ENTRUST DATACARD EUROPE S.L.

Certification Practice Statement (CPS)
For Qualified Certificates

Version: 1.1
10 June 2020

Revision History

Issue	Date	Changes in this Revision
1.0	11 December 2019	Initial version.
1.1	10 June 2020	Addition of QSeal and QSignature Certificates

TABLE OF CONTENTS

1. Introduction

Entrust Datacard Europe S.L. ("Entrust Datacard") uses its suite of software products to provide standards-compliant digital certificates that enable more secure on-line communications.

The Entrust Datacard CAs issue Certificates, which include the following Certificate types:

- eIDAS Qualified Signature Certificate(s) ("eIDAS QSigC(s)")
- eIDAS Qualified Seal Certificate(s) ("eIDAS QSealC(s)")
- PSD2 Qualified Seal Certificate(s) ("PSD2 QSealC(s)")
- eIDAS Qualified Web Authentication Certificate(s) ("eIDAS QWAC(s)")
- PSD2 Qualified Web Authentication Certificate(s) ("PSD2 QWAC(s)")

1.1 Overview

This CPS describes the practices and procedures of (i) the CAs, and (ii) RAs operating under the CAs. This CPS also describes the terms and conditions under which Entrust Datacard makes CA and RA services available in respect to Certificates. This CPS is applicable to all persons, entities, and organizations, including, without limitation, all Applicants, Subscribers, Relying Parties, Resellers, Co-marketers and any other persons, entities, or organizations that have a relationship with (i) Entrust Datacard in respect to Certificates and/or any services provided by Entrust Datacard in respect to Certificates, or (ii) any RAs operating under a CAs, or any Resellers or Co-marketers providing any services in respect to Certificates. This CPS is incorporated by reference into all Certificates issued by Entrust Datacard CAs. This CPS provides Applicants, Subscribers, Relying Parties, Resellers, Co-marketers and other persons, entities, and organizations with a statement of the practices and policies of the CAs and also of the RAs operating under the CAs. This CPS also provides a statement of the rights and obligations of Entrust Datacard, any third parties that are operating RAs under the CAs, Applicants, Subscribers, Relying Parties, Resellers, Co-marketers and any other persons, entities, or organizations that may use or rely on Certificates or have a relationship with a CA or a RA operating under a CA in respect to Certificates and/or any services in respect to Certificates. This CPS is structured in accordance with and includes all the information required by RFC 3647.

In respect to Qualified Certificates, Entrust Datacard conforms to Regulation (EU) No 910/2014 of the European Parliament And Of The Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, including its Annex IV ("eIDAS"). If there is any inconsistency between this document and eIDAS requirements, the eIDAS requirements take precedence over this document.

In respect to PSD2 Certificates, Entrust Datacard conforms to Regulation (EU) No 910/2014 of the European Parliament And Of The Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and 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"). If there is any inconsistency between this document and PSD2 requirements, the PSD2 requirements take precedence over this document.

Additionally, in respect to eIDAS QWACs and PSD2 QWACs, Entrust Datacard conforms to the current version of the Guidelines for the Issuance and Management of Extended Validation Certificates published at http://www.cabforum.org. The EV SSL Guidelines describe certain minimum requirements that a CA must meet in order to issue EV SSL Certificates. In the event of any inconsistency between this CPS and the EV SSL Guidelines, the EV SSL Guidelines take precedence over this CPS.

1.2 Document Name and Identification

This document is called the Entrust Datacard Europe S.L. Certification Practice Statement.

1.3 PKI Participants

1.3.1 Certification Authorities

In the Entrust Datacard public-key infrastructure, CAs may accept Certificate Signing Requests (CSRs) and Public Keys from Applicants whose identity has been verified as provided herein by an RA. If a Certificate Application is verified, the verifying RA will send a request to a CA for the issuance of a Certificate. The CA will create a Certificate containing the Public Key and identification information contained in the request sent by the RA to that CA. The Certificate created in response to the request will be digitally signed by the CA.

This CPS covers all Certificates issued and signed by the following CAs. The purpose of these CAs is to enable Entrust Datacard to issue the trusted Qualified certificate types listed in Section 1 in accordance with applicable rules and regulations.

Root
CN: Entrust Root Certification Authority – G2
Key Identifier: 6a 72 26 7a d0 1e ef 7d e7 3b 69 51 d4 6c 8d 9f 90 12 66 ab
Thumbprint (SHA-1): 8c f4 27 fd 79 0c 3a d1 66 06 8d e8 1e 57 ef bb 93 22 72 d4

Subordinate CA(s) to G2
CN: Entrust Certification Authority – QTSP1
Subject Key Identifier: 1c ad 3f 9c d7 2d 22 19 a1 9c 4b e9 da f1 2a 33 f7 fb ba 0d
Thumbprint (SHA-1): 4c 71 c1 41 51 d1 b0 7b fb fe 69 65 be 66 a7 00 83 7f b7 0d

CN: Entrust Certification Authority – AATL1
Subject Key Identifier: 63:f1:84:dd:03:be:a3:9f:64:fa:76:7a:47:c4:56:7e:c0:6d:a0:20

Subordinate CA(s) to AATL1
CN: Entrust Certification Authority – ES QSeal1
Subject Key Identifier: 56:80:15:23:95:71:7f:e7:2d:90:d0:cd:06:3a:4f:67:63:7d:3d:75

Subordinate CA(s)
CN: Entrust Certification Authority – ES QSig1
Subject Key Identifier: 5a:53:08:8a:61:30:a9:0d:ea:d5:43:97:d3:98:3b:95:1e:2e:6d:02

Entrust Datacard shall be responsible for ensuring that all Subordinate CAs complies with all applicable policy requirements for the Root "Entrust Root Certification Authority – G2".

Externally Issued Cross Certificates

Issuer: CN = Microsoft Code Verification Root, O = Microsoft Corporation, L = Redmond, S = Washington, C = US
Subject: CN = Entrust Root Certification Authority - G2, OU = (c) 2009 Entrust, Inc. - for authorized use only, OU = See www.entrust.net/legal-terms, O = Entrust, Inc., C = US
Serial Number: 33 00 00 00 42 00 ba 5e 23 b0 a1 f3 99 00 00 00 00 00 42
Subject Key Identifier: 6a 72 26 7a d0 1e ef 7d e7 3b 69 51 d4 6c 8d 9f 90 12 66 ab
Valid until: July 7, 2025
Thumbprint (SHA-1): d8 fc 24 87 48 58 5e 17 3e fb fb 30 75 c4 b4 d6 0f 9d 8d 08

1.3.2 Registration Authorities

RAs under the CA may accept Certificate Applications from Applicants and perform verification of the information contained in such Certificate Applications, according to the procedures established by the Policy Authority. A RA operating under a CA may send a request to such CA to issue a Certificate to the Applicant. Only RAs authorized by Entrust Datacard are permitted to submit requests to a CA for the issuance of Certificates.

Third Party RAs may not be delegated to validate FQDNs nor IP Addresses per §3.2.2.4 or §3.2.2.5.

The CA may designate an Enterprise RA to verify Certificate requests from the Enterprise RA's own organization or from an organization of which the Enterprise RA is an agent. The requested FQDNs must be within the Enterprise RA's domain namespace.

1.3.3 Subscribers

Subscribers may use CA services to support transactions and communications. The Subject of a Certificate is the party named in the Certificate. A Subscriber, as used herein, may refer to both the Subject of the Certificate and the entity that contracted with the CA for the Certificate's issuance. Prior to verification of identity and issuance of a Certificate, a Subscriber is an Applicant.

Entrust Datacard will make its services accessible to all Applicants and Subscribers whose activities fall within its declared field of operation and who agree to abide by all obligations as specified in Entrust Datacard's Subscription Agreement and this CPS.

1.3.4 Relying Parties

Relying Parties are entities that act in reliance on a Certificate and/or digital signature. Relying Parties should ensure the Certificate is not expired or revoked before relying on the Certificate or digital signature. Certificate revocation status can be confirmed by checking the appropriate CRL or OCSP response. The location of the CRL distribution point and/or OCSP response is detailed within the Certificate..

1.3.5 Other Participants

The CA may make use of third parties to provide parts of the certification service as described in this CPS. Third parties providing services to support the activities will abide by the current practices declared in this CPS.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

This CPS is applicable to the following Certificate types.

<u>eIDAS QSigC</u>
eIDAS QSigCs issued under this CPS 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.

<u>eIDAS QSealC</u>
eIDAS QSealCs issued under this CPS are aimed to support the advanced electronic seals based on a qualified certificate defined in articles 36 and 37 of the Regulation (EU) No 910/2014.

<u>eIDAS QWAC</u>
eIADS QWACs issued under this CPS are aimed to support website authentication based on a qualified certificate defined in articles 3 (38) and 45 of the Regulation (EU) No 910/2014.

<u>PSD2 Certificates</u>
PSD2 Certificates issued under this CPS 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.

1.4.2 Prohibited Certificate Uses

The use of all Certificates issued by the CA shall be for lawful purposes and consistent with applicable laws, including without limitation, applicable export or import laws.

Certificates and the services provided by Entrust Datacard in respect to Certificates are not designed, manufactured, or intended for use in or in conjunction with hazardous activities or uses requiring fail-safe performance, including the operation of nuclear facilities, aircraft navigation or communications systems, air traffic control, medical devices or direct life support machines.

Certificates issued under this CPS may not be used for "traffic management" or "man-in-the-middle" purposes.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The CPS is administered by the Policy Authority; it is based on the policies established by Entrust Datacard Europe S.L.

1.5.2 Contact Person

The contact information for questions about Certificates is:

Entrust Datacard Limited
1000 Innovation Drive
Ottawa, Ontario
Canada K2K 3E7
Attn: Entrust Certificate Services

Tel: 1-866-267-9297 or 1-613-270-2680
Email: ecs.support@entrustdatacard.com

Certificate Problem Reports, such as Certificate misuse, vulnerability reports or external reports of key compromise, must be emailed to ecs.support@entrustdatacard.com.

1.5.3 Person Determining CPS Suitability for the Policy

The Policy Authority determines the suitability and applicability of this CPS. The Policy Authority shall ensure the CPS meets the requirements of any applicable Certificate Policy.

1.5.4 CPS Approval Procedures

This CPS and any subsequent changes shall be approved by the Policy Authority.

This CPS will be published to the Entrust Datacard Repository, where it may be viewed by all Applicants, Subscribers, Relying Parties, and other third parties. After changes to this CPS have been approved by the Policy Authority they will be circulated to those Entrust Datacard employees, agents, and third parties who participate in providing the services provided herein and are affected by the changes.

Entrust Datacard may (i) revise the terms of this CPS; and/or (ii) change part of the services provided herein at any time. Any such change will be binding and effective immediately upon publication of the change in Entrust Datacard's Repository. If you do not agree with the change, you should terminate your use of or reliance on any Entrust Datacard Certificate immediately. By continuing to use or rely on any Entrust Datacard Certificate after such change, you agree to abide by and be bound thereby. Applicants, Subscribers, Relying Parties, and other third parties should look for updated versions of this CPS from time to time by checking our Repository. These provisions apply to all Applicants, Subscribers, Relying Parties, and other third parties.

1.6 Definitions and Acronyms

1.6.1 Definitions

Affiliate: means collectively, Entrust Datacard Corporation and any person or entity that directly, or indirectly through one or more intermediaries, controls, is controlled by or is under common control with a party hereto. In this context, a party "controls" a corporation or another entity if it directly or indirectly owns or controls fifty percent (50%) or more of the voting rights for the board of directors or other mechanism of control or, in the case of a non-corporate entity, an equivalent interest.

Applicant: means a person, entity, or organization applying for a Certificate, but which has not yet been issued a Certificate, or a person, entity, or organization that currently has a Certificate or Certificates and that is applying for renewal of such Certificate or Certificates or for an additional Certificate or Certificates.

Applicant Representative: as defined in the Baseline Requirements.

Application Software Vendor: means a developer of Internet browser software or other software that displays or uses Certificates.

Attestation Letter: as defined in the Baseline Requirements.

Authorization Domain Name: as defined in the Baseline Requirements.

Authorized Port: as defined in the Baseline Requirements.

Authorized Representative: An authorized representative of a legal person.

Base Domain Name: as defined in the Baseline Requirements.

Baseline Requirements: means the CA/Browser Forum Guidelines Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org. The Baseline Requirements describe certain minimum requirements that a CA must meet in order to issue SSL Certificates. In the event of any inconsistency between this CPS and the Baseline Requirements, the Baseline Requirements take precedence over this CPS.

Business Day: means any day, other than a Saturday, Sunday, statutory or civic holiday in the City of Madrid, Spain.

Certificate: means a digital document issued by the CA that, at a minimum: (a) identifies the CA issuing it, (b) names or otherwise identifies a Subject, (c) contains a Public Key of a Key Pair, (d) identifies its operational period, and (e) contains a serial number and is digitally signed by a CA. Certificate includes, without limitation, the following Certificate types issued by the CA; Qualified Certificate and PSD2 Certificate.

Certificate Application: means the form and application information requested by an RA operating under a CA and submitted by an Applicant when applying for the issuance of a Certificate.

Certificate Approver: means an employee or agent authorized to approve a request for a Certificate for an organization.

Certificate Beneficiaries: means, collectively, all Application Software Vendors with whom Entrust Datacard has entered into a contract to include its root Certificate(s) in software distributed by such Application Software Vendors, and all Relying Parties that actually rely on such Certificate during the Operational Period of such Certificate.

Certificate Requester: means an employee or agent authorized to request a Certificate for an organization.

Certificate Revocation List: means a time-stamped list of the serial numbers of revoked Certificates that has been digitally signed by a CA.

Certificate Problem Report: as defined in the Baseline Requirements.

Certificate Transparency: a method for publicly logging Certificates in accordance with IETF RFC 6962.

Certification Authority: means a certification authority operated by or on behalf of Entrust Datacard for the purpose of issuing, managing, revoking, renewing, and providing access to Certificates. The CA (i) creates and digitally signs Certificates that contain among other things a Subject's Public Key and other information that is intended to identify the Subject, (ii) makes Certificates available to facilitate communication with the Subject identified in the Certificate, and (iii) creates and digitally signs Certificate Revocation Lists containing information about Certificates that have been revoked and which should no longer be used or relied upon.

Certification Practice Statement: means this document, which is a statement of the practices that the CA uses in issuing, managing, revoking, renewing, and providing access to Certificates, and the terms and conditions under which the CA makes such services available.

Co-marketers: means any person, entity, or organization that has been granted by Entrust Datacard or an RA operating under a CA the right to promote Certificates.

Compromise: means a suspected or actual loss, disclosure, or loss of control over sensitive information or data.

Contract Signer: means an employee or agent authorized to sign the subscription agreement on behalf of the organization.

Cross Certificate(s): as defined in the Baseline Requirements.

Domain Contact: as defined in the Baseline Requirements.

Domain Name Registrant: as defined in the Baseline Requirements.

Domain Name Registrar: as defined in the Baseline Requirements.

DNS CAA Email Contact: as defined in the Baseline Requirements.

DNS CAA Phone Contact: as defined in the Baseline Requirements.

DNS TXT Record Email Contact: as defined in the Baseline Requirements.

DNS TXT Record Phone Contact: as defined in the Baseline Requirements.

Enterprise RA: as defined in the Baseline Requirements.

Entrust: means Entrust Datacard Limited.

Entrust.net: means Entrust Datacard Limited.

Entrust Datacard: means Entrust Datacard Europe S.L.

Entrust Datacard Group: Collectively Entrust Holdings, Inc., its subsidiaries, its licensors (including for the avoidance of any doubt Microsoft), its resellers, its suppliers, and the directors, officers, employees, agents and independent contractors of any of them.

Entrust Datacard Group Affiliates: Collectively, Entrust Datacard Limited and Affiliates.

ETSI Guidelines: Collectively, the ETSI guidelines as contained in ETSI EN 319 411-1 (V1.2.2); ETSI EN 319 411-2 (V2.2.2); ETSI TS 119 495 (V1.3.1) and related documents that apply to Qualified Certificates and PSD2 Certificates.

EV SSL Certificate: means an SSL Certificate issued by a CA meeting the requirements of the EV SSL Guidelines.

EV SSL Guidelines: means the CA/Browser Forum Guidelines For The Issuance and Management of Extended Validation Certificates published at http://www.cabforum.org. The EV SSL Guidelines describe the requirements that a CA must meet in order to issue EV SSL Certificates. In the event of any inconsistency between this CPS and the EV SSL Guidelines, the EV SSL Guidelines take precedence over this CPS.

FIPS: means the Federal Information Processing Standards. These are U.S. Federal standards that prescribe specific performance requirements, practices, formats, communication protocols, and other requirements for hardware, software, data, and telecommunications operation.

Fully-Qualified Domain Name: as defined in the Baseline Requirements.

IETF: means the Internet Engineering Task Force. The Internet Engineering Task Force is an international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the efficient operation of the Internet.

Internal Name: as defined in the Baseline Requirements.

IP Address: as defined in the Baseline Requirements.

IP Address Contact: as defined in the Baseline Requirements.

IP Address Registration Authority: as defined in the Baseline Requirements.

Issuing CA: In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.

Key Compromise: as defined in the Baseline Requirements.

Key Pair: means two mathematically related cryptographic keys, having the properties that (i) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is believed to be computationally infeasible to discover the other key.

National Competent Authority: as used under ETSI TS 119 495.

Object Identifier: means a specially-formatted sequence of numbers that is registered in accordance with internationally-recognized procedures for object identifier registration.

Operational Period: means, with respect to a Certificate, the period of its validity. The Operational Period would typically begin on the date the Certificate is issued (or such later date as specified in the Certificate), and ends on the date and time it expires as noted in the Certificate or earlier if the Certificate is Revoked.

Parent Company: as defined in the Baseline Requirements.

PKIX: means an IETF Working Group developing technical specifications for PKI components based on X.509 Version 3 Certificates.

Policy Authority: means those personnel who work for or on behalf of Entrust Datacard and who are responsible for determining the policies and procedures that govern the operation of the CAs. The Policy Authority is responsible for creating, implementing, and maintaining a statement of the practices and procedures used to address all the requirements identified for the applicable Entrust Datacard policy and its work is supervised by the senior executive management of Entrust Datacard S.L."

Private Key: means the key of a Key Pair used to decrypt an encrypted message. This key must be kept secret.

PSD2 Certificates: means PSD2 Qualified Web Authentication Certificate(s) and/or PSD2 Qualified Seal Certificate(s).

PSD2 Qualified Seal Certificate: means a Qualified Seal Certificate which is additionally issued under the requirements of 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.

PSD2 Qualified Web Authentication Certificate: means a Qualified Web Authentication Certificate which is additionally issued under the requirements of 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.

Public Key: means the key of a Key Pair used to encrypt a message. The Public Key can be made freely available to anyone who may want to send encrypted messages to the holder of the Private Key of the Key Pair. The Public Key is usually made publicly available in a Certificate issued by a CA and is often obtained by accessing a repository or database. A Public Key is used to encrypt a message that can only be decrypted by the holder of the corresponding Private Key.

Qualified Certificate: means eIDAS Qualified Web Authentication Certificate(s), eIDAS Qualified Seal Certificate(s) and/or eIDAS Qualified Signature Certificate.

Qualified Seal Certificate: means a Certificate issued for use as a qualified seal certificate as defined in eIDAS (Regulation (EU) No 910/2014), including Annex III and the requirements of ETSI EN 319 411-2 and related ETSI Guidelines

Qualified Signature Certificate: means a Certificate issued for use as a qualified signature certificate as defined in eIDAS (Regulation (EU) No 910/2014), including Annex I and the requirements of ETSI EN 319 411-2 and related ETSI Guidelines

Qualified Web Authentication Certificate: means a Certificate issued for use as a qualified web authentication certificate as defined in eIDAS (Regulation (EU) No 910/2014), including Annex IV and the requirements of ETSI EN 319 411-2 and related ETSI Guidelines.

Random Value: as defined in the Baseline Requirements.

Registration Authority: means an entity that performs two functions: (1) the receipt of information from a Subject to be named in a Certificate, and (2) the performance of verification of information provided by the Subject following the procedures prescribed by the CAs. In the event that the information provided by a Subject satisfies the criteria defined by the CAs, an RA may send a request to a CA requesting that the CA generate, digitally sign, and issue a Certificate containing the information verified by the RA. An RA may be operated by Entrust Datacard or by an independent third-party.

Reliable Data Source: as defined in the Baseline Requirements.

Relying Party: means a person, entity, or organization that relies on or uses a Certificate and/or any other information provided in a Repository under a CA to obtain and confirm the Public Key and identity of a Subscriber. For avoidance of doubt, an ASV is not a "Relying Party" when software distributed by such ASV merely displays information regarding a Certificate.

Relying Party Agreement: means the agreement between a Relying Party and Entrust Datacard or between a Relying Party and an independent third-party RA or Reseller under a CA in respect to the provision and use of certain information and services in respect to Certificates.

Repository: means a collection of databases and web sites that contain information about Certificates issued by a CA including among other things, the types of Certificates and services provided by the CA, fees for the Certificates and services provided by the CA, Certificate Revocation Lists, OCSP responses, descriptions of the practices and procedures of the CA, and other information and agreements that are intended to govern the use of Certificates issued by the CA.

Request Token: as defined in the Baseline Requirements.

Request Value: as defined in the Baseline Requirements.

Required Website Content: as defined in the Baseline Requirements.

Resellers: means any person, entity, or organization that has been granted by Entrust Datacard or an RA operating under a CA the right to license the right to use Certificates.

Reserved IP Address: as defined in the Baseline Requirements.

