PKI Disclosure Statement

1 Introduction

This document is the PKI Disclosure Statement ("PDS"), as required by European standards ETSI EN 319 411-1 ETSI EN 411 319-2, related to the Qualified Website Authentication Certificate ("QWAC"), Qualified Certificate for Electronic Seal (QSealC), and Qualified Certificate for Electronic Signature ("QSigC") certificate services offered by the Qualified Trust Service Provider **Entrust Datacard Europe, S.L.U.**, a Spanish company with VAT number ESB81188047 ("Entrust Datacard Europe").

Entrust Datacard Europe issues QWAC, QSealC, and QSigC Certificates pursuant to Regulation (EU) No 910/2014 of the European Parliament and of the Council dated 23 July 2014 "On Electronic Identification and Trust Services For Electronic Transactions in the Internal Market" ("eIDAS Regulation") and Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market ("PSD2").

This document does not substitute or replace the Terms and Conditions of the QWAC, QSealC, and QSigC certificate services nor the Entrust Datacard Europe Certification Practice Statement ("CPS") published on the Entrust Datacard Europe's website (see below - together referred to as the "requirements"). It merely provides an overview of the key Requirements in a simplified format.

2 CA contact information

The CA can be contacted at the following address:

Corporate Offices
Entrust Datacard Europe S.L.U.
Pe La Finca. Paseo Club Deportivo, 1 Bloque 3 BJ
28223 Pozuelo De Alarcón (Madrid)
Spain
Attn: Certificate Services

Support or Questions About Certificates
Tel: 1-866-267-9297 or 1-613-270-2680
Email: ecs.support@entrust.com

For questions relating to this PKI Disclosure Statement or other documents of the Entrust Datacard Europe QWAC, QSealC, or QSigC Certificate services, please send an email to ecs.support@entrust.com.

To request revocation of a certificate, follow the on-line procedure described in the CPS (which requires the

Subscriber's credentials which are provided at certificate issuance time) using the web page https://www.entrust.net/ev/misuse.cfm or using the email address evssl@entrust.com. For further information, refer to the CPS published on Entrust Datacard Europe's website.

3 Certificate types, validation procedures and usage

Entrust Datacard Europe issues QWACs, QSealC, and QSigC Certificates (together, "Certificates" provided by the certificate services) according to European standard ETSI EN 319 411-2, eIDAs Regulation 910/2014/CE and other related standards. Certificates are offered to the general public (private companies, public entities, and other legal persons, but not to natural persons), according to the terms and conditions published in Entrust Datacard Europe's CPS and Subscriber Agreement, which are available on the website. Any restrictions on certificate usage are noted in CPS Sections 1.4.1, 1.4.2, 4.5, and 6.1.7.

All Certificates are signed with the SHA-256 hashing function. For further information on the supported Certificate policies (e.g. their respective OIDs and other features) see the documentation published on Entrust Datacard Europe's website at https://eu.entrustdatacard.com/es/inicio/ and the CPS.

Information about Entrust Datacard Europe's relevant Root Certificates and issuing CAs are published on Entrust Datacard Europe's website. To confirm Entrust Datacard Europe's status as a Qualified Trust Service Provider on the Trusted List of the Government of Spain, see https://webgate.ec.europa.eu/tl-browser/#/tl/ES.

Entrust Datacard Europe makes both Certificate Revocations Lists (CRLs) and an on-line status checking service based on the OCSP standard available to allow validation of Certificates. The URLs of both are included in all Certificates, respectively in the CRLDistributionPoint ("CDP") and AuthorityInformationAccess ("AIA") extensions.

4 Reliance limits

Certificates are issued for QWAC, QSealC, and QSigC purposes.

Limitations on the use of Certificates may be specified within the Certificates themselves in the UserNotice attribute of the CertificatePolicies extension.

Limitations on the value of transactions in which the certificate can be used may be specified in certificates, within the QCStatements certificate extension, by means of the QCEuLimitValue item.

All records pertaining to the life-cycle of certificates, as well as all the CA service audit logs, are retained by Entrust Datacard Europe for fifteen years.

5 Obligations of subscribers

Certificate subscribers are subject to the following obligations:

