate defined in articles 26 and 27 of the Regulation (EU) No 910/2014.

The certificates are issued subject to the conditions and limitations defined in Entrust's terms and conditions and the CPS, see https://eu.entrustdatacard.com/resources/.

1.4 General Stipulations

1.4.1 Obligations Concerning Identification

Entrust verifies the identity and any other relevant circumstances of the Subject and 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

Entrust shall verify the identity of the Subject of the certificate in accordance with the CPS section 3.2.3.

The Subject shall be uniquely identified with a serial number attribute included in the Subject name of the certificate. The serial number shall be determined in accordance with the CPS section 3.1.5.

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 Subject can apply for a certificate through their account by providing the information to be included in the certificate. The Subject 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 Subject 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 Subject or 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 Subject or Subscriber shall request revocation of their certificate if they havw 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 certificate to become inaccurate, incomplete, or misleading.

2.6 Certificate Renewal

Subjects 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 Subscriber 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

QSigC Profile

Field		**Value**
Attributes		
Version		V3
Serial Number		Unique number with 64-bit entropy
Issuer Signature Algorithm		sha-256
Issuer DN		CN = Entrust Certification Authority – ES QSig1 OrganizationIdentifier = VATES-B81188047 O = Entrust Datacard Europe, 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> serialNumber (2.5.4.5) = <unique 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, 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
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)
Certificate Policies	No	[1]Certificate Policy: Policy Identifier= 2.16.840.1.114028.10.1.12.0 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.entrust.net/rpa [2]Certificate Policy: Policy Identifier=0.4.0.194112.1.0 [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		[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/esqsig1-g4.cer
CRL Distribution Points	No	uri: http://crl.entrust.net/esqsig1ca.crl
Archive Rev Info (1.2.840.113583.1.1.9.2)	No	30 03 02 01 01
Time-stamp (1.2.840.113583.1.1.9.1)	No	URI = http://timestamp.entrust.net/TSS/RFC3161sha2TS 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-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= http://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.