Revoke or Revocation: means, with respect to a Certificate, to prematurely end the Operational Period of that Certificate from a specified time forward.

Root CA: mean the top level CAs listed in §1.3.1.

SSL Certificate: means a Certificate issued by a CA for use on secure servers.

Subordinate CA: means collectively, the subordinate CAs listed in §1.3.1.

Subordinate CA Certificate: shall mean a Certificate that (i) includes the Public Key of a Public-Private Key Pair generated by a certification authority; and (ii) includes the digital signature of a Root CA.

Subject: means a person, entity, or organization whose Public Key is contained in a Certificate.

Subscriber: means a person, entity, or organization that has applied for and has been issued a Certificate.

Subscription Agreement: means the agreement between a Subscriber and Entrust Datacard (or an Affiliate of Entrust Datacard) or between a Subscriber and an independent third-party RA or Reseller under a CA in respect to the issuance, management, and provision of access to a Certificate and the provision of other services in respect to such Certificate.

Subsidiary Company: as defined in the Baseline Requirements.

Technically Constrained Subordinate CA: as defined in the Baseline Requirements.

Validation Specialist: as defined in the Baseline Requirements.

Wildcard Domain Name: A Domain Name consisting of a single asterisk character followed by a single full stop character ("*.") followed by a Fully-Qualified Domain Name.

1.6.2 Acronyms

ADN	Authorization Domain Name
ASV	Application Software Vendor
CA	Certification Authority
CAA	Certification Authority Authorization
CPR	Certificate Problem Report
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request

CT	Certificate Transparency
DBA	Doing Business As
DN	Distinguished Name
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
EAL	Evaluation Assurance Level
eIDAS	Electronic Identification, Authentication and Trust Services
EKU	Extended Key Usage
ETSI	European Telecommunications Standards Institute
EV	Extended Validation
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
NCA	National Competent Authority
NIST	(US Government) National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PA	Policy Authority
PSD2	(Revised) Payment Services Directive
PDS	PKI Disclosure Statement
PIN	Personal Identification Number
PKI	Public-Key Infrastructure
PSP	Payment Service Provider
QSealC	Qualified Seal Certificate
QSigC	Qualified Signature Certificate
QWAC	Qualified Web Authentication Certificate
RA	Registration Authority
RFC	Request for Comment
RSA	Rivest–Shamir–Adleman cryptosystem
SAN	Subject Alternative Name
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TSA	Time-Stamp Authority
URL	Universal Resource Locator

2. Publication and Repository Responsibilities

Entrust Datacard maintains the Repository to store various information related to Certificates and the operation of the CAs and RAs. The CPS and various other related information is published in the Repository.

2.1 Repositories

The CAs maintain the Repositories to allow access to Certificate-related and Certificate revocation information. The information in the Repositories is accessible through a web interface, available on a 24x7 basis and is periodically updated as set forth in this CPS. The Repositories are the only approved source for CRL and other information about Certificates.

The CA will adhere to the latest version of the CPS published in the Repository.

The Repository can be accessed at https://www.entrust.net/CPS.

Web pages that can be used by ASVs to test their software with Certificates that chain up to each publicly trusted Root Certificate are hosted at https://www.entrust.net/CPS.

2.2 Publication of Certification Information

The CA publishes its CPS, CA Certificates, Subscription Agreements, PKI Disclosure Statement, Relying Party Agreements, and CRLs in the Repositories.

2.3 Time or Frequency of Publications

The CPS will be re-issued and published at least once per year.

CRLs will be updated as per §4.9.7.

OCSP responses will be updated as per §4.9.10.

2.4 Access Controls on Repositories

Information published in the Repository is public information. Read only access is unrestricted. The CAs have implemented logical and physical controls to prevent unauthorized write access to its Repositories.

3. Identification and Authentication

The Policy Authority mandates the verification practices for verifying identification and authentication, and may, in its discretion, update such practices.

3.1 Naming

Before issuing an Certificate, the CAs ensure that all Subject organization information in the Certificate conforms to the requirements of, and has been verified in accordance with the procedures prescribed in this CPS and matches the information confirmed and documented by the RA pursuant to its verification processes.

eIDAS QWAC and PSD2 QWAC

The CA and RA must follow the verification procedures in this CPS, the EV SSL Guidelines, and the ETSI Guidelines and match the information confirmed and documented by the RA pursuant to its verification processes. Such verification procedures are intended to accomplish the following:

(i) Verify the Applicant's existence and identity, including;
   a. Verify the Applicant's legal existence and identity (as stipulated in the EV SSL Guidelines and ETSI Guidelines),
   b. Verify the Applicant's physical existence (business presence at a physical address) , and
   c. Verify the Applicant's operational existence (business activity).

(ii) Verify the Applicant's authorization for the Certificate, including;
   a. Verify the name, title, and authority of the Contract Signer, Certificate Approver, and Certificate Requester;
   b. Verify that Contract Signer signed the Subscription Agreement; and
   c. Verify that a Certificate Approver has signed or otherwise approved the Certificate request.

(iii) For PSD2 QWAC, verify the additional information required by ETSI TS 119 495, including the Applicant's organizationIdentifier assigned by an NCA and the Applicant's approved payment service provider roles.

3.1.1 Types of Names

The Subject names in a Certificate comply with the X.501 Distinguished Name (DN) form. The CAs shall use a single naming convention as set forth below.

Qualified Signature Certificates

(i) "Country Name" (C) which is the two-letter ISO 3166 code for the country in which the Applicant is located;
(ii) "State" (ST) (if applicable), which is the state or province of the organization's place of business;
(iii) "Locality" (L), which is the city or locality of the organization's place of business;
(iv) "Organization Name" (O) which is the name of the organization in the case of a corporation, partnership, or other entity. In the case of a sole proprietorship, the organization name can be the name of the Applicant;
(v) "Organizational Unit Name" (OU) which is an optional field. The OU field may be used to distinguish between different organizational groups within an organization (for example, to distinguish between human resources, marketing, and development);
(vi) "Surname" which is the validated surname of the Subject:
(vii) "First Name" which is the validated first name of the Subject;
(viii) "Serial Number" which is randomly generated and assigned to the Subject
(ix) "Common Name" (CN) which is the first name and the surname of the Subject .

Qualified Seal Certificates

(i) "Country Name" (C) which is the two-letter ISO 3166 code for the country in which the Applicant is located;

(ii) "State" (ST) (if applicable), which is the state or province of the organization's place of business;
(iii) "Locality" (L), which is the city or locality of the organization's place of business;
(iv) "Organization Name" (O) which is the name of the organization in the case of a corporation, partnership, or other entity. In the case of a sole proprietorship, the organization name can be the name of the Applicant;
(v) "Organization Identifier" which is the Organization Identifier;
(vi) "Organizational Unit Name" (OU) which is an optional field. The OU field may be used to distinguish between different organizational groups within an organization (for example, to distinguish between human resources, marketing, and development);
(vii) "Common Name" (CN) which is commonly used by the subject to represent itself .

Qualified Web Authentication Certificates

(i) "Country Name" (C) which is the two-letter ISO 3166 code for the country in which the Applicant is located and plans to host the secure server on which the Applicant is intending to install the Certificate;
(ii) "Organization Name" (O) which is the name of the organization in the case of a corporation, partnership, or other entity. In the case of a sole proprietorship, the organization name can be the name of the Applicant;
(iii) "Organizational Unit Name" (OU) which is an optional field. The OU field may be used to distinguish between different organizational groups within an organization (for example, to distinguish between human resources, marketing, and development);
(iv) "Common Name" (CN) which is the hostname, the fully qualified hostname or path used in the DNS of the secure server on which the Applicant is intending to install the Certificate;
(v) "Locality" (L), which is the city or locality of the organization's place of business; and
(vi) "State" (ST) (if applicable), which is the state or province of the organization's place of business.
(vii) "serialNumber" which is the registration number of Subscriber,
(viii) "businessCategory" which is the applicable business category clause per the EV SSL Guidelines,
(ix) "jurisdictionOfIncorporationLocalityName" (if applicable) which is the jurisdiction of registration or incorporation locality of Subscriber,
(x) "jurisdictionOfIncorporationStateOrProvinceName" (if applicable) which is the jurisdiction of registration or incorporation state or province of Subscriber, and
(xi) "jurisdictionOfIncorporationCountry" which is the jurisdiction of registration or incorporation country of Subscriber.

PSD2 Certificates

(i) Same as Qualified Seal Certificate or Qualified Web Authentication Certificates, plus
(ii) Applicant's "organizationIdentifier" assigned by an NCA.

3.1.2 Need for Names to be Meaningful

The Certificates issued pursuant to this CPS are meaningful only if the names that appear in the Certificates can be understood and used by Relying Parties. Names used in the Certificates must identify the person or object to which they are assigned in a meaningful way. CAs shall not issue Certificates to the Subscribers that contain domain names, IP Addresses, DN, URL, and/or e-mail addresses that the Subscribers do not legitimately own or control. Examples of fields and extensions where these names appear include subject DN and subject alternative names.

eIDAS QSigC

The value of the Common Name to be used in eIDAS QSigC shall be the Subject's first name and surname.

eIDAS QSEalC and PSD2 QSealC

The value of the Common Name to be used in eIDAS QSealC and PSD2 QSealC shall be the Applicant's organization name.

eIDAS QWAC and PSD2 QWAC

The value of the Common Name to be used in an eIDAS QWAC or PSD2 QWAC shall be the Applicant's FQDN that is used in the DNS of the secure server on which the Applicant is intending to install the Certificate. The FQDN for an eIDAS QWAC or PSD2 QWAC cannot be an IP address or a Wildcard Domain Name.

3.1.3 Anonymity or Pseudonymity of Subscribers

No stipulation.

3.1.4 Rules for Interpreting Various Name Forms

No stipulation.

3.1.5 Uniqueness of Names

Names shall be defined unambiguously for each Subject in a Repository. The Distinguished Name attribute will usually be unique to the Subject to which it is issued. Each Certificate shall be issued a unique serial number within the name space of the Subordinate CA.

3.1.6 Recognition, Authentication, and Role of Trademarks

The Subject names in Certificates are issued on a "first come, first served" basis. By accepting a Subject name for incorporation into a Certificate, an RA operating under a CA does not determine whether the use of such information infringes upon, misappropriates, dilutes, unfairly competes with, or otherwise violates any intellectual property right or any other rights of any person, entity, or organization. The CAs and any RAs operating under the CAs neither act as an arbitrator nor provide any dispute resolution between Subscribers or between Subscribers and third-party complainants in respect to the use of any information in an Certificate. The CPS does not bestow any procedural or substantive rights on any Subscriber or third-party complainant in respect to any information in a Certificate. Neither the CAs nor any RAs operating under the CAs shall in any way be precluded from seeking legal or equitable relief (including injunctive relief) in respect to any dispute between Subscribers or between Subscribers and third-party complainants or in respect to any dispute between Subscribers and a CA or an RA operating under a CA or between a third-party complainant and a CA or an RA operating under a CA arising out of any information in an Certificate. The CAs and RAs operating under the CAs shall respectively have the right to revoke and the right to request revocation of Certificates upon receipt of a properly authenticated order from an arbitrator or court of competent jurisdiction requiring the revocation of a Certificate.

A CA or an RA operating under a CA may, in certain circumstances, take action in respect to a Certificate containing information that possibly violates the trademark rights of a third-party complainant. In the event that a third-party complainant provides a CA or an RA operating under a CA with (i) a certified copy that is not more than three (3) months old of a trademark registration from the principal trademark office in any one of the United States, Canada, Japan, Australia or any of the member countries of the European Union, and further provided that such registration is still in full force and effect, and (ii) a copy of a prior written notice to the Subscriber of the Certificate in dispute, stating that the complainant believes that information in the Subscriber's Certificate violates the trademark rights of the complainant, and (iii) a representation by the complainant indicating the means of notice and basis for believing that such notice was received by the Subscriber of the Certificate in dispute, a CA or an RA operating under a CA may initiate the following actions. The CA or the RA operating under a CA may determine whether the issue date of the Subscriber's Certificate predates the registration date on the trademark registration provided by the complainant. If the date of issuance of the Subscriber's Certificate predates the trademark registration date, the CA or the RA operating under the CA will take no further action unless presented with an authenticated order from an arbitrator or court of competent jurisdiction. If the date of issuance of the Certificate is after the registration date on the trademark registration provided by the complainant, the CA or the RA operating under the CA shall request that the Subscriber provide a proof of ownership for the Subscriber's own corresponding trademark registration from the principal trademark office in any one of the United States, Canada, Japan, Australia or any of the member countries of the European Union. If the Subscriber can provide a certified copy, as set forth above, that predates or was issued on the same date as the complainant's trademark registration, the CA or the RA operating under the CA will take no further action

unless presented with an authenticated order from an arbitrator or court of competent jurisdiction. If the Subscriber does not respond within ten (10) Business Days, or if the date on the certified copy of the trademark registration provided by the Subscriber postdates the certified copy of the trademark registration provided by the complainant, the CA and the RAs operating under that CA respectively may revoke or may request revocation of the disputed Certificate.

If a Subscriber files litigation against a complainant, or if a complainant files litigation against a Subscriber, and such litigation is related to any information in an issued Certificate, and if the party instigating the litigation provides a CA or an RA operating under a CA with a copy of the file-stamped complaint or statement of claim, the CA will maintain the current status of the Certificate or the RA operating under the CA will request that the CA maintain the current status of the Certificate, subject to any requirements to change the status of such Certificate otherwise provided or required under this CPS, a Subscription Agreement, or any Relying Party Agreement. During any litigation, a CA will not revoke and an RA operating under a CA will not request revocation of a Certificate that is in dispute unless ordered by an arbitrator or a court of competent jurisdiction or as otherwise provided or required under this CPS, a Subscription Agreement, or any Relying Party Agreement. In the event of litigation as contemplated above, the CAs and RAs operating under the CAs will comply with any directions by a court of competent jurisdiction in respect to a Certificate in dispute without the necessity of being named as a party to the litigation. If named as a party in any litigation in respect to a Certificate, Entrust Datacard and/or any third party operating an RA under a CA shall be entitled to take any action that it deems appropriate in responding to or defending such litigation. Any Subscriber or Relying Party that becomes involved in any litigation in respect to a Certificate shall remain subject to all of the terms and conditions of the CPS, the Subscriber's Subscription Agreement, and the Relying Party's Relying Party Agreement.

RAs operating under a CA shall notify the CA of any disputes of which such RA is aware and which relate to any information contained in a Certificate whose issuance was requested by such RA.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

For Key Pairs generated by the Applicant, the CAs perform proof of possession tests for CSRs created using reversible asymmetric algorithms (such as RSA) by validating the signature on the CSR submitted by the Applicant with the Certificate Application.

3.2.2 Authentication of Organization Identity

3.2.2.1 Identity

RAs operating under the CAs shall perform verification of any organizational identities that are submitted by an Applicant or Subscriber in accordance with the practices mandated by the Policy Authority. RAs operating under the CAs shall determine whether the organizational identity, address, and domain name provided with a Certificate Application are consistent with information contained in third-party databases and/or governmental sources. The information and sources used for the verification of Certificate Applications may vary depending on the jurisdiction of the Applicant or Subscriber.

In the case of organizational identities that are not registered with any governmental sources, RAs operating under the CAs shall use commercially reasonable efforts to confirm the existence of the organization. Such commercially reasonable efforts may include site visits or third-party attestation letter.

<u>eIDAS QWAC and PSD2 QWAC</u>
The CA or RA will identify the organization and, if applicable, any specific attributes of the organization, will be verified by an Authorized Representative.

<u>eeIDAS QWAC</u>
RAs operating under the CAs shall also determine:

(i) Business Category;

(ii) Jurisdiction of Incorporation or Registration;
(iii) Registration Number;
(iv) Physical address of Place of Business; and
(v) Operational Existence.

PSD2 Certificates
RAs operating under the CAs shall also determine:
(vi) Applicable NCA;
(vii) organizationIdentifier assigned by the NCA; and
(viii) Payment service provider roles approved by the NCA.
Note: RAs shall conform to the specific NCA rules for verifying these attributes.

3.2.2.2 DBA/Tradename

If the subject identity information is to include a DBA or tradename, the RA must verify the Applicant's right to use the DBA/tradename using at least one of the following:

(i) The RA may verify the assumed name through use of a Qualified Government Information Source operated by, or on behalf of, an appropriate government agency in the jurisdiction of the Applicant's Place of Business, or by direct contact with such government agency in person or via mail, e-mail, Web address, or telephone; or
(ii) The RA may verify the assumed name through use of a Qualified Independent Information Source provided that the QIIS has verified the assumed name with the appropriate government agency.
(iii) The RA may rely on a Verified Professional Letter that indicates the assumed name under which the Applicant conducts business, the government agency with which the assumed name is registered, and that such filing continues to be valid.

3.2.2.3 Verification of Country

Verification of country will be done in accordance with the methods of § 3.2.2.1.

3.2.2.4 Validation of Domain Authorization or Control

The CA shall confirm that prior to issuance, the CA or the RA validated each Fully-Qualified Domain Name (FQDN) listed in the Certificate using at least one of the methods listed below.

Completed validations of Applicant authority may be used for the issuance of multiple Certificates over time. For purposes of domain validation, the term Applicant includes the Applicant's Parent Company, Subsidiary Company, or Affiliate.

The CA shall maintain a record of which domain validation method was used to validate every domain.

3.2.2.4.1 Validating the Applicant as a Domain Contact

This method of domain validation is not used.

3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact

Confirm the Applicant's control over the FQDN by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value. The Random Value must be sent to an email address, fax/SMS number, or postal mail address identified as a Domain Contact.

Each email, fax, SMS, or postal mail may confirm control of multiple ADNs.

The CA or RA may send the email, fax, SMS, or postal mail identified under this section to more than one recipient provided that every recipient is identified by the Domain Name Registrar as representing the Domain Name Registrant for every FQDN being verified using the email, fax, SMS, or postal mail.

The Random Value is unique in each email, fax, SMS, or postal mail.

The CA or RA may resend the email, fax, SMS, or postal mail in its entirety, including re-use of the Random Value, provided that the communication's entire contents and recipient(s) remain unchanged.

The Random Value will remain valid for use in a confirming response for no more than 30 days from its creation.

3.2.2.4.3 Phone Contact with Domain Contact

Confirm the Applicant's control over the FQDN by calling the Domain Name Registrant's phone number and obtaining a response confirming the Applicant's request for validation of the FQDN. The CA or RA shall place the call to a phone number identified by the Domain Name Registrar as the Domain Contact.

Each phone call shall be made to a single number and may confirm control of multiple FQDNs, provided that the phone number is identified by the Domain Registrar as a valid contact method for every Base Domain Name being verified using the phone call.

This method will not be re-used after May 31, 2019.

3.2.2.4.4 Constructed Email to Domain Contact

Confirm the Applicant's control over the FQDN by (i) sending an email to one or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at-sign ("@"), followed by an ADN, (ii) including a Random Value in the email, and (iii) receiving a confirming response utilizing the Random Value.

Each email may confirm control of multiple FQDNs, provided the ADN used in the email is an ADN for each FQDN being confirmed.

The Random Value shall be unique in each email.

The email may be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient shall remain unchanged.

The Random Value shall remain valid for use in a confirming response for no more than 30 days from its creation.

3.2.2.4.5 Domain Authorization Document

This method of domain validation is not used.

3.2.2.4.6 Agreed-Upon Change to Website

This method of domain validation is not used.

3.2.2.4.7 DNS Change

Confirm the Applicant's control over the FQDN by confirming the presence of a Random Value in a DNS CNAME, TXT or CAA record for an ADN or an ADN that is prefixed with a label that begins with an underscore character.

If a Random Value is used, the CA or RA shall provide a Random Value unique to the Certificate request and shall not use the Random Value after (i) 30 days or (ii) if the Applicant submitted the Certificate request, the timeframe permitted for reuse of validated information relevant to the Certificate.

3.2.2.4.8 IP Address

Confirming the Applicant's control over the FQDN by confirming that the Applicant controls an IP Address returned from a DNS lookup for A or AAAA records for the FQDN in accordance with § 3.2.2.5.

Once the FQDN has been validated using this method, the CA MAY NOT also issue Certificates for FQDNs for higher level domain levels that end in the validated FQDN unless the CA performs a separate validation for that FQDN using an authorized method. This method is NOT suitable for validating Wildcard Domain Names.

3.2.2.4.9 Test Certificate

This method of domain validation is not used.

3.2.2.4.10 TLS Using a Random Number

This method of domain validation is not used.

3.2.2.4.11 Any Other Method

This method of domain validation is not used.

3.2.2.4.12 Validating Applicant as a Domain Contact

This method of domain validation is not used.

3.2.2.4.13 Email to DNS CAA Contact

Confirm the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value will be sent to a DNS CAA Email Contact. The relevant CAA Resource Record Set will be found using the search algorithm defined in RFC 6844 Section 4, as amended by Errata 5065 (Appendix A).

Each email may confirm control of multiple FQDNs, provided that each email address is a DNS CAA Email Contact for each ADN Name being validated. The same email may sent to multiple recipients as long as all recipients are the DNS CAA Email Contacts for each ADN being validated.

The Random Value shall be unique in each email. The email may be re-sent in its entirety, including the reuse of the Random Value, provided that its entire contents and recipient(s) remain unchanged. The Random Value shall remain valid for use in a confirming response for no more than 30 days from its creation.

3.2.2.4.14 Email to DNS TXT Contact

Confirm the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value will be sent to a DNS TXT Record Email Contact for the ADN selected to validate the FQDN.

Each email may confirm control of multiple FQDNs, provided that each email address is DNS TXT Record Email Contact for each ADN being validated. The same email may be sent to multiple recipients as long as all recipients are the DNS TXT Record Email Contacts for each ADN being validated.