- All information provided, and all representations made, by Subscriber in relation to any Certificates are and will be complete, accurate and truthful (and Subscriber shall promptly update such information and representations from time to time as necessary to maintain such completeness and accuracy);
- Provision of verification information reasonably requested by Entrust Datacard Europe or its delegate will not be unreasonably delayed;
- The Private Key corresponding to the Public Key submitted to Entrust Datacard Europe in connection with an Certificate Application was created using sound cryptographic techniques, if not generated by a CA;
- All measures necessary have been taken to maintain sole control of, keep confidential, and properly protect the Private Key (and any associated access information or device – e.g., password or token) at all times;
- Any information provided to Entrust Datacard Europe or to any independent third-party RAs in connection with an Certificate Application does not infringe, misappropriate, dilute, unfairly compete with, or otherwise violate the intellectual property, or other rights of any person, entity, or organization in any jurisdiction;
- The Certificate(s) will not be installed or used until the Subscriber has reviewed and verified the accuracy of the data in each Certificate;
- Subscriber will immediately respond to Entrust Datacard Europe's instructions concerning (1) compromise of the Private Key associated with any Certificate and (2) misuse or suspected misuse of an Certificate;
- All use of the Certificate and its associated Private Key shall cease immediately, and the Subscriber shall promptly notify Entrust Datacard Europe and request the revocation of the Certificate, if (1) any information included in the Certificate changes, is or becomes incorrect or inaccurate, or if any change in any circumstances would make the information in the Certificate Application or Certificate incorrect, misleading or inaccurate; or (2) there is any actual or suspected misuse or compromise of the Private Key (or key activation data) associated with the Public Key in the Certificate;
- All use of the (1) Certificate and (2) Private Key associated with the Public Key in such Certificate shall cease upon expiration or revocation of such Certificate and such Certificate shall be removed from the devices and/or software in which it has been installed;
- The Certificates will not be used for any hazardous or unlawful (including tortious) activities; and used only for the purpose they have been issued;
- The subject named in the Certificate corresponds to the Subscriber, and that it legally exists as a valid entity in the jurisdiction of incorporation specified in the Certificates;
- For QWACs, the Certificate shall be installed only on the server accessible at the domain name listed in the Certificate, and will only be used in compliance with all applicable laws, solely for authorized company business, and solely in accordance with the Subscriber Agreement and the CPS;
- For QWACs, the Subscriber has the exclusive right to use the domain name listed in the Certificate;

- The subject named in the Certificate corresponds to the Subscriber, and that it legally exists as a valid entity in the Jurisdiction of Incorporation or Registration specified in the Certificates.

For further information, please refer to the CPS, including Section 9.6.3.

6 Certificate status checking obligations of relying parties

All those who rely on the information contained in Certificates ("Relying Parties") must first verify that Certificates are not suspended or revoked. Such verification can be performed by consulting the list of revoked Certificates (CRL) published by Entrust Datacard Europe or by querying the OCSP service provided by Entrust Datacard Europe at the addresses (URLs) contained in the Certificates themselves.

7 Limited warranty and disclaimer/limitation of liability

For warranty and liability limitations, please refer to the provisions of the Subscriber Agreement and the CPS (in particular, see Subscriber Agreement Sections 7 – 9 and CPS Sections 9.7 - 9.9).

8 Applicable agreements, CPS, CP

The agreements and conditions applying to the certificate services are found in the following documents, published on the Entrust Datacard Europe website:

- Entrust Datacard Europe Certification Practice Statement (CPS)
- Subscription Agreement

The supported Certificate Policies (CP) are described in the CPS; see also section 3 above.

9 Privacy policy

Entrust Datacard Europe complies with the General Data Protection Regulation (EU) 2016/679 ("GDPR"), and the Entrust Corporation Privacy Policy at https://www.entrust.com/pages/privacy-statement and the Entrust Data Protection Policy at https://www.entrust.com/-/media/documentation/licensingandagreements/data-protection-policy.pdf .

All records relating to Certificates issued by Entrust Datacard Europe (e.g. evidence of the identity of subscribers; certificate issuance requests, including acceptance of the Terms and Conditions; certificate revocation requests; etc.) are retained by Entrust Datacard Europe for seven years.

10 Refund policy

For Entrust Datacard Europe's refund policy, see CPS Sec. 9.1.5.

11 Applicable laws, complaints and dispute resolution

The certificate services provided by Entrust Datacard Europe is subject to the law of Ottawa, Canada. The

applicability, execution, interpretation and validity of the CPS are governed by the law of Ottawa, Canada, irrespective of the contract or other choice of legal provisions. For additional information, see CPS Sec. 9.13 and 9.14.

For all legal disputes related to the Entrust Datacard Europe certificate services, see the alternative dispute resolution provisions at CPS Sec. 9.13. For any matter not resolved by alternative dispute resolution, the courts of Ottawa, Canada shall have exclusive jurisdiction except as otherwise provided in the CPS and Subscriber Agreement. See in particular CPS Sec. 9.13 and 9.14.

12 QTSP trust list and audit

Entrust Datacard Europe is a Qualified Trust Service Provider listed on the Trust List of the Government of Spain as authorized to issue QWACs, QsealCs, and QSigCs in accordance with the eIDAS Regulation.

Entrust Datacard Europe's certificate services are subject to annual conformity assessment, according to European norms ETSI EN 319 411-1 and ETSI EN 319 411-2 and ETSI TS 119 495, and related standards by an independent, qualified and accredited auditor, as required by the eIDAS Regulation.

* * *