The Random Value shall be unique in each email. The email may be re-sent in its entirety, including the reuse of the Random Value, provided that its entire contents and recipient(s) remain unchanged. The Random Value shall remain valid for use in a confirming response for no more than 30 days from its creation.

3.2.2.4.15 Phone with Domain Contact

Confirm the Applicant’s control over the FQDN by calling the Domain Contact’s phone number and obtain a confirming response to validate the ADN. Each phone call may confirm control of multiple ADNs provided that the same Domain Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN.

In the event that someone other than a Domain Contact is reached, the CA may request to be transferred to the Domain Contact.

In the event of reaching voicemail, the CA may leave the Random Value and the ADN(s) being validated. The Random Value must be returned to the CA to approve the request.

The Random Value shall remain valid for use in a confirming response for no more than 30 days from its creation.

3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact

Confirm the Applicant's control over the FQDN by calling the DNS TXT Record Phone Contact's phone number and obtain a confirming response to validate the ADN. Each phone call may confirm control of multiple ADNs provided that the same DNS TXT Record Phone Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN.

The CA may not knowingly be transferred or request to be transferred as this phone number has been specifically listed for the purposes of domain validation.

In the event of reaching voicemail, the CA may leave the Random Value and the ADN(s) being validated. The Random Value must be returned to the CA to approve the request.

The Random Value shall remain valid for use in a confirming response for no more than 30 days from its creation.

3.2.2.4.17 Phone Contact with DNS CAA Phone Contact

Confirm the Applicant's control over the FQDN by calling the DNS CAA Phone Contact's phone number and obtain a confirming response to validate the ADN. Each phone call may confirm control of multiple ADNs provided that the same DNS CAA Phone Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN. The relevant CAA Resource Record Set must be found using the search algorithm defined in RFC 6844 Section 4, as amended by Errata 5065 (Appendix A).

The CA may not knowingly be transferred or request to be transferred as this phone number has been specifically listed for the purposes of domain validation.

In the event of reaching voicemail, the CA may leave the Random Value and the ADN(s) being validated. The Random Value must be returned to the CA to approve the request.

The Random Value shall remain valid for use in a confirming response for no more than 30 days from its creation.

3.2.2.4.18 Agreed-Upon Change to Website v2

Confirm the Applicant's control over the FQDN by verifying that the Request Token or Random Value is contained in the contents of a file.

(i) The entire Request Token or Random Value must not appear in the request used to retrieve the file, and
(ii) the CA MUST receive a successful HTTP response from the request (meaning a 2xx HTTP status code must be received).

The file containing the Request Token or Random Number:

(iii) Must be located on the Authorization Domain Name, and
(iv) Must be located under the "/.well-known/pki-validation" directory, and
(v) Must be retrieved via either the "http" or "https" scheme, and
(vi) Must be accessed over an Authorized Port.

If the CA follows redirects the following apply:

(vii) Redirects must be initiated at the HTTP protocol layer (e.g. using a 3xx status code).

(viii) Redirects must be the result of an HTTP status code result within the 3xx Redirection class of status codes, as defined in RFC 7231, Section 6.4.

(ix) Redirects must be to resource URLs with either via the "http" or "https" scheme.

(x) Redirects must be to resource URLs accessed via Authorized Ports.

If a Random Value is used, then:

(xi) The CA must provide a Random Value unique to the certificate request.

(xii) The Random Value must remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values, in which case the CA must follow its CPS.

Note: Once the FQDN has been validated using this method, the CA may also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.19 Agreed-Upon Change to Website - ACME

This method of domain validation is not used.

3.2.2.5 Authentication of an IP Address

IP addresses are not permitted for Certificates.

3.2.2.6 Wildcard Validation

Wildcards are not permitted for eIDAS QWAC or PSD2 QWAC.

3.2.2.7 Data Source Accuracy

Prior to using any data source as a Reliable Data Source, the RA shall evaluate the source for its reliability, accuracy, and resistance to alteration or falsification.

3.2.2.8 CAA Records

Entrust Datacard policy on CAA records is stated in §4.2.4.

3.2.2.9 Authentication of Email Address

The CA uses one of the following methods to confirm that the Applicant has control of or right to use email addresses:

(i) Sending a URL including a random value to the email address and then receiving an acknowledgement click-through with passphrase on the web page utilizing the random value URL; or

(ii) Using a domain validation process from §3.2.2.4 to demonstrate control over or right to use an FQDN. Once verified, the Enterprise RA can approve issuance of Certificates containing email addresses under that FQDN or associated Base Domain Name.

3.2.2.10 Organization Identifier

The organization identifier must contain a registration reference for a legal entity assigned in accordance to the identified registration scheme.

The registration scheme must be identified using the using the following structure in the presented order:

(i) 3 character registration scheme identifier;

(ii) 2 character ISO 3166 country code for the nation in which the registration scheme is operated, or if the

(iii) scheme is operated globally ISO 3166 code "XG" shall be used;

(iv) For the NTR registration scheme identifier, if required, a 2 character ISO 3166-2 identifier for the subdivision (state or province) of the nation in which the registration scheme is operated, preceded by plus "+" (0x2B (ASCII), U+002B (UTF-8));
(v) a hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8));
(vi) Registration Reference allocated in accordance with the identified Registration Scheme

Note: Registration references may contain hyphens, but registration schemes, ISO 3166 country codes, and ISO 3166-2 identifiers do not. Therefore if more than one hyphen appears in the structure, the leftmost hyphen is a separator, and the remaining hyphens are part of the registration reference.

The CA or RA shall:
(vii) Confirm that the organization represented by the registration reference is the same as the organization named within the context of the Subject's jurisdiction per §3.2.2.1;
(viii) Further verify the registration reference matches other information verified in accordance with §3.2.2;
(ix) Take appropriate measures to disambiguate between different organizations as described in Appendix B for each registration scheme;
(x) Apply the validation rules relevant to the registration scheme as specified in Appendix B.

3.2.3 Authentication of Individual Identity

RAs operating under the CAs shall use the methods set out below to verify any individual identities that are submitted by an Applicant or Subscriber.

The CA or RA will verify the Authorized Representative or Subject by:
(i) Physical presence; or
(ii) Means of a Certificate of a qualified electronic signature or of a qualified electronic seal.

eIDAS QWAC and PSD2 QWAC
RAs operating under the CAs shall perform a verification of the identity and authority of the Contract Signer, the Certificate Approver, and the Certificate Requestor associated with Certificate Applications that are submitted by an Applicant or Subscriber. In order to establish the accuracy of an individual identity, the RA operating under a CA shall perform identity and authority verification consistent with the requirements set forth in the EV SSL Guidelines published by the CA/Browser Forum and the ETSI Guidelines.

3.2.4 Non-verified Subscriber Information

No stipulation.

3.2.5 Validation of Authority

If the Applicant for a Certificate containing subject identity information is an organization, the RA will use a reliable method of communication to verify the authenticity of the Applicant representative's Certificate request.

The RA may use the sources listed in §3.2.2.1 to verify the reliable method of communication. Provided that the RA uses a reliable method of communication, the RA may establish the authenticity of the Certificate request directly with the Applicant representative or with an authoritative source within the Applicant's organization, such as the Applicant's main business offices, corporate offices, human resource offices, information technology offices, or other department that the RA deems appropriate.

The CA allows a Subscriber to specify the individuals who may request Certificates and will not accept any Certificate requests that are outside this specification. The CAs will provide a Subscriber with a list of its authorized Certificate Requesters upon the Subscriber's verified written request.

eIDAS QWAC and PSD2 QWAC
The CA or RA must verify the identity and authority of the Contract Signer and Certificate Approver in accordance with EV SSL Guidelines section 11.8.

3.2.6 Criteria for Interpretation

Externally issued Cross Certificates that identify Entrust Datacard as the subject are disclosed in §1.3.1, provided that Entrust Datacard arranged for or accepted the establishment of the trust relationship (i.e. the Cross Certificate at issue).

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

Each Certificate shall contain a Certificate expiration date. The reason for having an expiration date for a Certificate is to minimize the exposure of the Key Pair associated with the Certificate. For this reason, when processing a new Certificate Application, the CA recommends that a new Key Pair be generated and that the new Public Key of this Key Pair be submitted with the Applicant's Certificate Application. If a Subscriber wishes to continue to use a Certificate beyond the expiry date for the current Certificate, the Subscriber must obtain a new Certificate and replace the Certificate that is about to expire. Subscribers submitting a new Certificate Application will be required to complete the initial application process, as described in §4.1. The RA may reuse documents and data provided in §3.2 to verify Certificate information per §4.2.1.

The RA that processed the Subscriber's Certificate Application shall make a commercially reasonable effort to notify Subscribers of the pending expiration of their Certificate by sending an email to the technical contact listed in the corresponding Certificate Application. Upon expiration of a Certificate, the Subscriber shall immediately cease using such Certificate and shall remove such Certificate from any devices and/or software in which it has been installed.

eIADS QWAC and PSD2 QWAC
The Subscriber may request a replacement Certificate using an existing key pair.

3.3.2 Identification and Authentication for Re-key after Revocation

The CAs and RAs operating under the CAs do not renew Certificates that have been revoked. If a Subscriber wishes to use a Certificate after revocation, the Subscriber must apply for a new Certificate and replace the Certificate that has been revoked. In order to obtain another Certificate, the Subscriber shall be required to complete the initial application process, as described in §4.1. Upon revocation of a Certificate, the Subscriber shall immediately cease using such Certificate and shall remove such Certificate from any devices and/or software in which it has been installed.

3.4 Identification and Authentication for Revocation Requests

A Subscriber may request revocation of their Certificate at any time provided that the Subscriber can validate to the RA that processed the Subscriber's Certificate Application that the Subscriber is the person, organization, or entity to whom the Certificate was issued. The RA shall authenticate a request from a Subscriber for revocation of their Certificate by authenticating the Subscriber or confirming authorization of the Subscriber through a reliable method of communication. Upon receipt and confirmation of such information, the RA shall then process the revocation request as stipulated in §4.9.

An Enterprise RA may use multi-factor authentication to request revocation of a Certificate.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

To obtain a Certificate, an Applicant must:

(i) generate a secure and cryptographically sound Key Pair, if not generated by a CA
(ii) agree to all of the terms and conditions of the CPS and the Subscription Agreement, and
(iii) complete and submit a Certificate Application, providing all information requested by an RA without any errors, misrepresentation, or omissions.

If the Applicant is not the same as the Subject of the Certificate being requested by the Applicant, then both the Applicant and the Subject must agree to all of the terms and conditions of the CPS and the Subscription Agreement.

To avoid any conflicts of interests, the Subscriber and Entrust Datacard shall be separate entities. The only exception is Entrust Datacard running all or part of the RA tasks when subscribing a certificate for itself or for persons identified in association with Entrust Datacard as the Subject.

Upon an Applicant's completion of the Certificate Application and acceptance of the terms and conditions of this CPS and the Subscription Agreement, an RA shall follow the procedures described in §3.2 to perform verification of the information contained in the Certificate Application. If the verification performed by an RA is successful, the RA may, in its sole discretion, request the issuance to the Applicant of a Certificate from a CA. If an RA refuses to request the issuance of a Certificate, the RA shall (i) use commercially reasonable efforts to notify the Applicant by email of any reasons for refusal, and (ii) promptly refund any amounts that have been paid in connection with the Certificate Application.

In the event of successful verification of a Certificate Application, the RA shall submit a request to a CA for the issuance of a Certificate and shall notify the Applicant. The CA will provide the Certificate pickup through either email, URL link or through the API.

<u>eIDAS QWAC and PSD2 QWAC</u>

(iv) Certificate Requester – The Certificate request must be signed and submitted by an authorized Certificate Requester.
(v) Certificate Approver – The Certificate request must be reviewed and approved by an authorized Certificate Approver.
(vi) Contract Signer – A Subscription Agreement applicable to the requested Certificate must be signed by an authorized Contract Signer.

One person may be authorized by the Applicant to fill one, two, or all three of these roles. An Applicant may also authorize more than one person to fill each of these roles.

4.1.1 Who Can Submit a Certificate Application

Either the Applicant or an individual authorized to request Certificates on behalf of the Applicant may submit Certificate requests. Applicants are responsible for any data that the Applicant or an agent of the Applicant supplies to the RA.

The CAs shall identify subsequent suspicious Certificate requests in accordance with the high risk process per §4.2.1.

The CAs do not issue Certificates to any persons or entities on a government denied list maintained by Spain and Canada or that is located in a country with which the laws of Spain or Canada prohibit doing business.

4.1.2 Enrollment Process and Responsibilities

The CAs require each Applicant to submit a Certificate request and application information prior to issuing a Certificate. The CAs or RAs authenticates all communication from an Applicant and protects communication from modification.

Generally, Applicants request a Certificate by completing the request forms online. Applicants are solely responsible for submitting a complete and accurate Certificate request for each Certificate.

The enrollment process includes:

(i) Agreeing to the applicable Subscription Agreement,
(ii) Paying any applicable fees,
(iii) Submitting a complete Certificate application,
(iv) Generating a key pair, and
(v) Delivering the public key of the key pair to the CA.

By executing the Subscription Agreement, Subscribers warrant that all of the information contained in the Certificate request is correct.

The Subscription Agreement may be signed in either of the following two methods:

- If the Subscription Agreement is in electronic form, it will be signed with an online click-through process.
- In the alternative, Subscribers may print and sign a signature page referring to the Subscription Agreement, and email or upload the signed document to Entrust Datacard.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

The CAs and RAs may use the documents and data provided in §3.2 to verify Certificate information.

The CAs maintain procedures to identify high risk Certificate requests that require additional verification activity prior to Certificate issuance. High risk certificate procedures include processes to verify high risk domain names and/or evaluate deceptive domain names.

eIDAS QWAC and PSD2 QWAC
With the exception of PSD2 specific attributes, reuse of previous validation data or documentation obtained from a source specified under §3.2 may be used no more than 13 months after such data or documentation was validated.

PSD2 Certificates
PSD2 specific attributes shall only be used for 30 days after validation is completed.

4.2.2 Approval or Rejection of Certificate Applications

The CAs shall not issue Certificates containing Internal Names.

4.2.3 Time to Process Certificate Applications

No stipulation.

4.2.4 Certification Authority Authorization (CAA) Records

Prior to issuing eIDAS QWAC or PSD2 QWAC, the CA checks for certification authority authorization (CAA) records for each dNSName in the subjectAltName extension of the Certificate to be issued, according to the procedure in RFC 6844, following the processing instructions set down in RFC 6844 for

any records found. If the Certificate is issued, it will be issued within the TTL of the CAA record, or 8 hours, whichever is greater.

When processing CAA records, the CAs process the issue, issuewild, and iodef property tags as specified in RFC 6844. The CA may not act on the contents of the iodef property tag. The CAs respect the critical flag and will not issue a Certificate if they encounter an unrecognized property with this flag set.

The CAs may not check CAA records for the following exceptions:

(i) For Certificates for which a Certificate Transparency pre-certificate was created and logged in at least two public logs, and for which CAA was checked.
(ii) For Certificates issued by a Technically Constrained Subordinate CA Certificate as set out in Baseline Requirements section 7.1.5, where the lack of CAA checking is an explicit contractual provision in the contract with the Applicant.
(iii) If the CA or an Affiliate of the CA is the DNS Operator (as defined in RFC 7719) of the domain's DNS.

The CA treats a record lookup failure as permission to issue if:

(iv) the failure is outside the CA's infrastructure; and
(v) the lookup has been retried at least once; and
(vi) the domain's zone does not have a DNSSEC validation chain to the ICANN root.

The CA documents potential issuances that were prevented by a CAA record in sufficient detail to provide feedback to the CAB Forum on the circumstances, and will dispatch reports of such issuance requests to the contact(s) stipulated in the CAA iodef record(s), if present. The CAs support mailto: and https: URL schemes in the iodef record.

Entrust Datacard CAA identifying domain is '**entrust.net**'.

4.3 Certificate Issuance

After performing verification of the information provided by an Applicant with a Certificate Application, an RA operating under a CA may request that a CA issue a Certificate. Upon receipt of a request from an RA operating under a CA, the CA may generate and digitally sign an Certificate in accordance with the Certificate profile described in §7. An Enterprise RA can approve issuance of Certificates and submit the certificate request to an RA.

Entrust Datacard shall not issue certificates whose lifetime exceeds that of the CA's Certificate.

Upon issuance of a Certificate, neither Entrust Datacard nor any independent third-party RA operating under a CA, nor any Resellers or Co-marketers, or any subcontractors, distributors, agents, suppliers, employees, or directors of any of the foregoing shall have any obligation to perform any ongoing monitoring, investigation, or verification of the information provided in a Certificate Application.

eIDAS QWAC and PSD2 QWAC

The CA assigns a person who is not responsible for the collection of information to review all of the information and documentation assembled in support of the Certificate Application and look for discrepancies or other details requiring further explanation. Upon successful completion of this final cross-correlation and due diligence step, the CA may generate and digitally sign a Certificate.

4.3.1 CA Actions During Certificate Issuance

Certificate issuance by the Root CA shall require an individual authorized by the CA (i.e. the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation.

eIDAS QSigC
If the CA generated the Key Pair, the secure cryptographic device containing the Private Key shall be securely delivered to the registered Subject or, in the case of the CA managing the Private Key on behalf of the Subject, the CA shall ensure that the Subject has sole control over its Private Key.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

Once a Certificate has been generated and placed in a Repository, the RA that requested the issuance of the Certificate shall use commercially reasonable efforts to notify the Applicant by email that the Applicant's Certificate is available. The email may contain a URL for use by the Applicant to retrieve the Certificate.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

No stipulation.

4.4.2 Publication of the Certificate by the CA

No stipulation.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Subordinate CA Certificates
Subordinate CA Certificates shall be disclosed in the CA Common Database (i.e., https://ccadb.force.com) within one week of Certificate issuance.

eIDAS QWAC and PSD2 QWAC
eIDAS QWAC and PSD2 QWAC will include two or more signed certificate timestamps (SCT) from ASV approved independent Certificate Transparency logs.

PSD2 Certificates
If the NCA provides an email address where the CA can inform the NCA identified in a newly issued Certificate then the CA shall send to that email address information on the content of the Certificate in plain text including the Certificate serial number in hexadecimanl, the subject distinguished name, the issuer distinguished name, the Certificate validity period, as well as contact information and instructions for revocation requests and a copy of the Certificate file.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscriber shall conform to §9.6.3.

4.5.2 Relying Party Public Key and Certificate Usage

No stipulation.

4.6 Certificate Renewal

4.6.1 Circumstance for Certificate Renewal

In accordance with the Subscription Agreement, CAs or RAs will provide a Certificate lifecycle monitoring service which will support Certificate renewal.

4.6.2 Who May Request Renewal

Subscribers or Subscriber agents may request renewal of Certificates.

4.6.3 Processing Certificate Renewal Requests

CAs or RAs will process Certificate renewal requests with validated verification data. Previous verification data may be used as specified in §4.2.1.

Certificates may be renewed using the previously accepted Public Key, if the Public Key meets the key size requirements of §6.1.5.

4.6.4 Notification of New Certificate Issuance to Subscriber

CAs or RAs will provide Certificate renewal notification to the Subscriber or Subscriber agents through an Internet link or by email.

Subscribers or Subscriber agents may request that email renewal notices are not sent for their expiring Certificates.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

No stipulation.

4.6.6 Publication of the Renewal Certificate by the CA

CAs or RAs will provide the Subscriber with a Certificate through an Internet link.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.7 Certificate Re-key

4.7.1 Circumstance for Certificate Re-key

No stipulation.

4.7.2 Who May Request Certification of a New Public Key

No stipulation.

4.7.3 Processing Certificate Re-keying Requests

No stipulation.

4.7.4 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

No stipulation.

4.7.6 Publication of the Re-keyed Certificate by the CA

No stipulation.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.8 Certificate Modification

4.8.1 Circumstance for Certificate Modification

No stipulation.

4.8.2 Who May Request Certificate Modification

No stipulation.

4.8.3 Processing Certificate Modification Requests

No stipulation.

4.8.4 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

No stipulation.

4.8.6 Publication of the Modified Certificate by the CA

No stipulation.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.9 Certificate Revocation and Suspension

The CA shall revoke a Certificate after receiving a valid revocation request from an RA operating under such CA. An RA operating under a CA shall be entitled to request and may request that a CA revoke a Certificate after such RA receives a valid revocation request from the Subscriber for such Certificate. An RA operating under a CA shall be entitled to request and shall request that a CA revoke a Certificate if such RA becomes aware of the occurrence of any event that would require a Subscriber to cease to use such Certificate.

CAs do not support the suspension of Certificates.

4.9.1 Circumstances for Revocation

4.9.1.1 Reasons for Revoking a Subscriber Certificate

The CA shall be entitled to revoke and may revoke, and an RA operating under a CA shall be entitled to request revocation of and shall request revocation of, a Subscriber's Certificate if the CA or RA has knowledge of or a reasonable basis for believing that of any of the events listed in this section have occurred.

The CA will revoke a Certificate within 24 hours if one or more of the following occurs:

(i) The Subscriber requests in writing that the CA revoke the Certificate;
(ii) The Subscriber notifies the CA that the original Certificate request was not authorized and does not retroactively grant authorization;
(iii) The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise; or
(iv) The CA obtains evidence that the validation of the domain authorization or control for any FQDN or IP Address in the Certificate should not be relied upon.

The CA should revoke a Certificate within 24 hours and must revoke a Certificate within 5 days if one or more of the following occurs:

(v) The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6;
(vi) The CA obtains evidence that the Certificate was misused;
(vii) The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscription Agreement;

(viii) The CA is made aware of any circumstance indicating that use of a FQDN or IP Address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
(ix) The CA is made aware that a Certificate with a Wildcard Domain Name has been used to authenticate a fraudulently misleading subordinate FQDN;
(x) The CA is made aware of a material change in the information contained in the Certificate;
(xi) The CA is made aware that the Certificate was not issued in accordance with this CPS;
(xii) The CA determines that any of the information appearing in the Certificate is inaccurate;
(xiii) The CA's right to issue Certificates under this CPS expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository;
(xiv) Revocation is required by any other section in this CPS;
(xv) The CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, methods have been developed that can easily calculate it based on the Public Key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys), or if there is clear evidence that the specific method used to generate the Private Key was flawed;
(xvi) The technical content or format of the Certificate presents an unacceptable risk to ASVs or Relying Parties;
(xvii) A Certificate is used to digitally sign hostile code, including spyware or other malicious software (malware); or
(xviii) Any other reason that may be reasonably expected to affect the integrity, security, or trustworthiness of a Certificate or CA.

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

The Issuing CA shall revoke a Subordinate CA Certificate within seven (7) days if one or more of the following occurs:

(i) The Subordinate CA requests revocation in writing;
(ii) The Subordinate CA notifies the Issuing CA that the original Certificate request was not authorized and does not retroactively grant authorization;
(iii) The Issuing CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of §6.1.5 and §6.1.6,
(iv) The Issuing CA obtains evidence that the Certificate was misused;
(v) The Issuing CA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with the Baseline Requirements, EV SSL Guidelines, Minimum Requirements for Code Signing or this CPS;
(vi) The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
(vii) The Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
(viii) The Issuing CA's or Subordinate CA's right to issue Certificates under the Baseline Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository; or
(ix) Revocation is required by the Issuing CA's CPS.

4.9.2 Who Can Request Revocation

CAs, RAs and Subscribers may initiate revocation.

A Subscriber or another appropriately authorized party (such as an administrative contact, a Contract Signer, Certificate Approver, or Certificate Requester) may request revocation of their Certificate at any time for any reason. If a Subscriber requests revocation of their Certificate, the Subscriber must be able to validate themselves as set forth in §3.4 to the RA that processed the Subscriber's Certificate Application. The CAs shall not be required to revoke and the RAs operating under the CAs shall not be required to

request revocation of an Certificate until a Subscriber can properly validate themselves as set forth in §4.9.3. A CA shall be entitled to revoke and shall revoke, and an RA operating under a CA shall be entitled to request revocation of and shall request revocation of, a Subscriber's Certificate at any time for any of the reasons set forth in §4.9.1.

Subscribers, Relying Parties, ASVs, Anti-Malware Organizations and other third parties may submit CPRs informing the CA of a reasonable cause to revoke the Certificate.

4.9.3 Procedure for Revocation Request

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.

A Subscriber request for revocation of their Certificate may be verified by (i) Subscriber authentication credentials, or (ii) authorization of the Subscriber through a reliable method of communication.

If a Subscriber's Certificate is revoked for any reason, the Subscriber shall be notified by sending an email to the technical and security contacts listed in the Certificate Application. Revocation of a Certificate shall not affect any of the Subscriber's contractual obligations under this CPS, the Subscriber's Subscription Agreement, or any Relying Party Agreements.

Subscribers, Relying Parties, ASVs, Anti-Malware Organizations and other third parties may submit a CPR by notification through the contact information specified in §1.5.2. If a CPR is received, the CA shall:

(v) Log the CPR as high severity into a ticketing system for tracking purposes;
(vi) Review the CPR and engage the necessary parties to verify the CPR, draft a CPR investigation report and provide the CPR investigation report to the Subscriber and the party that provided the CPR within 24 hours from receipt of the CPR;
(vii) Determine if there was Certificate mis-issuance. In the case of Certificate miss-issuance, the incident must be 1) escalated to the policy authority team and to service management and 2) a Certificate mis-issuance report must be publicly post within one business day;
(viii) If Certificate revocation is required, perform revocation in accordance with the requirements of §4.9.1.1;
(ix) Update Certificate mis-issuance report within 5 days from receipt of CPR; and
(x) Complete the CPR investigation report when the incident is closed and provide to the Subscriber and the party that provided the CPR.

PSD2 Certificates
Additional provisions concerning revocation of PSD2 Certificates are addressed in §4.9.17.

4.9.4 Revocation Request Grace Period

In the case of Private Key Compromise, or suspected Private Key Compromise, a Subscriber shall request revocation of the corresponding Certificate immediately upon detection of the Compromise or suspected Compromise. Revocation requests for other required reasons shall be made as soon as reasonably practicable.

4.9.5 Time within Which CA Must Process the Revocation Request

Within 24 hours after receiving a CPR, the CA will investigate the facts and circumstances related to the CPR and provide a preliminary report to both the Subscriber and the entity who filed the CPR.

After reviewing the facts and circumstances, the CA will work with the Subscriber and any entity reporting the CPR or other revocation-related notice to establish whether or not the Certificate will be revoked, and if so, a date which the CA will revoke the Certificate. The period from receipt of the CPR or revocation-related notice to published revocation will not exceed the timeframe set forth in §4.9.1.1. The date selected by the CA will consider the following criteria:

(i) The nature of the alleged problem (scope, context, severity, magnitude, risk of harm);
(ii) The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties);
(iii) The number of CPRs received about a particular Certificate or Subscriber;
(iv) The entity making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that they didn't receive the goods they ordered); and
(v) Relevant legislation.

The maximum time between the confirmation of the revocation of a certificate to become effective and the actual change of the status information of the certificate in Entrust's revocation services shall be at most 60 minutes. Entrust Datacard synchronizes its system time at least every 24 hours using a real time value distributed by a recognized UTC(k) laboratory or National Measurement Institute.

4.9.6 Revocation Checking Requirement for Relying Parties

A Relying Party shall check whether the Certificate that the Relying Party wishes to rely on has been revoked. A Relying Party shall check the Certificate Revocation Lists maintained in the appropriate Repository or perform an on-line revocation status check using OCSP to determine whether the Certificate that the Relying Party wishes to rely on has been revoked. In no event shall the Entrust Datacard Group be liable for any damages whatsoever due to (i) the failure of a Relying Party to check for revocation or expiration of a Certificate, or (ii) any reliance by a Relying Party on a Certificate that has been revoked or that has expired.

4.9.7 CRL Issuance Frequency

The CAs shall issue CRLs as follows:

(i) CRLs for Certificates issued to Subordinate CAs shall be issued at least once every twelve months or within 24 hours after revoking a Subordinate CA Certificate. The next CRL update shall not be more than twelve months from the last update.
(ii) CRLs for Certificates shall be issued within 60 minutes of revocation of a certificate, and at least once every 24 hours. The next CRL update is 24 hours from the last update.
(iii) Revocation status information for a Certificate shall be made available beyond the validity period of the certificate. Entrust Datacard will not remove from the CRL revoked certificates after they have expired and the CRL shall include the X.509 "ExpiredCertsOnCRL" extension.
(iv) Entrust Datacard shall not issue a last CRL until all certificates in the scope of the CRL are either expired or revoked. If Entrust Datacard decides or is required to terminate a CRL, Entrust Datacard will issue and publish at the corresponding CRL Distribution Point a last CRL with a nextUpdate field value in the CRL set to "99991231235959Z";
(v) CRLs and OCSP services shall be consistent over time taking into account different delays in updating the status information for both methods. The revocation status information shall be publicly and internationally available.

4.9.8 Maximum Latency for CRLs

No stipulation.

4.9.9 On-line Revocation/Status Checking Availability

On-line revocation/status checking of Certificates is available on a continuous basis by CRL or On-line Certificate Status Protocol (OCSP).

OCSP responses are signed by an OCSP responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked. The OCSP signing Certificate contains an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960.

4.9.10 On-line Revocation Checking Requirements

The CAs support an OCSP capability using the GET and POST methods for Certificates issued in accordance with this CPS.

The CAs shall sign and make available OCSP as follows:

(i) OCSP responses for Certificates issued to Subordinate CAs shall be issued at least once every twelve months or within 24 hours after revoking a Subordinate CA Certificate.

(ii) OCSP responses for Subscriber Certificates shall be issued within 60 minutes of revocation of a certificate, and at least once every 24 hours. OCSP responses will have a maximum expiration time of 10 days.

(iii) The OCSP responder will use the ArchiveCutOff extension as specified in IETF RFC 6960, with the archiveCutOff date set to the CA's certificate "notBefore" time and date value. Entrust Datacard's issuing certificate is about to expire, the Entrust Datacard will compute a last OCSP answer for each and every issued certificate (whether revoked or not), with the "nextUpdate" field set to "99991231235959Z.

If the OCSP responder receives a request for status of a Certificate serial number that is "unused", then the responder will not respond with a "good" status.

The on-line locations of the CRL and the OCSP response are included in the Certificate to support software applications that perform automatic Certificate status checking. A Relying Party can also be check Certificate revocation status directly with the Repository at https://www.entrust.net/CPS.

4.9.11 Other Forms of Revocation Advertisements Available

CAs do not rely on stapling for OCSP responses.

4.9.12 Special Requirements Re Key Compromise

If a Subscriber suspects or knows that the Private Key corresponding to the Public Key contained in the Subscriber's Certificate has been Compromised, the Subscriber shall immediately notify the RA that processed the Subscriber's Certificate Application, using the procedures set forth in §3.4, of such suspected or actual Compromise. The Subscriber shall immediately stop using such Certificate and shall remove such Certificate from any devices and/or software in which such Certificate has been installed. The Subscriber shall be responsible for investigating the circumstances of such Compromise or suspected Compromise and for notifying any Relying Parties that may have been affected by such Compromise or suspected Compromise.

4.9.13 Circumstances for Suspension

The Repository will not include entries that indicate that a Certificate has been suspended.

4.9.14 Who Can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.9.17 Additional Provisions for PSD2 Certificates

The following additional provisions concerning revocation shall apply to PSD2 Certificates:

Certificate revocation requests by NCAs may be submitted by email to nca@entrustdatacard.com. Entrust Datacard will check the authenticity of all certificate revocation requests submitted by NCAs using either of the following methods of authentication of the NCA's revocation request as selected by the NCA:

- a shared secret if it was provided by Entrust Datacard to the NCA for revocation purposes, or
- a digital signature supported by a certificate issued to the NCA by Entrust Datacard compliant with a qualified certificate policy.

If Entrust Datacard is notified of an email address where it can contact the respective NCA then Entrust Datacard will inform the NCA, using this email address, how the NCA can authenticate itself in revocation requests.

Entrust Datacard shall allow the NCA, as the owner of the PSD2 specific information, to request certificate revocation by the following procedure. The NCA may specify a reason, which can be descriptive rather than in a standard form, for the revocation. Entrust Datacard shall process such requests, and shall validate their authenticity. If it is not clearly indicated or implied why the revocation is requested or the reason is not in the area of responsibility of the NCA then the Entrust Datacard may decide to not take action. Based on an authentic request from an NCA, the Entrust Datacard shall revoke the certificate in a timely manner, and in any event within 24 hours after the receipt of the acceptable revocation request, if any of the following conditions holds (in addition to any general requirements of Section 4.9 of this CPS):

- the authorization of the Subscriber has been revoked, or
- any PSP role included in the certificate has been revoked.

If the NCA as the owner of the PSD2 specific information notifies Entrust Datacard that information has changed which can affect the validity of the certificate, but without a properly authenticated request with an acceptable reason for why the certificate should be revoked, Entrust Datacard shall investigate this notification regardless of its content and format, and shall revoke the affected certificate(s) if necessary. This notification need not be processed within 24 hours.

NCAs may send notifications about changes of relevant PSD2 regulatory information of the PSP which can affect the validity of the certificate to the following email address: nca@entrustdatacard.com. The content and format of these notifications may be agreed between the NCA and Entrust Datacard. However, Entrust Datacard shall investigate this notification regardless of its format. If Entrust Datacard is notified of an email address where it can inform the NCA identified in a revoked certificate then Entrust Datacard shall send to that email address information about the certificate revocation.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Revocation entries on a CRL or OCSP response are not removed until after the expiration of the issuing CA.

4.10.2 Service Availability

The CA operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

The CA maintains an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by the CA.

The CA maintains a continuous 24x7 ability to respond internally to a high-priority CPR. Where appropriate, the CA forwards such a complaint to law enforcement authorities, and/or revokes a Certificate that is the subject of such a complaint.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

No stipulation.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy Practices

No stipulation.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5. Facility, Management, and Operational Controls

The CA/Browser Forum's Network and Certificate System Security Requirements are incorporated by reference as if fully set forth herein. Entrust Datacard retains overall responsibility for conformance with the procedures prescribed in its information security policy even as to those policies whose functionality is undertaken by outsourcers.

5.1 Physical Security Controls

5.1.1 Site Location and Construction

The computing facilities that host the CA services are located in Ottawa, Canada. The CA equipment is located in a security zone that is physically separated from Entrust Datacard's other systems to restrict access to personnel in trusted roles. The security zone is constructed slab-to-slab with drywall and wire mesh. The security zone is protected by electronic control access systems, alarmed doors and is monitored via a 24 x7 recorded security camera and motion detector system.

5.1.2 Physical Access

The room containing the CA software is designated a two (2) person zone, and controls are used to prevent a person from being in the room alone. Alarm systems are used to notify security personnel of any violation of the rules for access to a CA.

5.1.3 Power and Air Conditioning

The Security zone is equipped with:

- Filtered, conditioned, power connected to an appropriately sized UPS and generator;
- Heating, ventilation, and air conditioning appropriate for a commercial data processing facility; and
- Emergency lighting.

The environmental controls conform to local standards and are appropriately secured to prevent unauthorized access and/or tampering with the equipment. Temperature control alarms and alerts are activated upon detection of threatening temperature conditions.

5.1.4 Water Exposures

No liquid, gas, exhaust, etc. pipes traverse the controlled space other than those directly required for the area's HVAC system and for the pre-action fire suppression system. Water pipes for the pre-action fire suppression system are only filled on the activation of multiple fire alarms.

5.1.5 Fire Prevention and Protection

The CA facility is fully wired for fire detection, alarm and suppression. Routine, frequent inspections of all systems are made to assure adequate operation.

5.1.6 Media Storage

All media is stored away from sources of heat and from obvious sources of water or other obvious hazards. Electromagnetic media (e.g. tapes) are stored away from obvious sources of strong magnetic fields. Archived material is stored in a room separate from the CA equipment until it is transferred to the archive storage facility.

Entrust Datacard employs media management procedures to protect against obsolescence and deterioration of media within the period of time that records are required to be retained.

5.1.7 Waste Disposal

Waste is removed or destroyed in accordance with industry best practice. Media used to store sensitive data is destroyed, such that the information is unrecoverable, prior to disposal.

5.1.8 Off-site Backup

As stipulated in §5.5.

5.2 Procedural Controls

5.2.1 Trusted Roles

The CAs have a number of trusted roles for sensitive operations of the CA software.

5.2.2 Number of Persons Required per Task

CA operations related to changing CA policy settings require more than one person with a trusted role to perform the operation.

The CA Private Keys are backed up, stored, and recovered only by personnel in trusted roles using dual control in a physically secured environment.

5.2.3 Identification and Authentication for Each Role

Personnel in trusted roles must undergo background investigations and must be trained for their specific role.

5.2.4 Roles Requiring Separation of Duties

No stipulation.

5.3 Personnel Controls

Operational personnel for a CA will not be assigned other responsibilities that conflict with their operational responsibilities for the CA. The privileges assigned to operational personnel for a CA will be limited to the minimum required to carry out their assigned duties.

5.3.1 Qualifications, Experience and Clearance Requirements

Prior to the engagement of any person in the Certificate management process, the CA or RA shall verify the identity and trustworthiness of such person.

5.3.2 Background Check Procedures

No stipulation.

5.3.3 Training Requirements

CAs or RAs must provide a trusted role of Validation Specialist to perform information verification duties with skills-training that covers basic PKI knowledge, authentication and vetting policies and procedures (including this CPS), common threats to the information verification process (including phishing and other social engineering tactics), and the Baseline Requirements.

Validation Specialists receive skills-training prior to commencing their job role and are required them to pass an examination on the applicable information verification requirements.

CAs maintain records of such training and ensures that personnel entrusted with Validation Specialist duties maintain an appropriate skill level.

5.3.4 Retraining Frequency and Requirements

CAs and RAs provide refresher training and informational updates sufficient to ensure that all personnel in trusted roles retain the requisite degree of expertise.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

No stipulation.

5.3.7 Independent Contractor Requirements

Third Party RAs personnel involved in the issuance of a Certificate shall meet the training and skills requirements of §5.3.3 and the document retention and event logging requirements of §5.4.1.

5.3.8 Documentation Supplied to Personnel

No stipulation.

5.4 Audit Logging Procedures

Significant security events in the CAs are automatically time-stamped and recorded as audit logs in audit trail files. The audit trail files are processed (reviewed for policy violations or other significant events) on a regular basis. Audit trail files are archived periodically. All files including the latest audit trail file are moved to backup media and stored in a secure archive facility.

Entrust Datacard synchronizes its system time at least every 24 hours using a real time value distributed by a recognized UTC(k) laboratory or National Measurement Institute.

5.4.1 Types of Events Recorded

The CAs and all RAs operating under a CA record in detail every action taken to process an Certificate request and to issue an Certificate, including all information generated or received in connection with an Certificate request, and every action taken to process the Request, including time, date, and personnel involved in the action.

The foregoing record requirements include, but are not limited to, an obligation to record the following events:

(i) CA key lifecycle management events, including:
- a. Key generation, backup, storage, recovery, archival, and destruction; and
- b. Cryptographic device lifecycle management events.

(ii) CA and Certificate lifecycle management events, including:
- c. Certificate requests, renewal and re-key requests, and revocation;
- d. All verification activities required by this CPS;
- e. Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
- f. Acceptance and rejection of Certificate requests;
- g. Issuance of Certificates; and
- h. Generation of Certificate Revocation Lists (CRLs) and OCSP messages.

(iii) Security events, including:
- i. Successful and unsuccessful PKI system access attempts;
- j. PKI and security system actions performed;
- k. Security profile changes;
- l. System crashes, hardware failures, and other anomalies;
- m. Start-up and shutdown of the logging functions; and availability and utilization of needed services;
- n. Firewall and router activities; and
- o. Entries to and exits from the CA facility.

(iv) Log entries include the following elements:
- p. Date and time of entry;
- q. Identity of the person making the journal entry; and
- r. Description of entry.

5.4.2 Frequency of Processing Log

No stipulation

5.4.3 Retention Period for Audit Log

The CA retains any audit logs generated for at least seven years. The audit logs will be made available to the Qualified Auditor upon request.

5.4.4 Protection of Audit Log

Only trusted roles have access to read or archive the logs. Audit logs are protected from destruction prior to the end of the audit log retention period and are retained securely on-site until transferred to an off-site storage location. The off-site storage location is a safe and secure location that is separate from the location where the data was generated.

5.4.5 Audit Log Backup Procedures

No stipulation.

5.4.6 Audit Collection System

No stipulation.

5.4.7 Notification to Event-causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

CAs annually perform a risk assessment that:

(i) Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate data or Certificate management processes;

(ii) Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate data and Certificate management processes; and

(iii) Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

Based on the risk assessment, a security plan is developed, implemented, and maintained consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to manage and control the risks identified during the risk assessment. The security plan includes administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the Certificate data and Certificate management processes. The security plan also takes into account then-available technology and the cost of implementing the specific measures, and implements a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

5.5 Records Archival

5.5.1 Types of Records Archived

The audit trail files, databases and revocation information for the CAs are archived.

5.5.2 Retention Period of for Archive

The CA will retain all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, for at least seven years after any Certificate based on that documentation ceases to be valid.

5.5.3 Protection of Archive

The databases for CAs are encrypted and protected by CA master keys. The archive media is protected through storage in a restricted-access facility to which only Entrust Datacard-authorized personnel have access. Archive files are backed up as they are created. Originals are stored on-site and housed with a CA system. Backup files are stored at a secure and separate geographic location.

5.5.4 Archive Backup Procedures

No stipulation.

5.5.5 Requirements for Time-stamping of Records

No stipulation.

5.5.6 Archive Collection System

No stipulation.

5.5.7 Procedures to Obtain and Verify Archive Information

No stipulation.

5.6 Key Changeover

CAs' key pairs will be retired from service at the end of their respective lifetimes as defined in §6.3. New CA key pairs will be created as required to support the continuation of CA Services. Each CA will continue to publish CRLs signed with the original key pair until all Certificates issued using that original key pair have expired. The CA key changeover process will be performed such that it causes minimal disruption to Subscribers and Relying Parties.

Specifically, before expiration of any Entrust Datacard certificate which is used for signing subject keys (for example as indicated by expiration of and Entrust Datacard certificate), in case of continuing with the service:

(i) Entrust Datacard shall generate a new certificate for signing subject key pairs, and shall apply all necessary actions to avoid disruption to the operations of any entity that may rely on the Entrust Datacard certificate;

(ii) the new CA certificate shall also be generated and distributed in accordance with the present document.

Subsections (i) and (ii) will be performed with a suitable interval between certificate expiry date and the last certificate signed to allow all parties that have relationships with Entrust Datacard (subjects, subscribers, relying parties, CAs higher in the CA hierarchy, etc.) to be aware of this key changeover and to implement the required operations to avoid inconveniences and malfunctions. The minimum changeover period will be two years before the certificate expiry date. This does not apply if Entrust Datacard will cease its operations before its own certificate-signing certificate expiration date.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

CAs have a security incident response plan, a disaster recovery plan, and a business continuity plan to provide for timely recovery of services in the event of a security incident, breach of security, loss of system integrity, or system outage. The address the following:

(i) the conditions for activating the plans;
(ii) resumption procedures;
(iii) a maintenance schedule for the plan;
(iv) awareness and education requirements;

(v) the responsibilities of the individuals;
(vi) recovery point objective (RPO) of fifteen minutes;
(vii) recovery time objective (RTO) of 72 hours for essential CA operations which include Certificate revocation, and issuance of Certificate revocation status; and
(viii) testing of recovery plans.

In order to mitigate the event of a disaster, the CAs have implemented the following:

(ix) secure on-site and off-site storage of backup HSMs containing copies of all CA Private Keys
(x) secure on-site and off-site storage of all requisite activation materials
(xi) regular synchronization of critical data to the disaster recovery site
(xii) regular incremental and daily backups of critical data within the primary site
(xiii) weekly backup of critical data to a secure off-site storage facility
(xiv) secure off-site storage of disaster recovery plan and disaster recovery procedures
(xv) environmental controls as described in §5.1
(xvi) high availability architecture for critical systems

Entrust Datacard has implemented a secure disaster recovery facility that is greater than 250 km from the primary secure CA facilities.

In the event of any security incident, breach of security, loss of system integrity, or system outage affecting Subscribers, ASVs, Relying Parties, or other entities with which Entrust Datacard has agreements or other form of established relations, Entrust Datacard shall inform them within 24 hours of the problem being identified by sending one or more email messages to Subscribers, ASVs and other entities with which Entrust Datacard has agreements or other form of established relations based on records of current email addresses, and will post one or more messages to Relying Parties on its website describing the nature of the problem.

If appropriate, Entrust Datacard will notify all parties that certificates and revocation status information issued using this CA key may no longer be valid include a recommendation that Subscribers replace all certificates affected by the problem, that all ASVs, other entities with which Entrust Datacard has agreements or other form of established relations, and that Relying Parties cease to rely on all certificates affected by the problem. These communications will be made by the Computer Security Incident Response Team established by Entrust Datacard's Security Incident Response Plan and according to the procedures established in such Plan, together with assistance from such other Entrust Datacard staff as may be required by the Computer Security Incident Response Team to send such notifications. Following any disaster, any security incident, breach of security, loss of system integrity, or system outage, Entrust Datacard shall, where practical, take steps to avoid repetition of the problem. Entrust Datacard shall revoke any CA certificate that has been issued for the compromised CA when Entrust Datacard is informed of the compromise of another CA (e.g., for cross-certificates).

Upon system failure, service or other factors which are not under the control of Entrust Datacard, we shall apply our commercially reasonable endeavors to ensure that the service is not unavailable for longer than a maximum period of 72 hours.

Entrust Datacard requires rigorous security controls to maintain the integrity of the CAs. The Compromise of the Private Key used by a CA is viewed by Entrust Datacard as being very unlikely; however, Entrust Datacard has policies and procedures that will be employed in the event of such a Compromise. At a minimum, all Subscribers, ASVs, and Relying Parties shall be informed as soon as practicable of such a Compromise and information shall be posted in the Repository. To inform these parties in the event of key compromise, Entrust Datacard will send one or more email messages to Subscribers and ASVs based on records of current email addresses and will post one or more messages to Relying Parties on its website describing the nature of the key compromise, stating that certificates and revocation status information issued using this CA key may no longer be valid, and recommending that Subscribers replace all certificates issued from the CA that was subject to key compromise and that all ASVs and Relying Parties cease to rely on all certificates issued from the CA that was subject to key compromise.

5.7.2 Computing Resources, Software and/or Data are Corrupted

No stipulation.

5.7.3 Entity Private Key Compromise Procedures

No stipulation.

5.7.4 Business Continuity Capabilities after a Disaster

No stipulation.

5.8 CA or RA Termination

In the event of CA termination, Entrust will:

(i) Provide notice and information about the CA termination by sending notice to Subscribers with unrevoked unexpired Certificates, Application Software Vendors and Relying Parties and by posting such information in the Repository and sending informational emails; and

(ii) Transfer all responsibilities to a qualified successor entity.

If a qualified successor entity does not exist, Entrust will:

(iii) Transfer those functions capable of being transferred to a reliable third party and arrange to preserve all relevant records with a reliable third party or a government, regulatory, or legal body with appropriate authority;

(iv) Revoke all Certificates that are still unrevoked or unexpired on a date as specified in the notice and publish final CRLs;

(v) Destroy all CA Private Keys; and

(vi) Make other necessary arrangements that are in accordance with this CPS.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

The CAs will perform the following when generating a Key Pair for a CA:

(i) Prepare and follow a key generation script;
(ii) Have a qualified auditor witness the key generation process;
(iii) Have a qualified auditor issue a report opining that the CA followed its key generation ceremony during its key generation process and the controls to ensure the integrity and confidentiality of the Key Pair;
(iv) Generate the Key Pair in a physically secured environment;
(v) Generate the Key Pair using personnel in trusted roles under the principles of multiple person control and split knowledge;
(vi) Generate the Key Pair within cryptographic modules meeting the applicable requirements of §6.2.11;
(vii) Log its key generation activities; and
(viii) Maintain effective controls to provide reasonable assurance that the private key was generated and protected in conformance with the procedures described in this CPS and (if applicable) its key generation script.

CA Administrators

Keys Pairs for CA administrators must be generated and protected on a cryptographic module that meets or exceeds the requirements as defined in §6.2.11. The cryptographic modules are prepared using the software provided by the module vendor. The cryptographic modules are personalized for the administrator by giving the card an identity and a password known by the administrator. The Key Pair is generated by creating the administrator as a user in the CA and performing an enrollment process which is authenticated with the administrator's module password.

6.1.1.2 RA Key Pair Generation

No stipulation.

6.1.1.3 Subscriber Key Pair Generation

The Applicant or Subscriber is required to generate a new, secure, and cryptographically sound Key Pair to be used in association with the Subscriber's Certificate or Applicant's Certificate Application.

The CAs will reject a Certificate request if it is known to have a weak private key (i.e., Debian weak key).

eIDAS QSigC

Subscriber Key Pairs must be generated in a manner that ensures that the Private Key is not known to or accessible by anybody other than the Subscriber or a Subscriber's authorized representative. Subscriber Key Pairs must be generated in a cryptographic module that prevents exportation or duplication and that meets or exceed the requirements as defined in §6.2.11.

6.1.2 Private Key Delivery to Subscriber

If the CA generates the Subscriber's Key Pair, the CA will have a secure process to generate the Key Pair on a secure cryptographic device. The CA will securely store and/or distribute the secure cryptographic device.

6.1.3 Public Key Delivery to Certificate Issuer

The Public Key to be included in a Certificate is delivered to the CA in a signed Certificate Signing Request (CSR) as part of the Certificate Application process. The signature on the CSR will be verified by the CA prior to issuing the Certificate.

6.1.4 CA Public Key Delivery to Relying Parties

The Public-Key Certificate for CAs are made available to Subscribers and Relying parties through inclusion in third party software as distributed by the applicable software manufacturers. The Public Key Certificate for cross certified Subordinate CAs is provided to the Subscriber with the Subscriber certificate.

Public Key Certificates for CAs are also available for download from the Repository.

6.1.5 Key Sizes

CA Key Size
For CAs, the minimum key size shall be no less than 2048 bit RSA.

Qualified Certificates and PSD2 Certificates
The RSA key sizes supported are 2048, 3072 and 4096-bits.

6.1.6 Public Key Parameters Generation and Quality Checking

For RSA public keys, CAs shall confirm that the value of the public exponent is an odd number equal to 3 or more. Additionally, the public exponent will be in the range between $2^{16}+1$ and $2^{256}-1$. The modulus will also have the following characteristics: an odd number, not the power of a prime, and have no factors smaller than 752.

Should any of the algorithms, or associated parameters, used by the CA or its Subscribers become insufficient for its remaining intended usage then the CA shall inform all Subscribers and Relying Parties with whom the CA has agreement or other form of established relations. The CA will also post this information to make available to other relying parties. Should any of the algorithms, or associated parameters, used by the CA or its Subscribers become insufficient for its remaining intended usage then the CA shall schedule a revocation of any affected certificate.

6.1.7 Key Usage Purposes

Root CA Private Keys must not be used to sign Certificates except in the following cases:

(i) Self-signed Certificates to represent the Root CA itself;
(ii) Certificates for Subordinate CAs and Cross Certificates;
(iii) Certificates for infrastructure purposes (e.g. administrative role certificates, internal CA operational device certificates, and OCSP Response verification Certificates); and
(iv) Certificates issued solely for the purpose of testing products with Certificates issued by a Root CA.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The CAs have implemented physical and logical safeguards to prevent unauthorized Certificate issuance. Protection of the CA Private Key outside the validated system consist of physical security, encryption, or a combination of both, implemented in a manner that prevents disclosure of the CA Private Key. The CA encrypts its Private Key with an algorithm and key-length that are capable of withstanding cryptanalytic attacks for the residual life of the encrypted key.

6.2.1 Cryptographic Module Standards and Controls

CA Private Keys
CA Private Keys must be stored and protected on cryptographic modules that meet or exceed the requirements as defined in §6.2.11. Private Keys on cryptographic modules are held in secure facilities under two-person control. RA Private Keys must be stored and protected on cryptographic modules that meet or exceed the requirements defined in §6.2.11.

If the CA generates the Key Pair on behalf of the Subject or Subscriber, the keys will be generated in a confidential process.

eIDAS QSigC
eIDAS QSigC Private Keys must be generated, stored and protected on a secure cryptographic device that meets or exceeds the requirements defined in §6.2.11.

6.2.2 Private Key (N out of M) Multi-person Control

A minimum of two-person control shall be established on any CA Private Key for all purposes including activation and backup, and may be implemented as a combination of technical and procedural controls. Persons involved in management and use of the CA Private Keys shall be designated as authorized by the CA for this purpose. The names of the parties used for two-person control shall be maintained on a controlled list.

6.2.3 Private Key Escrow

Entrust Datacard does not escrow the CAs' Private Keys.

6.2.4 Private Key Backup

CA Private Keys
CA Private Keys shall be backed up under the two-person control used to create the original version of the Private Keys. All copies of the CA Private Key shall be securely protected.

Subscriber Private Keys
Subscribers are responsible for protecting the Private Key associated with the Public Key in the Subscriber's Certificate.

6.2.5 Private Key Archival

CA Private Keys
Upon retirement of a CA, the Private Keys will be archived securely using hardware cryptographic modules that meet the requirements §6.2.11. The Key Pairs shall not be used unless the CA has been removed from retirement or the keys are required temporarily to validate historical data. Private Keys required for temporary purposes shall be removed from archive for a short period of time.

The archived CA Private Keys will be reviewed on an annual basis. After the minimum period of 5 years, the CA Private Keys may be destroyed according to the requirements in §6.2.10. The CA Private Keys must not be destroyed if they are still required for business or legal purposes.

Third parties will not archive CA Private Keys.

6.2.6 Private Key Transfer into or from Cryptographic Module

CA Private Keys shall be generated by and secured in a cryptographic module. In the event that a Private Key is to be transported from one cryptographic module to another, the Private Key must be migrated using the secure methodology supported by the cryptographic module.

If the Private Key of a Subordinate CA is communicated to an unauthorized third party, then the Subordinate CA shall revoke all Certificates corresponding to Private Key.

6.2.7 Private Key Storage on Cryptographic Module

CA Private Keys are stored on a cryptographic module are secured in cryptographic module as defined in §6.2.11.

6.2.8 Method of Activating Private Key

CA Private Keys
CA Private Keys shall be activated under two-person control using the methodology provided with the cryptographic module.

Subscriber Private Keys
Subscriber Private Keys shall be activated by the Subscriber to meet the requirements of the security software used for their applications. Subscribers shall protect their Private Keys corresponding to the requirements in §9.6.3.

6.2.9 Method of Deactivating Private Key

CA Private Keys
CA Private Keys shall be deactivated when the CA is not required for active use. Deactivation of the Private Keys shall be done in accordance with the methodology provided with the cryptographic module.

CA Administrators
The administrator's identity is deactivated in the CA and the administrator's Certificate is revoked.

6.2.10 Method of Destroying Private Key

CA Private Keys
CA Private Keys destruction will be two-person controlled and may be accomplished by executing a "zeroize" command or by destruction of the cryptographic module. Destruction of CA Private Keys must be authorized by the Policy Authority.

If the CA is removing a cryptographic module from service, then all Private Keys must be removed from the module. If the CA cryptographic module is intended to provide tamper-evident characteristics is removed from service, then the device will be destroyed.

CA Administrators
The administrator's Private Key is destroyed by reinitializing the cryptographic module.

6.2.11 Cryptographic Module Rating

CA Key Pairs
CA Key Pairs must be generated and protected on a cryptographic module that is compliant to at least FIPS 140-2 Level 3 certification standards.

CA Administrators
Key Pairs for CA administrators must be generated and protected on a cryptographic module that is compliant to at least FIPS 140-2 Level 2 certification standards.

eIDAS QSigC
Key Pairs must be generated and protected on a secure cryptographic device that is compliant to at least Common Criteria EAL 4+ certification standards or equivalent.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

No stipulation.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

CA Key Pairs
CA 2048-bit RSA Key Pairs may have a validity period expiring no later than 31 December 2030.

eIDAS QWAC and PSD2 QWAC
eIDAS QWAC and PSD2 QWAC may have a validity period of up to, but no more than, 825-days. Effective 1 September 2020, eIDAS QWAC and PSD2 QWAC may have a validity period of up to, but no more than, 398-days.

eIDAS QSealC, PSD2 QSealC and eIDAS QSigC
eIDAS QSealC, PSD2 QSealC and eIDAS QSigC may have a validity period of up to, but no more than, 3 years.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

No stipulation.

6.4.2 Activation Data Protection

No stipulation.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The workstations on which the CAs operate are physically secured as described in §5.1. The operating systems on the workstations on which the CAs operate enforce identification and authentication of users. Access to CA software databases and audit trails is restricted as described in this CPS. All operational personnel that are authorized to have access to the CAs are required to use hardware tokens in conjunction with a PIN to gain access to the physical room that contains the CA software being used for such CAs.

The CA enforces multi-factor authentication for all accounts capable of directly causing Certificate issuance.

For Subscriber accounts, the CA has implemented technical controls to restrict Certificate issuance to a limited set of pre-approved domains.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Security Controls

6.6.1 System Development Controls

The CA makes use of Commercial Off The Shelf (COTS) products for the hardware, software, and network components. Systems developed by the CA are deployed in accordance with Entrust Datacard software lifecycle development standards.

6.6.2 Security Management Controls

The configuration of the CA system as well as any modifications and upgrades are documented and controlled. Methods of detecting unauthorized modifications to the CA equipment and configuration are in place to ensure the integrity of the security software, firmware, and hardware for correct operation. A formal configuration management methodology is used for installation and ongoing maintenance of the CA system and quarterly reviews.

When first loaded, the CA software is verified as being that supplied from the vendor, with no modifications, and be the version intended for use.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls Security Controls

Remote access to CA application via the Administration software interface is secured.

6.8 Time-stamping

No stipulation.

7. Certificate, CRL and OCSP Profiles

The profile for the Certificates and Certificate Revocation List (CRL) issued by a CA conform to the specifications contained in the IETF RFC 5280 Internet X.509 PKI Certificate and Certificate Revocation List (CRL) Profile.

7.1 Certificate Profile

CAs issue Certificates in accordance with the X.509 version 3. Certificate profiles for Root CA Certificate, Subordinate CA Certificates, and Subscriber Certificates are described in Appendix A and the sections below.

Certificates have a serial number greater than zero (0) that contains at least 64 unpredictable bits.

7.1.1 Version Number

All Certificates issued by the CAs are X.509 version 3 certificates.

7.1.2 Certificate Extensions

7.1.2.1 Root CA Certificate

Certificate extensions are as set as stipulated in IETF RFC 5280 and in accordance with Appendix A.

7.1.2.2 Subordinate CA Certificate

Certificate extensions are as set as stipulated in IETF RFC 5280 and in accordance with Appendix A.

The extension requirements for extended key usage are:

(i) Must contain an EKU extension,
(ii) Must not include the anyExtendedKeyUsage EKU, and
(iii) Must not include either id-kp-serverAuth, id-kp-emailProtection, id-kp-codeSigning or id-kp-timeStamping EKUs in the same certificate.

7.1.2.3 Subscriber Certificate

Certificate extensions are as set as stipulated in IETF RFC 5280 and in accordance with Appendix A.

Qualified Certificates
Qualified Certificates shall include qcStatements as required by ETSI EN 319 412-5.

PSD2 Certificates
PSD2 Certificates shall include the PSD2 qcStatement as required by ETSI EN 319 495 and include the role of the payment service provider, which maybe one or more of the following:

(i) account servicing (PSP_AS);
(ii) payment initiation (PSP_PI);
(iii) account information (PSP_AI);
(iv) issuing of card-based payment instruments (PSP_IC).

7.1.2.4 All Certificates

All other fields and extensions MUST be set in accordance with RFC 5280.

7.1.2.5 Application of RFC 5280

For purposes of clarification, a precertificate, as described in RFC 6962 (Certificate Transparency), shall not be considered to be a "certificate" subject to the requirements of RFC 5280.

7.1.3 Algorithm Object Identifiers

The CAs issue Certificates using the SHA-2 hash algorithm. SHA-2 Certificates will not chain up to a SHA-1 Subordinate CA Certificate.

The CAs will not issue any Certificates or Subordinate CA Certificates using the SHA-1 hash algorithm.

The CA will sign Certificates based on the algorithm specified in Appendix A.

7.1.4 Name Forms

7.1.4.1 Issuer Information

The content of the certificate issuer DN field will match the subject DN of the issuing CA to support name chaining as specified in RFC 5280, section 4.1.2.4.

7.1.4.2 Subject Information – Subscriber Certificates

Subject information must meet the requirements stated in Appendix A.

Name forms for Subscriber Certificates are as stipulated in §3.1.1. All other optional attributes must contain information that has been verified by the CA or RA. Optional attributes will not contain only metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.

Entries in the dNSName are in the "preferred name syntax" as specified in IETF RFC 5280 and thus do not contain underscore characters.

eIDAS QWAC and PSD2 QWAC
CAs shall not issue a Certificate with a domain name containing a Reserved IP Address or Internal Name

7.1.4.3 Subject Information – Root Certificates and Subordinate CA Certificates

Subject information must meet the requirements stated in Appendix A.

7.1.5 Name Constraints

CAs do not support the issuance of technically constrained Subordinate CA Certificates.

7.1.6 Certificate Policy Object Identifier

7.1.6.1 Reserved Certificate Policy Identifiers

Certificates must include one or more of the following reserved Certificate Policy Identifiers:

Extended Validation (EV) SSL Certificates	2.23.140.1.1
Qualified Signature Certificates	0.4.0.194112.1.0
Qualified Seal Certificates	0.4.0.194112.1.1
Qualified Web Authentication Certificates	0.4.0.194112.1.4
PSD2 Certificates	0.4.0.19495.3.1

7.1.6.2 Root CA Certificates

Root CA Certificates do not contain the certificate policy object identifiers.

7.1.6.3 Subordinate CA Certificates

Subordinate CA
Subordinate CA Certificates must include either the "any policy" certificate policy object identifier or one or more explicit certificate policy object identifiers that indicates compliance with a specific certificate policy. Certificate policy object identifiers are listed in §7.1.6.4.

7.1.6.4 Subscriber Certificates

Certificates include one or more of the following certificate policy identifiers:

Extended Validation (EV) SSL Certificates	2.16.840.1.114028.10.1.2
Document Signing Certificates (AATL)	2.16.840.1.114028.10.1.6
Qualified Signature Certificates	2.16.840.1.114028.10.1.12.0
Qualified Seal Certificates	2.16.840.1.114028.10.1.12.1
Qualified Web Authentication Certificates	2.16.840.1.114028.10.1.12.4
PSD2 Qualified Seal Certificates	2.16.840.1.114028.10.1.12.5
PSD2 Qualified Web Authentication Certificates	2.16.840.1.114028.10.1.12.6

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

CAs include policy qualifiers in all Subscriber Certificates as stipulated in Appendix A.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Certificate policies extension is marked Not Critical

7.2 CRL Profile

The following fields of the X.509 version 2 CRL format are used by the CAs:

- version: set to v2
- signature: identifier of the algorithm used to sign the CRL
- issuer: the full Distinguished Name of the CA issuing the CRL
- this update: time of CRL issuance
- next update: time of next expected CRL update
- revoked Certificates: list of revoked Certificate information

7.2.1 Version Number

No stipulation.

7.2.2 CRL and CRL Entry Extensions

No stipulation.

7.3 OCSP Profile

The profile for the Online Certificate Status Protocol (OCSP) messages issued by a CA conform to the specifications contained in the IETF RFC 6960 Internet X.509 PKI Online Certificate Status Protocol (OCSP) Profile.

7.3.1 Version Number

No stipulation.

7.3.2 OCSP Extensions

No stipulation.

8. Compliance Audit and Other Assessment

8.1 Frequency or Circumstances of Assessment

The CAs and RAs shall be audited for compliance with the practices and procedures set forth in the CPS. The period during which the CA issues Certificates will be divided into an unbroken sequence of audit periods. An audit period will not exceed one year in duration.

8.2 Identity/Qualifications of Assessor

The compliance audit of the CAs shall be performed by an auditor which possesses the following qualifications and skills:

i. Independence from the subject of the audit;
ii. Ability to conduct an audit that addresses the criteria of the audit schemes specified in §8.4;
iii. Employs individuals who have proficiency in examining PKI technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
iv. Performed by a licensed conformity assessment body accredited in accordance with ISO 17065 applying the requirements specified in ETSI EN 319 403;
v. Bound by law, government regulation, or professional code of ethics; and
vi. Maintains professional liability/errors and omissions insurance policy limits of at least one million US dollars coverage.

8.3 Assessor's Relationship to Assessed Entity

The certified public accounting firm selected to perform the compliance audit for the CAs and RAs shall be independent from the entity being audited.

8.4 Topics Covered by Assessment

The compliance audit shall test compliance of the CAs and RAs against the policies and procedures set forth, as applicable in:

i. This CPS;
ii. ETSI EN 319 411-2 and related standards documents;
iii. ETSI TS 119 495 and related standards documents.

8.5 Actions Taken as a Result of Deficiency

Upon receipt of a compliance audit that identifies any deficiencies, the audited CA or RA shall use commercially reasonable efforts to correct any such deficiencies in an expeditious manner.

8.6 Communication of Results

The results of all compliance audits shall be communicated to the Policy Authority and to any third party entities which are entitled by law or regulation to receive a copy of the audit results.

The results of the most recent compliance audit will be posted within three months from the end of the audit period to the Repository.

eIDAS QWAC and PSD2 QWAC
The audit results will also be posted to the CA Common Database (i.e., https://ccadb.force.com).

8.7 Self-audits

eIDAS QWAC and PSD2 QWAC
The CA will monitor adherences to this CPS, ETSI Guidelines, and the Baseline Requirements and strictly control its service quality by performing self-audits on at least a quarterly basis against a randomly selected sample of the greater of one Certificate or at least three percent of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

9. Other Business and Legal Matters

9.1 Fees

Unless otherwise set out in a Subscription Agreement, the fees for services provided by Entrust Datacard in respect to Certificates are set forth in the Repository. Unless otherwise set out in a Subscription Agreement, these fees are subject to change, and any such changes shall become effective immediately after posting in the Repository. The fees for services provided by independent third-party RAs, Resellers and Co-marketers in respect to Certificates are set forth on the web sites operated by such RAs, Resellers and Co-marketers. These fees are subject to change, and any such changes shall become effective immediately after posting in such web sites.

9.1.1 Certificate Issuance or Renewal Fees

See the Repository for the fees charged by Entrust Datacard. See the web sites operated by RAs operating under the CAs, Resellers, and Co-marketers for the fees charged by such RAs, Resellers, and Co-marketers.

9.1.2 Certificate Access Fees

See the Repository for the fees charged by Entrust Datacard. See the web sites operated by RAs operating under the CAs, Resellers, and Co-marketers for the fees charged by such RAs, Resellers, and Co-marketers.

9.1.3 Revocation or Status Information Access Fees

See the Repository for the fees charged by Entrust Datacard. See the web sites operated by RAs operating under the CAs, Resellers, and Co-marketers for the fees charged by such RAs, Resellers, and Co-marketers.

9.1.4 Fees for Other Services

See the Repository for the fees charged by Entrust Datacard. See the web sites operated by RAs operating under the CAs, Resellers, and Co-marketers for the fees charged by such RAs, Resellers, and Co-marketers.

9.1.5 Refund Policy

Except for a formal written Entrust Datacard refund policy, if any, neither Entrust Datacard nor any RAs operating under the CAs nor any Resellers or Co-Marketers provide any refunds for Certificates or services provided in respect to Certificates.

9.2 Financial Responsibility

Subscribers and Relying Parties shall be responsible for the financial consequences to such Subscribers, Relying Parties, and to any other persons, entities, or organizations for any transactions in which such Subscribers or Relying Parties participate and which use Certificates or any services provided in respect to Certificates. Entrust Datacard makes no representations and gives no warranties or conditions regarding the financial efficacy of any transaction completed utilizing an Certificate or any services provided in respect to Certificates and the Entrust Datacard Group shall have no liability except as explicitly set forth herein in respect to the use of or reliance on an Certificate or any services provided in respect to Certificates.

9.2.1 Insurance Coverage

Entrust Datacard maintains (a) Commercial General Liability insurance with policy limits of at least two million US dollars (US$2,000,000.00) in coverage; and (b) Professional Liability/Errors and Omissions insurance, with policy limits of at least five million US dollars (US$5,000,000.00) in coverage. Such insurance policies will be carried with companies rated no less than A- as to Policy Holder's Rating in the current edition of Best's Insurance Guide.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-entities

No stipulation.

9.3 Confidentiality of Business Information

Neither Entrust Datacard nor any independent third-party RAs operating under the CAs, nor any Resellers or Co-Marketers shall disclose or sell Applicant or Subscriber names (or other information submitted by an Applicant or Subscriber when applying for a Certificate), except in accordance with this CPS, a Subscription Agreement, or a Relying Party Agreement. Entrust Datacard and all independent third-party RAs operating under the CAs, and all Resellers and Co-Marketers shall use a commercially reasonable degree of care to prevent such information from being used or disclosed for purposes other than those set forth in the CPS, a Subscription Agreement, or a Relying Party Agreement. Notwithstanding the foregoing, Applicants and Subscribers acknowledge that some of the information supplied with a Certificate Application is incorporated into Certificates and that Entrust Datacard and all independent third-party RAs operating under the CAs, and all Resellers and Co-Marketers shall be entitled to make such information publicly available.

9.3.1 Scope of Confidential Information

Information that is supplied by Applicants, Subscribers, or Relying Parties for the subscription for, use of, or reliance upon an Certificate, and which is not included in the information described in §9.3.2 below, shall be considered to be confidential. Entrust Datacard and RAs shall be entitled to disclose such information to any subcontractors or agents that are assisting in the verification of information supplied in Certificate Applications or that are assisting in the operation of the CAs or Entrust Datacard RAs. Information considered to be confidential shall not be disclosed unless compelled pursuant to legal, judicial, or administrative proceedings, or otherwise required by law. Entrust Datacard and independent third-party RAs shall be entitled to disclose information that is considered to be confidential to legal and financial advisors assisting in connection with any such legal, judicial, administrative, or other proceedings required by law, and to potential acquirers, legal counsel, accountants, banks and financing sources and their advisors in connection with mergers, acquisitions, or reorganizations.

9.3.2 Information not with the Scope of Confidential Information

Information that is included in a Certificate or a Certificate Revocation List, including without limitation personal information, shall not be considered confidential. Information contained in the CPS shall not be considered confidential. Without limiting the foregoing, information that (i) was or becomes known through no fault of Entrust Datacard, an independent third-party RA under a CA, a Reseller, or a Co-marketer, (ii) was rightfully known or becomes rightfully known to Entrust Datacard, an independent third-party RA under the CA, a Reseller, or a Co-marketer without confidential or proprietary restriction from a source other than the Subscriber, (iii) is independently developed by Entrust Datacard, an independent third-party RA under a CA, a Reseller, or a Co-marketer, or (iv) is approved by a Subscriber for disclosure, shall not be considered confidential.

9.3.3 Responsibility to Protect Confidential Information

Entrust Datacard's employees, agents, and contractors are responsible for protecting confidential information and are contractually obligated to do so. Entrust Datacard systems are configured to protect confidential information.

9.4 Privacy or Personal Information

9.4.1 Data Protection Policy

Entrust Datacard follows the Data Protection Policy available at www.entrustdatacard.com when handling personal information.

9.4.2 Information Treated as Private

Entrust Datacard treats all personal information about an individual as personal information in accordance with the Data Protection Policy.

9.4.3 Information not Deemed Private

Certificates, CRLs, and OCSP and the personal or corporate information appearing in them are not considered confidential information.

9.4.4 Responsibility to Protect Private Information

Entrust Datacard personnel are required to protect personal information in accordance with the Data Protection Policy.

9.4.5 Notice and Consent to Use Private Information

Unless otherwise stated in the CPS, Data Protection Policy or other agreement (such as a Subscription Agreement or Relying Party Agreement), personal information will not be used without the consent of the subject of such personal information. Notwithstanding the foregoing, personal information contained in a Certificate may be published in online public repositories and all Subscribers consent to the global transfer of any personal data contained in the Certificate.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Entrust Datacard, independent third-party RAs under a CA, Resellers, and Co-marketers shall have the right to release information that is considered to be personal and/ or confidential to law enforcement officials in compliance with applicable law.

Entrust Datacard, independent third-party RAs under a CA, Resellers, and Co-marketers may disclose information that is considered confidential during the course of any arbitration, litigation, or any other legal, judicial, or administrative proceeding relating to such information. Any such disclosures shall be permissible provided that Entrust Datacard, the independent third-party RA, Reseller, or Co-marketer uses commercially reasonable efforts to obtain a court-entered protective order restricting the use and disclosure of any such information to the extent reasonably required for the purposes of such arbitration, litigation, or any other legal, judicial, or administrative proceeding.

9.4.7 Other Information Disclosure Circumstances

Entrust Datacard, independent third-party RAs under a CA, Resellers, and Co-marketers may disclose information provided to Entrust Datacard, such RA, Reseller or Co-marketer, by an Applicant, a Subscriber, or a Relying Party upon request of such Applicant, Subscriber, or Relying Party.

If a Certificate is revoked by a CA, a serial number will be included in the Certificate Revocation List entry for the revoked Certificate.

9.5 Intellectual Property Rights

Entrust Datacard retains all right, title, and interest (including all intellectual property rights), in, to and under all Certificates, except for any information that is supplied by an Applicant or a Subscriber and that is included in an Certificate, which information shall remain the property of the Applicant or Subscriber. All Applicants and Subscribers grant to Entrust Datacard and any RAs operating under the CAs a non-exclusive, worldwide, paid-up, royalty-free license to use, copy, modify, publicly display, and distribute such information, by any and all means and through any and all media whether now known or hereafter devised for the purposes contemplated under the CPS, the Subscriber's Subscription Agreement, and any Relying Party Agreements. Entrust Datacard and any RAs operating under the CAs shall be entitled to transfer, convey, or assign this license in conjunction with any transfer, conveyance, or assignment as contemplated in §9.16.2. Entrust Datacard grants to Subscribers and Relying Parties a non-exclusive, non-transferable license to use, copy, and distribute Certificates, subject to such Certificates being used as contemplated under the CPS, the Subscriber's Subscription Agreement, and any Relying Party Agreements, and further provided that such Certificates are reproduced fully and accurately and are not published in any

publicly available database, repository, or directory without the express written permission of Entrust Datacard. Except as expressly set forth herein, no other right is or shall be deemed to be granted, whether by implication, estoppel, inference or otherwise. Subject to availability, Entrust Datacard may in its discretion make copies of one or more Subordinate CA Certificate(s) available to Subscribers for use solely with the Certificate issued to such Subscribers. Entrust Datacard retains all right, title, and interest (including all intellectual property rights), in, to and under the Subordinate CA Certificate(s).

Entrust Datacard grants permission to reproduce the CPS provided that (i) the copyright notice on the first page of this CPS is retained on any copies of the CPS, and (ii) the CPS is reproduced fully and accurately. Entrust Datacard retains all right, title, and interest (including all intellectual property rights), in, to and under the CPS.

In no event shall the Entrust Datacard Group be liable to any Applicants, Subscribers, or Relying Parties or any other third parties for any losses, costs, liabilities, expenses, damages, claims, or settlement amounts arising from or relating to claims of infringement, misappropriation, dilution, unfair competition, or any other violation of any patent, trademark, copyright, trade secret, or any other intellectual property or any other right of person, entity, or organization in any jurisdiction arising from or relating to any Certificate or arising from or relating to any services provided in relation to any Certificate.

9.6 Representation and Warranties

9.6.1 CA Representations and Warranties

A CA shall:

(i) provide CA services in accordance with the terms and conditions of the CPS;
(ii) upon receipt of a request from an RA operating under such CA, issue an Certificate in accordance with the terms and conditions of the CPS;
(iii) make available Certificate revocation information by issuing Certificates and by issuing and making available Certificate CRLs in an Repository in accordance with the terms and conditions of the CPS;
(iv) issue and publish Certificate CRLs on a regular schedule in accordance with the terms and conditions of the CPS; and
(v) upon receipt of a revocation request from an RA operating under such CA, revoke the specified Certificate in accordance with the terms and conditions of the CPS.

In operating the CAs, Entrust Datacard may use one or more representatives or agents to perform its obligations under the CPS, any Subscription Agreements, or any Relying Party Agreements, provided that Entrust Datacard shall remain responsible for its performance.

9.6.1.1 Warranties and Limitations on Warranties

Entrust Datacard makes the following limited warranties to Subscribers with respect to the operation of the CAs:

(i) CAs shall provide Repository services consistent with the practices and procedures set forth in this CPS;
(ii) CAs shall perform Certificate issuance consistent with the procedures set forth in this CPS; and
(i) CAs shall provide revocation services consistent with the procedures set forth in this CPS.

Notwithstanding the foregoing, in no event does the Entrust Datacard Group make any representations, or provide any warranties, or conditions to any Applicants, Subscribers, Relying Parties, or any other persons, entities, or organizations with respect to (i) the techniques used in the generation and storage of the Private Key corresponding to the Public Key in an Certificate, including, whether such Private Key has been Compromised or was generated using sound cryptographic techniques, (ii) the reliability of any cryptographic techniques or methods used in conducting any act, transaction, or process involving or utilizing an Certificate, (iii) any software whatsoever, or (iv) non-repudiation of any Certificate or any

transaction facilitated through the use of an Certificate, since such determination is a matter of applicable law.

Applicants, Subscribers, and Relying Parties acknowledge and agree that operations in relation to Certificates and Certificate Applications are dependent on the transmission of information over communication infrastructures such as, without limitation, the Internet, telephone and telecommunications lines and networks, servers, firewalls, proxies, routers, switches, and bridges ("Telecommunication Equipment") and that this Telecommunication Equipment is not under the control of Entrust Datacard. The Entrust Datacard Group shall not be liable for any error, failure, delay, interruption, defect, or corruption in relation to a Certificate, a Certificate CRL, OCSP message, or a Certificate Application to the extent that such error, failure, delay, interruption, defect, or corruption is caused by such Telecommunication Equipment.

9.6.2 RA Representations and Warranties

RAs operating under a CA shall:

(i) receive Certificate Applications in accordance with the terms and conditions of the CPS;
(ii) perform, log and secure verification of information submitted by Applicants when applying for Certificates, and if such verification is successful, submit a request to a CA for the issuance of a Certificate, all in accordance with the terms and conditions of the CPS;
(iii) receive and verify requests from Subscribers for the revocation of Certificates, and if the verification of a revocation request is successful, submit a request to a CA for the revocation of such Certificate, all in accordance with the terms and conditions of the CPS;
(iv) notify Subscribers, in accordance with the terms and conditions of the CPS, that an Certificate has been issued to them; and
(v) notify Subscribers, in accordance with the terms and conditions of the CPS that and Certificate issued to them has been revoked or will soon expire.

Entrust Datacard may use one or more representatives or agents to perform its obligations in respect of an Entrust Datacard RA under the CPS, any Subscription Agreements, or any Relying Party Agreements, provided that Entrust Datacard shall remain responsible for the performance of such representatives or agents under the CPS, any Subscription Agreements, or any Relying Party Agreements. Entrust Datacard may appoint independent third parties to act as RAs under a CA. Such independent third-party RAs shall be responsible for their performance under the CPS, any Subscription Agreements, or any Relying Party Agreements. Entrust Datacard shall not be responsible for the performance of such independent third-party RAs. Independent third-party RAs may use one or more representatives or agents to perform their obligations when acting as an RA under a CA. Independent third-party RAs shall remain responsible for the performance of such representatives or agents under the CPS, any Subscription Agreements, or any Relying Party Agreements. Entrust Datacard may appoint Resellers and Co-marketers for (i) Certificates, and (ii) services provided in respect to Certificates. Such Resellers and Co-marketers shall be responsible for their performance under the CPS, any Subscription Agreements, or any Relying Party Agreements. Entrust Datacard shall not be responsible for the performance of any such Resellers and Co-marketers. Resellers and Co-marketers may use one or more representatives or agents to perform their obligations under the CPS, any Subscription Agreements, or any Relying Party Agreements. Resellers and Co-marketers shall remain responsible for the performance of such representatives or agents under the CPS, any Subscription Agreements, or any Relying Party Agreements. Independent third-party RAs, Resellers, and Co-marketers shall be entitled to receive all of the benefit of all (i) disclaimers of representations, warranties, and conditions, (ii) limitations of liability, (iii) representations and warranties from Applicants, Subscribers, and Relying Parties, and (iv) indemnities from Applicants, Subscribers, and Relying Parties, set forth in this CPS, any Subscription Agreements, and any Relying Party Agreements.

The same liability provisions that apply in §9.6.1 with respect to the CAs shall apply with respect to RAs.

9.6.3 Subscriber representations and Warranties

Subscribers and Applicants shall:

(i) understand and, if necessary, receive proper education in the use of Public-Key cryptography and Certificates including Certificates;
(ii) provide, in any communications with Entrust Datacard or an independent third-party RA, correct information with no errors, misrepresentations, or omissions;
(iii) provide verification information that Entrust Datacard may request, within the time period requested;
(iv) generate a new, secure, and cryptographically sound Key Pair to be used in association with the Subscriber's Certificate or Applicant's Certificate Application, if not generated by a CA;
(v) read and agree to all terms and conditions of the CPS and Subscription Agreement;
(vi) refrain from modifying the contents of an Certificate;
(vii) use Certificates exclusively for legal and authorized purposes in accordance with the terms and conditions of the CPS and applicable laws including, without limitation, laws relating to import, export, data protection and the right to include personal information in Certificates;
(viii) only use an Certificate on behalf of the person, entity, or organization listed as the Subject in such Certificate;
(ix) keep confidential and properly protect the Subscriber's or Applicant's Private Keys;
(x) notify Entrust Datacard or, if Applicant submitted its Certificate Application to an independent third-party RA, such independent third-party RA, as soon as reasonably practicable of any change to any information included in the Applicant's Certificate Application or any change in any circumstances that would make the information in the Applicant's Certificate Application misleading or inaccurate;
(xi) notify Entrust Datacard or, if Subscriber received its Certificate through an independent third-party RA, such independent third-party RA, as soon as reasonably practicable of any change to any information included in the Subscriber's Certificate or any change in any circumstances that would make the information in the Subscriber's Certificate misleading or inaccurate;
(xii) immediately cease to use an Certificate if any information included in the Subscriber's Certificate or if a change in circumstances would make the information in the Subscriber's Certificate misleading or inaccurate;
(xiii) notify Entrust Datacard or, if Subscriber received its Certificate from an independent third-party RA, such independent third-party RA, immediately of any suspected or actual Compromise of the Subscriber's or Applicant's Private Keys and request the revocation of such Certificate;
(xiv) immediately cease to use the Subscriber's Certificate upon (a) expiration or revocation of such Certificate, or (b) any suspected or actual Compromise of the Private Key corresponding to the Public Key in such Certificate, and remove such Certificate from the devices and/or software in which it has been installed, where applicable;
(xv) refrain from using the Subscriber's Private Key corresponding to the Public Key in the Subscriber's Certificate to sign other Certificates; and
(xvi) use the Subscriber's or Applicant's own judgment about whether it is appropriate, given the level of security and trust provided by an Certificate, to use an Certificate in any given circumstance.

Certificates and related information may be subject to export, import, and/or use restrictions. Subscribers shall comply with all laws and regulations applicable to a Subscriber's right to export, import, and/or use Certificates and/or related information, including, without limitation, all laws and regulations in respect to nuclear, chemical or biological weapons proliferation. Subscribers shall be responsible for procuring all required licenses and permissions for any export, import, and/or use of Certificates and/or related information. Certain cryptographic techniques, software, hardware, and firmware ("Technology") that may be used in processing or in conjunction with Certificates may be subject to export, import, and/or use restrictions. Subscribers shall comply with all laws and regulations applicable to a Subscriber's right to export, import, and/or use such Technology or related information. Subscribers shall be responsible for procuring all required licenses and permissions for any export, import, and/or use of such Technology or related information.

Subscribers and Applicants represent and warrant to Entrust Datacard and to all Certificate Beneficiaries, that:

(i) 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);

(ii) provision of verification information reasonably requested by Entrust Datacard or its delegate will not be unreasonably delayed;

(iii) the Private Key corresponding to the Public Key submitted to Entrust Datacard in connection with an Certificate Application was created using sound cryptographic techniques, if not generated by a CA;

(iv) 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;

(v) any information provided to Entrust Datacard 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;

(vi) the Certificate(s) will not be installed or used until it has reviewed and verified the accuracy of the data in each Certificate;

(vii) Subscriber will immediately respond to Entrust Datacard's instructions concerning (1) compromise of the Private Key associated with any Certificate and (2) misuse or suspected misuse of an Certificate;

(viii) all use of the Certificate and its associated Private Key shall cease immediately, and the Subscriber shall promptly notify Entrust Datacard 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;

(ix) 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;

(x) the Certificates will not be used for any hazardous or unlawful (including tortious) activities; and

(xi) 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;

(xii) 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 Subscription Agreement and the CPS;

(xiii) the Subscriber has the exclusive right to use the domain name listed in the Certificate; and

(xiv) 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.

eIDAS QSigC

In respect to eIDAS QSigC, Subscribers and Applicants represent and warrant to Entrust Datacard and to all Certificate Beneficiaries, that:

(xv) Key Pairs shall only be used for cryptographic functions within the secure cryptographic device as defined in §6.2.11;

(xvi) If the Subscriber or Applicant generates the Key Pair, they will be generated with the secure cryptographic device; and

(xvii) Key Pairs shall only be used for electronic signatures.

eIDAS QSealC and PSD2 QSealC

In respect to eIDAS QSealC and PSD2 QSealC, Subscribers and Applicants represent and warrant to Entrust Datacard and to all Certificate Beneficiaries, that:

(xviii) Key Pairs shall only be used for electronic seals.

9.6.4 Relying Parties Representations and Warranties

Relying Parties shall:

(i) understand and, if necessary, receive proper education in the use of Public-Key cryptography and Certificates including Certificates;

(ii) read and agree to all terms and conditions of the CPS and the Relying Party Agreement;

(iii) verify Certificates, including use of CRLs, in accordance with the certification path validation procedure specified in ITU-T Rec. X.509:2005 | ISO/IEC 9594-8 (2005), taking into account any critical extensions and approved technical corrigenda as appropriate;

(iv) trust and make use of a Certificate only if the Certificate has not expired or been revoked and if a proper chain of trust can be established to a trustworthy Root; and

(v) make their own judgment and rely on a Certificate only if such reliance is reasonable in the circumstances, including determining whether such reliance is reasonable given the nature of the security and trust provided by a Certificate and the value of any transaction that may involve the use of a Certificate.

(vi) trust and make use of a Certificate only if the Certificate has not expired or been revoked and if a proper chain of trust can be established to a trustworthy root.

Certificates and related information may be subject to export, import, and/or use restrictions. Relying Parties shall comply with all laws and regulations applicable to a Relying Party's right to use Certificates and/or related information, including, without limitation, all laws and regulations in respect to nuclear, chemical or biological weapons proliferation. Relying Parties shall be responsible for procuring all required licenses and permissions for any export, import, and/or use of Certificates and/or related information. Certain cryptographic techniques, software, hardware, and firmware ("Technology") that may be used in processing or in conjunction with Certificates may be subject to export, import, and/or use restrictions. Relying Parties shall comply with all laws and regulations applicable to a Relying Party's right to export, import, and/or use such Technology or related information. Relying Parties shall be responsible for procuring all required licenses and permissions for any export, import, and/or use of such Technology or related information.

Relying Parties represent and warrant to Entrust Datacard that:

(i) the Relying Party shall properly validate a Certificate before making a determination about whether to rely on such Certificate, including confirmation that the Certificate has not expired or been revoked and that a proper chain of trust can be established to a trustworthy root;

(ii) the Relying Party shall not rely on an Certificate that cannot be validated back to a trustworthy root;

(iii) the Relying Party shall exercise its own judgment in determining whether it is reasonable under the circumstances to rely on an Certificate, including determining whether such reliance is reasonable given the nature of the security and trust provided by an Certificate and the value of any transaction that may involve the use of an Certificate; and

(iv) the Relying Party shall not use a Certificate for any hazardous or unlawful (including tortious) activities.

(v) the Relying Party shall not rely on a revoked or expired Certificate;

9.6.5 Representations and Warranties of Other Participants

Third parties performing Certificate services shall provide those services in accordance with the requirements of the CPS.

9.7 Disclaimers of Warranties

EXCEPT FOR THE LIMITED WARRANTY DESCRIBED IN §9.6.1 §9.6.1.1 ABOVE, ENTRUST DATACARD AND ENTRUST DATACARD GROUP AFFILIATES EXPRESSLY DISCLAIMS AND

MAKES NO REPRESENTATION, WARRANTY OR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, WITH RESPECT TO THIS CPS OR ANY CERTIFICATE ISSUED HEREUNDER, INCLUDING WITHOUT LIMITATION, ALL WARRANTIES OF QUALITY, MERCHANTABILITY, NON-INFRINGEMENT, TITLE AND FITNESS FOR A PARTICULAR PURPOSE, AND ALL WARRANTIES, REPRESENTATIONS, CONDITIONS, UNDERTAKINGS, TERMS AND OBLIGATIONS IMPLIED BY STATUTE OR COMMON LAW, TRADE USAGE, COURSE OF DEALING OR OTHERWISE ARE HEREBY EXCLUDED TO THE FULLEST EXTENT PERMITTED BY LAW. EXCEPT FOR THE LIMITED WARRANTY DESCRIBED ABOVE, ENTRUST DATACARD AND ENTRUST DATACARD GROUP AFFILIATES FURTHER DISCLAIM AND MAKES NO REPRESENTATION, WARRANTY OR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, TO ANY APPLICANT, SUBSCRIBER OR ANY RELYING PARTY THAT (A) THE SUBSCRIBER TO WHICH IT HAS ISSUED A CERTIFICATE IS IN THE FACT THE PERSON, ENTITY OR ORGANIZATION IT CLAIMS TO HAVE BEEN (B) A SUBSCRIBER IS IN FACT THE PERSON, ENTITY OR ORGANIZATION LISTED IN THE CERTIFICATE, OR (C) THAT THE INFORMATION CONTAINED IN THE CERTIFICATES OR IN ANY CERTIFICATE STATUS MECHANISM COMPILED, PUBLISHED OR OTHERWISE DISSEMINATED BY ENTRUST DATACARD, OR THE RESULTS OF ANY CRYPTOGRAPHIC METHOD IMPLEMENTED IN CONNECTION WITH THE CERTIFICATES IS ACCURATE, AUTHENTIC, COMPLETE OR RELIABLE.

IT IS AGREED AND ACKNOWLEDGED THAT APPLICANTS AND SUBSCRIBERS ARE LIABLE FOR ANY MISREPRESENTATIONS MADE TO ENTRUST DATACARD AND RELIED UPON BY A RELYING PARTY. ENTRUST DATACARD AND ENTRUST DATACARD GROUP AFFILIATES DO NOT WARRANT OR GUARANTEE UNDER ANY CIRCUMSTANCES THE "NON-REPUDIATION" BY A SUBSCRIBER AND/OR RELYING PARTY OF ANY TRANSACTION ENTERED INTO BY THE SUBSCRIBER AND/OR RELYING PARTY INVOLVING THE USE OF OR RELIANCE UPON A CERTIFICATE.

IT IS UNDERSTOOD AND AGREED UPON BY SUBSCRIBERS AND RELYING PARTIES THAT IN USING AND/OR RELYING UPON A CERTIFICATE THEY ARE SOLELY RESPONSIBLE FOR THEIR RELIANCE UPON THAT CERTIFICATE AND THAT SUCH PARTIES MUST CONSIDER THE FACTS, CIRCUMSTANCES AND CONTEXT SURROUNDING THE TRANSACTION IN WHICH THE CERTIFICATE IS USED IN DETERMINING SUCH RELIANCE.

THE SUBSCRIBERS AND RELYING PARTIES AGREE AND ACKNOWLEDGE THAT CERTIFICATES HAVE A LIMITED OPERATIONAL PERIOD AND MAY BE REVOKED AT ANY TIME. SUBSCRIBERS AND RELYING PARTIES ARE UNDER AN OBLIGATION TO VERIFY WHETHER A CERTIFICATE IS EXPIRED OR HAS BEEN REVOKED. ENTRUST DATACARD AND ENTRUST DATACARD GROUP AFFILIATES HEREBY DISCLAIM ANY AND ALL LIABILITY TO SUBSCRIBERS AND RELYING PARTIES WHO DO NOT FOLLOW SUCH PROCEDURES. MORE INFORMATION ABOUT THE SITUATIONS IN WHICH A CERTIFICATE MAY BE REVOKED CAN BE FOUND IN §4.9.3 OF THIS CPS.

9.8 Limitations of Liability

9.8.1 IN RESPECT TO APPLICANT'S, SUBSCRIBERS AND RELYING PARTIES, THE ENTRUST GROUP'S ENTIRE LIABILITY UNDER THE CPS IS SET FORTH IN THE APPLICABLE SUBSCRIPTION AGREEMENT(S) AND/OR RELYING PARTY AGREEMENT(S). THE ENTRUST DATACARD GROUP'S ENTIRE LIABILITY TO ANY OTHER PARTY IS SET OUT IN THE AGREEMENT(S) BETWEEN ENTRUST DATACARD AND SUCH OTHER PARTY. TO THE EXTENT ENTRUST DATACARD HAS ISSUED THE CERTIFICATE IN COMPLIANCE WITH THE CPS, THE ENTRUST DATACARD GROUP SHALL HAVE NO LIABILITY TO THE SUBSCRIBER, RELYING PARTY OR ANY OTHER PARTY FOR ANY CLAIMS, DAMAGES OR LOSSES SUFFERED AS THE RESULT OF THE USE OF OR RELIANCE ON SUCH CERTIFICATE.

FOR GREATER CERTAINTY, ENTRUST DATACARD GROUP'S ENTIRE LIABILITY UNDER THIS CPS TO: (I) AN APPLICANT OR SUBSCRIBER IS SET OUT IN THE SUBSCRIPTION AGREEMENT BETWEEN ENTRUST DATACARD (OR AN AFFILIATE OF ENTRUST DATACARD) AND SUCH SUBSCRIBER; AND (II) A RELYING PARTY IS SET OUT IN THE RELYING PARTY AGREEMENT POSTED IN THE REPOSITORY ON THE DATE THE RELYING PARTY RELIES ON SUCH CERTIFICATE.

9.8.2 TO THE EXTENT ENTRUST DATACARD HAS ISSUED THE CERTIFICATE(S) IN COMPLIANCE WITH THE CPS, THE ENTRUST DATACARD GROUP SHALL HAVE NO LIABILITY TO THE SUBSCRIBER, RELYING PARTY OR ANY OTHER PARTY FOR ANY CLAIMS, DAMAGES OR LOSSES SUFFERED AS THE RESULT OF THE USE OF OR RELIANCE ON SUCH CERTIFICATE. SUBJECT TO THE FOREGOING AND IF §9.8.1 ABOVE DOES NOT APPLY:

9.8.2.1 ENTRUST DATACARD GROUP AFFILIATES, ANY RESELLERS, CO-MARKETERS, SUBCONTRACTORS, DISTRIBUTORS, AGENTS, SUPPLIERS, AND EMPLOYEES AND DIRECTORS OF ANY OF THE FOREGOING (COLLECTIVELY, "ENTRUST DATACARD AND ITS ENTITIES") SHALL NOT BE LIABLE IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, FOR BREACH OF A STATUTORY DUTY OR IN ANY OTHER WAY (EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) FOR:

(I) ANY ECONOMIC LOSS (INCLUDING, WITHOUT LIMITATION, LOSS OF REVENUES, PROFITS, CONTRACTS, BUSINESS OR ANTICIPATED SAVINGS);

(II) TO THE EXTENT ALLOWED BY APPLICABLE LAW, ANY LOSS OR DAMAGE RESULTING FROM DEATH OR INJURY OF SUBSCRIBER AND/OR ANY RELYING PARTY OR ANYONE ELSE;

(III) ANY LOSS OF GOODWILL OR REPUTATION;

(IV) ANY OTHER INDIRECT, CONSEQUENTIAL, INCIDENTAL, MULTIPLE, SPECIAL, PUNITIVE, EXEMPLARY DAMAGES, OR

V) ANY LOSS OR DAMAGE THAT IS NOT DIRECTLY ATTRIBUTABLE TO THE USE OR RELIANCE ON A CERTIFICATE OR SERVICE PROVIDED UNDER THIS CPS INCLUDING, WITHOUT LIMITATION, ANY LOSS OR DAMAGE RESULTING FROM THE COMBINATION OR INTEGRATION OF THE CERTIFICATE OR SERVICE WITH ANY SOFTWARE OR HARDWARE NOT PROVIDED BY ENTRUST DATACARD IF THE LOSS OR DAMAGE WOULD NOT HAVE OCCURRED AS A RESULT OF USE OF THE CERTIFICATE ALONE.

IN ANY CASE WHETHER OR NOT SUCH LOSSES OR DAMAGES WERE WITHIN THE CONTEMPLATION OF THE PARTIES AT THE TIME OF THE APPLICATION FOR, INSTALLATION OF, USE OF OR RELIANCE ON THE CERTIFICATE, OR AROSE OUT OF ANY OTHER MATTER OR SERVICES (INCLUDING, WITHOUT LIMITATION, ANY SUPPORT SERVICES) UNDER THIS AGREEMENT, THE APPLICABLE CPS OR WITH REGARD TO THE USE OF OR RELIANCE ON THE CERTIFICATE.

9.8.2.2 SUBJECT TO 9.8.3 BELOW, IN NO EVENT SHALL THE TOTAL AGGREGATE LIABILITY OF ENTRUST DATACARD AND ITS ENTITIES TO ANY APPLICANT, SUBSCRIBER, RELYING PARTY OR ANY OTHER PERSON, ENTITY, OR ORGANIZATION ARISING OUT OF OR RELATING TO THIS AGREEMENT, THE CPS AND ALL CERTIFICATES ISSUED (INCLUDING WITHOUT LIMITATION, THE INSTALLATION OF, USE OF OR RELIANCE UPON A CERTIFICATE) AND SERVICES PROVIDED UNDER THIS AGREEMENT UNDER ANY CAUSE OF ACTION, OR ANY CONTRACT, STRICT LIABILITY, TORT (INCLUDING NEGLIGENCE), OR OTHER LEGAL OR EQUITABLE THEORY OR IN ANY OTHER WAY, EXCEED THE GREATER OF ONE THOUSAND UNITED STATES DOLLARS ($1,000.00 U.S.), OR (2) THE FEES PAID BY SUCH PARTY TO ENTRUST DATACARD UNDER THIS CPS DURING THE TWELVE MONTHS PRIOR TO THE INITIATION OF THE CLAIM TO A MAXIMUM OF ONE HUNDRED THOUSAND DOLLARS ($100,000.00)) (EXCEPT THAT FOR ANY EIDAS QUALIFIED WEB AUTHENTICATION CERTIFICATES OR PSD2 QUALIFIED WEB AUTHENTICATION CERTIFICATES ISSUED UNDER THIS CPS, ENTRUST DATACARD AND ITS ENTITIES'

AGGREGATE LIABILITY IS LIMITED TO TWO THOUSAND U.S. DOLLARS (US$2,000.00) PER SUBSCRIBER OR RELYING PARTY PER EV SSL CERTIFICATE, UP TO A MAXIMUM OF ONE HUNDRED THOUSAND U.S. DOLLARS (US$100,000.00).

9.8.3 BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, THE ABOVE EXCLUSIONS OF INCIDENTAL AND CONSEQUENTIAL DAMAGES MAY NOT APPLY TO AN APPLICANT, SUBSCRIBER AND/OR A RELYING PARTY BUT SHALL BE GIVEN EFFECT TO THE FULL EXTENT PERMITTED BY LAW.

9.8.4 Without limitation, the Entrust Datacard Group shall not be liable to any Applicants, Subscribers, Relying Parties or any other person, entity, or organization for any losses, costs, expenses, liabilities, damages, claims, or settlement amounts arising out of or relating to use of an Certificate or any services provided in respect to an Certificate if:

(i) the Certificate was issued as a result of errors, misrepresentations, or other acts or omissions of a Subscriber or of any other person, entity, or organization;
the Certificate has expired or has been revoked;
the Certificate has been modified or otherwise altered;
the Subscriber failed to stop using an Certificate after the information contain in such Certificate changed or after circumstances changed so that the information contained in such Certificate became misleading or inaccurate;
a Subscriber breached the CPS or the Subscriber's Subscription Agreement, or a Relying Party breached the CPS or the Relying Party's Relying Party Agreement;
the Private Key associated with the Certificate has been Compromised; or
the Certificate is used other than as permitted by the CPS or is used in contravention of applicable law.

In no event shall the Entrust Datacard Group be liable to any Applicant, Subscriber, or any other person, entity, or organization for any losses, costs, liabilities, expenses, damages, claims, or settlement amounts arising out of or relating to the refusal by Entrust Datacard to issue or request the issuance of a Certificate. In no event shall the Entrust Datacard Group be liable to any Applicant, Subscriber, or any other person, entity, or organization for any losses, costs, liabilities, expenses, damages, claims, or settlement amounts arising out of or relating to any delay by the Entrust Datacard Group, in issuing or in requesting the issuance of a Certificate.

In no event shall the Entrust Datacard Group be liable to any Subscriber, Relying Party, or any other person, entity, or organization for any losses, costs, expenses, liabilities, damages, claims, or settlement amounts arising out of or relating to any proceeding or allegation that an Certificate or any information contained in an Certificate infringes, misappropriates, dilutes, unfairly competes with, or otherwise violates any patent, trademark, copyright, trade secret, or any other intellectual property right or other right of any person, entity, or organization in any jurisdiction.

9.9 Indemnities

9.9.1 Indemnification by CAs

Entrust Datacard will defend, indemnify, and hold harmless each Application Software Vendor for any and all third party claims, damages, and losses suffered by such Application Software Vendor related to a Certificate issued by the CA that is not in compliance with the Baseline Requirements in effect at the time the Certificate was issued, regardless of the cause of action or legal theory involved. This does not apply, however, to any claim, damages, or loss suffered by such Application Software Vendor related to a Certificate issued by the CA where such claim, damage, or loss was directly or indirectly caused by such Application Software Vendor's software displaying as not trustworthy a Certificate that is still valid, or displaying as trustworthy: (1) a Certificate that has expired, or (2) a Certificate that has been revoked (but only in cases where the revocation status is currently available from the CA online, and the application software either failed to check such status or ignored an indication of revoked status).

9.9.2 Indemnification for Relying Parties

RELYING PARTIES SHALL INDEMNIFY AND HOLD ENTRUST DATACARD AND ALL INDEPENDENT THIRD-PARTY REGISTRATION AUTHORITIES OPERATING UNDER AN CERTIFICATION AUTHORITY, AND ALL RESELLERS, CO-MARKETERS, AND ALL SUBCONTRACTORS, DISTRIBUTORS, AGENTS, APPLICATION SOFTWARE VENDORS, SUPPLIERS, EMPLOYEES, AND DIRECTORS OF ANY OF THE FOREGOING (COLLECTIVELY, THE "INDEMNIFIED PARTIES") HARMLESS FROM AND AGAINST ANY AND ALL LIABILITIES, LOSSES, COSTS, EXPENSES, DAMAGES, CLAIMS, AND SETTLEMENT AMOUNTS (INCLUDING REASONABLE ATTORNEY'S FEES, COURT COSTS, AND EXPERT'S FEES) ARISING OUT OF OR RELATING TO ANY USE OR RELIANCE BY A RELYING PARTY ON ANY CERTIFICATE OR ANY SERVICE PROVIDED IN RESPECT TO CERTIFICATES, INCLUDING (I) LACK OF PROPER VALIDATION OF AN CERTIFICATE BY A RELYING PARTY, (II) RELIANCE BY THE RELYING PARTY ON AN EXPIRED OR REVOKED CERTIFICATE, (III) USE OF AN CERTIFICATE OTHER THAN AS PERMITTED BY THE CPS, THE SUBSCRIPTION AGREEMENT, ANY RELYING PARTY AGREEMENT, AND APPLICABLE LAW, (IV) FAILURE BY A RELYING PARTY TO EXERCISE REASONABLE JUDGMENT IN THE CIRCUMSTANCES IN RELYING ON AN CERTIFICATE, OR (V) ANY CLAIM OR ALLEGATION THAT THE RELIANCE BY A RELYING PARTY ON AN CERTIFICATE OR THE INFORMATION CONTAINED IN AN CERTIFICATE INFRINGES, MISAPPROPRIATES, DILUTES, UNFAIRLY COMPETES WITH, OR OTHERWISE VIOLATES THE RIGHTS INCLUDING INTELLECTUAL PROPERTY RIGHTS OR ANY OTHER RIGHTS OF ANYONE IN ANY JURISDICTION. NOTWITHSTANDING THE FOREGOING, RELYING PARTIES SHALL NOT BE OBLIGATED TO PROVIDE ANY INDEMNIFICATION TO AN INDEMNIFIED PARTY IN RESPECT TO ANY LIABILITIES, LOSSES, COSTS, EXPENSES, DAMAGES, CLAIMS, AND SETTLEMENT AMOUNTS (INCLUDING REASONABLE ATTORNEY'S FEES, COURT COSTS AND EXPERT'S FEES) TO THE EXTENT THAT SUCH LIABILITIES, LOSSES, COSTS, EXPENSES, DAMAGES, CLAIMS, AND SETTLEMENT AMOUNTS (INCLUDING REASONABLE ATTORNEY'S FEES, COURT COSTS, AND EXPERT'S FEES) ARISE OUT OF OR RELATE TO ANY WILLFUL MISCONDUCT BY SUCH INDEMNIFIED PARTY.

9.9.3 Indemnification by Subscribers

SUBSCRIBERS SHALL INDEMNIFY AND HOLD ENTRUST DATACARD AND ALL INDEPENDENT THIRD-PARTY REGISTRATION AUTHORITIES OPERATING UNDER A CERTIFICATION AUTHORITY, AND ALL RESELLERS, CO-MARKETERS, AND ALL SUBCONTRACTORS, DISTRIBUTORS, AGENTS, APPLICATION SOFTWARE VENDORS, SUPPLIERS, EMPLOYEES, OR DIRECTORS OF ANY OF THE FOREGOING (COLLECTIVELY, THE "INDEMNIFIED PARTIES") HARMLESS FROM AND AGAINST ANY AND ALL LIABILITIES, LOSSES, COSTS, EXPENSES, DAMAGES, CLAIMS, AND SETTLEMENT AMOUNTS (INCLUDING REASONABLE ATTORNEY'S FEES, COURT COSTS, AND EXPERT'S FEES) ARISING OUT OF OR RELATING TO ANY RELIANCE BY A RELYING PARTY ON ANY CERTIFICATE OR ANY SERVICE PROVIDED IN RESPECT TO CERTIFICATES, INCLUDING ANY (I) ERROR, MISREPRESENTATION OR OMISSION MADE BY A SUBSCRIBER IN USING OR APPLYING FOR AN CERTIFICATE, (II) MODIFICATION MADE BY A SUBSCRIBER TO THE INFORMATION CONTAINED IN AN CERTIFICATE, (III) USE OF AN CERTIFICATE OTHER THAN AS PERMITTED BY THE CPS, THE SUBSCRIPTION AGREEMENT, ANY RELYING PARTY AGREEMENT, AND APPLICABLE LAW, (IV) FAILURE BY A SUBSCRIBER TO TAKE THE NECESSARY PRECAUTIONS TO PREVENT LOSS, DISCLOSURE, COMPROMISE OR UNAUTHORIZED USE OF THE PRIVATE KEY CORRESPONDING TO THE PUBLIC KEY IN SUCH SUBSCRIBER'S CERTIFICATE, OR (V) ALLEGATION THAT THE USE OF A SUBSCRIBER'S CERTIFICATE OR THE INFORMATION CONTAINED IN A SUBSCRIBER'S CERTIFICATE INFRINGES, MISAPPROPRIATES, DILUTES, UNFAIRLY COMPETES WITH, OR OTHERWISE VIOLATES THE RIGHTS INCLUDING INTELLECTUAL PROPERTY RIGHTS OR ANY OTHER RIGHTS OF ANYONE IN ANY JURISDICTION. NOTWITHSTANDING THE FOREGOING, A SUBSCRIBER SHALL NOT BE OBLIGATED TO PROVIDE ANY INDEMNIFICATION TO AN INDEMNIFIED PARTY IN RESPECT TO ANY LIABILITIES, LOSSES,

COSTS, EXPENSES, DAMAGES, CLAIMS, AND SETTLEMENT AMOUNTS (INCLUDING REASONABLE ATTORNEY'S FEES, COURT COSTS AND EXPERTS FEES) TO THE EXTENT THAT SUCH LIABILITIES, LOSSES, COSTS, EXPENSES, DAMAGES, CLAIMS, AND SETTLEMENT AMOUNTS (INCLUDING REASONABLE ATTORNEY'S FEES, COURT COSTS, AND EXPERT'S FEES) ARISE OUT OF OR RELATE TO ANY WILLFUL MISCONDUCT BY SUCH INDEMNIFIED PARTY.

9.10 Term and Termination

9.10.1 Term

This CPS will be effective on the date this CPS is published in the Repository and will continue until a newer version of the CPS is published.

9.10.2 Termination

This CPS will remain in effect until replaced by a newer version.

9.10.3 Effect of Termination and Survival

The provisions of sections 1.6, 3.1.6, 5.5, 9.1, 9.3, 9.4, 9.5, 9.7, 9.8, 9.9.2, 9.9.3, 9.10.3, 9.13, 9.14 and 9.16 shall survive termination or expiration of the CPS, any Subscription Agreements, and any Relying Party Agreements. All references to sections that survive termination of the CPS, any Subscription Agreements, and any Relying Party Agreements, shall include all sub-sections of such sections. All payment obligations shall survive any termination or expiration of the CPS, any Subscription Agreements, and any Relying Party Agreements.

9.11 Individual Notices and Communications with Participants

Unless otherwise set out in in a Subscription Agreement or Relying Party Agreement, any notice to be given to Entrust Datacard under this CPS, a Subscription Agreement, or a Relying Party Agreement shall be given in writing to the address specified in §1.5.2 by prepaid receipted mail, overnight courier or email, and shall be effective as follows (i) in the case of courier or email, on the next Business Day, and (ii) in the case of receipted mail, five (5) Business Days following the date of deposit in the mail. Any notice to be given by Entrust Datacard under the CPS, any Subscription Agreement, or any Relying Party Agreement shall be given by email or courier to the last address or email address for the Subscriber on file with Entrust Datacard. The notice shall become effective on the next Business Day.

9.12 Amendments

9.12.1 Procedure for Amendment

Entrust Datacard may, in its discretion, modify the CPS and the terms and conditions contained herein from time to time. Entrust Datacard shall modify the CPS to stay concurrent with the latest version of the Baseline Requirements, EV SSL Guidelines, and ETSI Guidelines.

9.12.2 Notification Mechanism and Period

Modifications to the CPS shall be published in the Repository. Such modifications shall become effective immediately upon publication in the Repository and remain valid until the duration of such publication. In the event that Entrust Datacard makes a significant modification to CPS, the version number of the CPS shall be updated. Unless a Subscriber ceases to use, removes, and requests revocation of such Subscriber's Certificate(s) prior to the date on which an updated version of the CPS becomes effective, such Subscriber shall be deemed to have consented to the terms and conditions of such updated version of the CPS and shall be bound by the terms and conditions of such updated version of the CPS.

9.12.3 Circumstances Under which OID must be Changed

No stipulation.

9.13 Dispute Resolution Provisions

Unless otherwise set out in in a Subscription Agreement or Relying Party Agreement, any disputes between a Subscriber or an Applicant and Entrust Datacard or any third-party RAs operating under the CAs, or a Relying Party and Entrust Datacard or any third-party RAs operating under the CAs, shall be submitted to mediation in accordance with the Commercial Mediation Rules of the American Arbitration Association which shall take place in English in Ottawa, Ontario. In the event that a resolution to such dispute cannot be achieved through mediation within thirty (30) days, the dispute shall be submitted to binding arbitration. The arbitrator shall have the right to decide all questions of arbitrability. The dispute shall be finally settled by arbitration in accordance with the rules of the American Arbitration Association, as modified by this provision. Such arbitration shall take place in English in Ottawa, Ontario, before a sole arbitrator appointed by the American Arbitration Association (AAA) who shall be appointed by the AAA from its Technology Panel and shall be reasonably knowledgeable in electronic commerce disputes. The arbitrator shall apply the laws of the Province of Ontario, without regard to its conflict of laws provisions, and shall render a written decision within thirty (30) days from the date of close of the arbitration hearing, but no more than one (1) year from the date that the matter was submitted for arbitration. The decision of the arbitrator shall be binding and conclusive and may be entered in any court of competent jurisdiction. In each arbitration, the prevailing party shall be entitled to an award of all or a portion of its costs in such arbitration, including reasonable attorney's fees actually incurred. Nothing in the CPS, or in any Subscription Agreement, or any Relying Party Agreement shall preclude Entrust Datacard or any third-party RAs operating under the CAs from applying to any court of competent jurisdiction for temporary or permanent injunctive relief, without breach of this §9.13 and without any abridgment of the powers of the arbitrator, with respect to any (i) alleged Compromise that affects the integrity of an Certificate, or (ii) alleged breach of the terms and conditions of the CPS, any Subscription Agreement, or any Relying Party Agreement. The institution of any arbitration or any action shall not relieve an Applicant, Subscriber or Relying Party of its obligations under the CPS, any Subscription Agreement, or any Relying Party Agreement.

Any and all arbitrations or legal actions in respect to a dispute that is related to an Certificate or any services provided in respect to an Certificate shall be commenced prior to the end of one (1) year after (i) the expiration or revocation of the Certificate in dispute, or (ii) the date of provision of the disputed service or services in respect to the Certificate in dispute, whichever is sooner. If any arbitration or action in respect to a dispute that is related to an Certificate or any service or services provided in respect to an Certificate is not commenced prior to such time, any party seeking to institute such an arbitration or action shall be barred from commencing or proceeding with such arbitration or action.

9.14 Governing Law

Unless otherwise set out in in a Subscription Agreement or Relying Party Agreement, the laws of the Province of Ontario, Canada,, excluding its conflict of laws rules, shall govern the construction, validity, interpretation, enforceability and performance of the CPS, all Subscription Agreements and all Relying Party Agreements. The application of the United Nations Convention on Contracts for the International Sale of Goods to the CPS, any Subscription Agreements, and any Relying Party Agreements is expressly excluded. Any dispute arising out of or in respect to the CPS, any Subscription Agreement, any Relying Party Agreement, or in respect to any Certificates or any services provided in respect to any Certificates that is not resolved by alternative dispute resolution, shall be brought in the provincial or federal courts sitting in Ottawa, Ontario, and each person, entity, or organization hereby agrees that such courts shall have personal and exclusive jurisdiction over such disputes. In the event that any matter is brought in a provincial or federal court, Applicants, Subscribers, and Relying Parties waive any right that such Applicants, Subscribers, and Relying Parties may have to a jury trial.

9.15 Compliance with Applicable Law

Subscribers and Relying Parties acknowledge and agree to use Certificates in compliance with all applicable laws and regulations, including without limitation all applicable export laws and regulations. Entrust Datacard may refuse to issue or may revoke Certificates if in the reasonable opinion of Entrust Datacard such issuance or the continued use of such Certificates would violate applicable laws and regulations.

Entrust Datacard shall ensure that it operates in a legal and trustworthy manner. In particular, Entrust Datacard shall comply with all the applicable legal requirements (such as the General Data Protection Regulation (GDPR)) by maintaining a competent and licensed legal department staff that is knowledgeable about all applicable laws and regulations, performs ongoing continuing legal education as to new laws and regulations, updates Entrust Datacard internal policies and practices (including this CPS) to comply with applicable laws and regulations, and trains other Entrust Datacard staff (as applicable) in all new laws and regulations pertaining to their functions and duties.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

Certificates and the rights granted under the CPS, any Subscription Agreement, or any Relying Party Agreement are personal to the Applicant, Subscriber, or Relying Party that entered into the Subscription Agreement or Relying Party Agreement and cannot be assigned, sold, transferred, or otherwise disposed of, whether voluntarily, involuntarily, by operation of law, or otherwise, without the prior written consent of Entrust Datacard or the relevant RA under a CA. Any attempted assignment or transfer without such consent shall be void and shall automatically terminate such Applicant's, Subscriber's or Relying Party's rights under the CPS, any Subscription Agreement, or any Relying Party Agreement. Entrust Datacard may assign, sell, transfer, or otherwise dispose of the CPS, any Subscription Agreements, or any Relying Party Agreements together with all of its rights and obligations under the CPS, any Subscription Agreements, and any Relying Party Agreements (i) to an Affiliate, or (ii) as part of a sale, merger, or other transfer of all or substantially all the assets or stock of the business of Entrust Datacard to which the CPS, the Subscription Agreements, and Relying Party Agreements relate. Subject to the foregoing limits, this CPS and terms and conditions of any Subscription Agreement, or any Relying Party Agreement shall be binding upon and shall inure to the benefit of permitted successors and assigns of Entrust Datacard, any third-party RAs operating under the CAs, Applicants, Subscribers, and Relying Parties, as the case may be.

The CPS, the Subscription Agreements, and the Relying Party Agreements state all of the rights and obligations of the Entrust Datacard Group, any Applicant, Subscriber, or Relying Party and any other persons, entities, or organizations in respect to the subject matter hereof and thereof and such rights and obligations shall not be augmented or derogated by any prior agreements, communications, or understandings of any nature whatsoever whether oral or written. The rights and obligations of the Entrust Datacard Group may not be modified or waived orally and may be modified only in a writing signed or authenticated by a duly authorized representative of Entrust Datacard.

9.16.3 Severability

Whenever possible, each provision of the CPS, any Subscription Agreements, and any Relying Party Agreements shall be interpreted in such a manner as to be effective and valid under applicable law. If the application of any provision of the CPS, any Subscription Agreements, or any Relying Party Agreements or any portion thereof to any particular facts or circumstances shall be held to be invalid or unenforceable by an arbitrator or court of competent jurisdiction, then (i) the validity and enforceability of such provision as applied to any other particular facts or circumstances and the validity of other provisions of the CPS, any Subscription Agreements, or any Relying Party Agreements shall not in any way be affected or impaired thereby, and (ii) such provision shall be enforced to the maximum extent possible so as to effect its intent and it shall be reformed without further action to the extent necessary to make such provision valid and enforceable.

9.16.4 Enforcement

No stipulation.

9.16.5 Force Majeure

The Entrust Datacard Group shall not be in default hereunder or liable for any losses, costs, expenses, liabilities, damages, claims, or settlement amounts arising out of or related to delays in performance or from failure to perform or comply with the terms of the CPS, any Subscription Agreement, or any Relying Party Agreement due to any causes beyond its reasonable control, which causes can include (without limitation) acts of God or the public enemy, riots and insurrections, war, accidents, fire, strikes and other labor difficulties (whether or not Entrust Datacard is in a position to concede to such demands), embargoes, judicial action, failure or default of any superior CA, lack of or inability to obtain export permits or approvals, necessary labor, materials, energy, utilities, components or machinery, acts of civil or military authorities.

9.17 Other Provisions

9.17.1 Conflict of Provisions

In the event of any inconsistency between the provisions of this CPS and the provisions of any Subscription Agreement or any Relying Party Agreement, the terms and conditions of this CPS shall govern.

9.17.2 Fiduciary Relationships

Nothing contained in this CPS, or in any Subscription Agreement, or any Relying Party Agreement shall be deemed to constitute the Entrust Datacard Group as the fiduciary, partner, agent, trustee, or legal representative of any Applicant, Subscriber, Relying Party or any other person, entity, or organization or to create any fiduciary relationship between the Entrust Datacard Group and any Subscriber, Applicant, Relying Party or any other person, entity, or organization, for any purpose whatsoever. Nothing in the CPS, or in any Subscription Agreement or any Relying Party Agreement shall confer on any Subscriber, Applicant, Relying Party, or any other third party, any authority to act for, bind, or create or assume any obligation or responsibility, or make any representation on behalf of the Entrust Datacard Group.

9.17.3 Waiver

The failure of Entrust Datacard to enforce, at any time, any of the provisions of this CPS, a Subscription Agreement with Entrust Datacard, or a Relying Party Agreement with Entrust Datacard or the failure of Entrust Datacard to require, at any time, performance by any Applicant, Subscriber, Relying Party or any other person, entity, or organization of any of the provisions of this CPS, a Subscription Agreement with Entrust Datacard, or a Relying Party Agreement with Entrust Datacard, shall in no way be construed to be a present or future waiver of such provisions, nor in any way affect the ability of Entrust Datacard to enforce each and every such provision thereafter. The express waiver by Entrust Datacard of any provision, condition, or requirement of this CPS, a Subscription Agreement with Entrust Datacard, or a Relying Party Agreement with Entrust Datacard shall not constitute a waiver of any future obligation to comply with such provision, condition, or requirement. The failure of an independent third-party RA or Reseller operating under a CA to enforce, at any time, any of the provisions of a this CPS, any Subscription Agreement with such RA, or any Relying Party Agreement with such RA or the failure to require by such RA, at any time, performance by any Applicant, Subscriber, Relying Party or any other person, entity, or organization of this CPS, any Subscription Agreement with such RA, or any Relying Party Agreement with such RA shall in no way be construed to be a present or future waiver of such provisions, nor in any way affect the ability of such RA to enforce each and every such provision thereafter. The express waiver by a RA of any provision, condition, or requirement of a Subscription Agreement with such RA or a Relying Party Agreement with such RA shall not constitute a waiver of any future obligation to comply with such provision, condition, or requirement.

9.17.4 Interpretation

All references in this CPS to "section" or "§" refer to the sections of this CPS unless otherwise stated. As used in this CPS, neutral pronouns and any variations thereof shall be deemed to include the feminine and masculine and all terms used in the singular shall be deemed to include the plural, and vice versa, as the context may require. The words "hereof", "herein", and "hereunder" and other words of similar import refer to this CPS as a whole, as the same may from time to time be amended or supplemented, and not to

any subdivision contained in this CPS. The word “including” when used herein is not intended to be exclusive and means “including, without limitation”.

Appendix A – Certificate Profiles

Root Certificate

Root Certificate Field	Critical Extension	Content
Issuer		Must match subject
Subject		Must contain countryName, organizationName and commonName
Extension: subjectKeyIdentifier	Not critical	160-bit SHA-1 hash of subjectPublicKey per RFC 5280
Extension: basicConstraints	Critical	cA is TRUE; pathLenConstraint is not present
Extension: keyUsage	Critical	keyCertsign and cRLSign bits are set

Subordinate CA Certificate

Field	Critical Extension	Content
Validity: notAfter		Not later than the notAfter of the signing certificate
Subject		Must contain countryName, organizationName and commonName and may contain organizationIdentifier
Extension: subjectKeyIdentifier	Not critical	160-bit SHA-1 hash of subjectPublicKey per RFC 5280
Extension: authorityKeyIdentifier	Not critical	Matches subjectKeyIdentifier of signing certificate
Extension: certificatePolicies	Not critical	Must contain at least one set of policyInformation containing at least a policyIdentifier
Extension: basicConstraints	Critical	cA is TRUE
Extension: keyUsage	Critical	keyCertsign and cRLSign bits are set
Extension: extKeyUsage	Not critical	Must be present when associated with public trust roots
Extension: authorityInfoAccess	Not critical	Must contain one AccessDescription with an accessMethod of caIssuers and a Location of type uniformResourceIdentifier and one AccessDescription with an accessMethod of ocsp and a Location of type uniformResourceIdentifier
Extension: cRLDistributionPoints	Not critical	Must have at least one DistributionPoint containing a fullName of type uniformResourceIdentifier

eIDAS Qualified Signature Certificate

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) = <randomly generated> 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
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
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

eIDAS Qualified Seal Certificate

Field		**Value**
Attributes		
Version		V3
Serial Number		Unique number to PKI domain
Issuer Signature Algorithm		sha-256
Issuer DN		CN = Entrust Certification Authority – ES QSeal1 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> 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= 2.16.840.1.114028.10.1.12.1 [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 (Optional)
Basic Constraints	No	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/esqseal1-g4.cer
CRL Distribution Points	No	uri: http://crl.entrust.net/esqseal1ca.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= http://www.entrust.net/rpa Language = en

PSD2 Qualified Seal Certificate

Field		**Value**
Attributes		
Version		V3
Serial Number		Unique number to PKI domain
Issuer Signature Algorithm		sha-256
Issuer DN		CN = Entrust Certification Authority – ES QSeal1 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> 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		[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/esqseal1-g4.cer
CRL Distribution Points	No	uri: http://crl.entrust.net/esqseal1ca.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= http://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 Web Authentication Certificate

Field		**Value**
Attributes		
Version		V3
Serial Number		Unique number to PKI domain
Issuer Signature Algorithm		sha-256
Issuer DN		CN = Entrust Certification Authority – QTSP1 OrganizationIdentifier = VATES-B81188047 O = Entrust Datacard Europe, 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) 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		Minimum 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
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= 2.16.840.1.114028.10.1.12.4 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.entrust.net/rpa [2] Certificate Policy: Policy Identifier=0.4.0.194112.1.4 [3] Certificate Policy: Policy Identifier=2.16.840.1.114028.10.1.2 [4] Certificate Policy: Policy Identifier=2.23.140.1.1
Basic Constraints	No	Subject Type = End Entity

		Path Length Constraint = None
Authority Information Access		• 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/qtsp1-chain256.cer
CRL Distribution Points	No	uri: http://crl.entrust.net/qtsp1.crl
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= http://www.entrust.net/CPS Language = en

PSD2 Qualified Web Authentication Certificate

Field		**Value**
Attributes		
Version		V3
Serial Number		Unique number to PKI domain
Issuer Signature Algorithm		sha-256
Issuer DN		CN = Entrust Certification Authority – QTSP1 OrganizationIdentifier = VATES-B81188047 O = Entrust Datacard Europe, 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		Minimum 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
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= 2.16.840.1.114028.10.1.12.6 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.entrust.net/rpa [2] Certificate Policy: Policy Identifier=0.4.0.194112.1.4 [3] Certificate Policy Policy identifier=2.16.840.1.114028.10.1.2 [4] Certificate Policy:

		Policy Identifier=2.23.140.1.1 [5] Certificate Policy Policy Identifier=0.4.0.19495.3.1
Basic Constraints	No	Subject Type = End Entity Path Length Constraint = None
Authority Information Access		• 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/qtsp1-chain256.cer
CRL Distribution Points	No	uri: http://crl.entrust.net/qtsp1.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= http://www.entrust.net/CPS Language = en
id-etsi-psd2-qcStatement	No	Id-etsi-psd2-qcStatement (0.4.0.19495.2) PSD2QcType ::= SEQUENCE{ rolesOfPSP RolesOfPSP, nCAName NCAName, nCAId NCAId }

Appendix B – Registration Schemes

The following Registration Schemes are currently recognized as valid under these guidelines:

NTR: The information carried in this field shall be the same as held in Subject registration number as specified in §3.2.2.1 and the country code used in the registration scheme identifier shall match that of the subject's jurisdiction as specified in §3.2.2.1.

Where the Subject jurisdiction of incorporation or registration field in §3.2.2.1 includes more than the country code, the additional locality information shall be included as specified in §3.2.2.10.

VAT: Reference allocated by the national tax authorities to a legal entity. This information shall be validated using information provided by the national tax authority against the organization as identified by the Subject organization name and Subject registration number within the context of the Subject's jurisdiction as specified in §3.2.2.1.

PSD: Authorization number as specified in ETSI TS 119 495 clause 4.4 allocated to a payment service provider and containing the information as specified in ETSI TS 119 495 clause 5.2.1. This information shall be obtained directly from the national competent authority register for payment services or from an information source approved by a government agency, regulatory body, or legislation for this purpose. This information shall be validated by being matched directly or indirectly (for example, by matching a globally unique registration number) against the organization as identified by the Subject organization name and Subject registration number within the context of the subject's jurisdiction as specified in §3.2.2.1. The stated address of the organization combined with the organization name shall not be the only information used to disambiguate the organization.