



# **ENTRUST CERTIFICATE SERVICES**

## ***Certification Practice Statement***

### ***For Private Trust Certificates***

Version: 2.0  
July 25, 2019

© 2019 Entrust Datacard Limited. All rights reserved.

## Revision History

Issue	Date	Changes in this Revision
1.0	December 1, 2013	Initial version.
1.1	March 4, 2014	Addition of mobile device certificates and change to Loss Limitations
1.2	February 17, 2015	Correct CA public key distribution and add new SHA-2 issuing CA
1.3	February 12, 2016	Update for Subscriber Obligations and HSM criteria
1.4	March 7, 2016	Update to allow SHA-1 signed certificates and update approved key sizes
1.5	September 19, 2016	Update to remove restriction for SHA-1 signed SSL certificates
1.6	February 1, 2017	Changes to Definitions, Disclaimers, Loss Limitations and Conflict of Provisions
1.7	July 14, 2017	Update for domain validation methods, inclusion of IP address validation methods and no stipulation for CAA and CT
1.8	February 1, 2018	Added requirements for Shared and Dedicated CAs for Private SSL
2.0	June 30, 2019	Upgrade CPS to RFC 3647 format

## TABLE OF CONTENTS

<b>1. Introduction</b>	<b>1</b>
1.1 Overview	1
1.2 Document Name and Identification	1
1.3 PKI Participants	1
1.3.1 Certification Authorities	1
1.3.2 Registration Authorities	2
1.3.3 Subscribers	2
1.3.4 Relying Parties	2
1.3.5 Other Participants	2
1.4 Certificate Usage	2
1.4.1 Appropriate Certificate Uses	2
1.4.2 Prohibited Certificate Uses	3
1.5 Policy Administration	3
1.5.1 Organization Administering the Document	3
1.5.2 Contact Person	3
1.5.3 Person Determining CPS Suitability for the Policy	3
1.5.4 CPS Approval Procedures	3
1.6 Definitions and Acronyms	3
1.6.1 Definitions	3
1.6.2 Acronyms	6
<b>2. Publication and Repository Responsibilities</b>	<b>8</b>
2.1 Repositories	8
2.2 Publication of Certification Information	8
2.3 Time or Frequency of Publications	8
2.4 Access Controls on Repositories	8
<b>3. Identification and Authentication</b>	<b>9</b>
3.1 Naming	9
3.1.1 Types of Names	9
3.1.2 Need for Names to be Meaningful	9
3.1.3 Anonymity or Pseudonymity of Subscribers	10
3.1.4 Rules for Interpreting Various Name Forms	10
3.1.5 Uniqueness of Names	10
3.1.6 Recognition, Authentication, and Role of Trademarks	10
3.2 Initial Identity Validation	11
3.2.1 Method to Prove Possession of Private Key	11
3.2.2 Authentication of Organization Identity	11
3.2.2.2 DBA/Tradename	11
3.2.2.3 Verification of Country	11
3.2.2.4 Validation of Domain Authorization or Control	12
3.2.2.5 Authentication of an IP Address	12
3.2.2.6 Wildcard Validation	12
3.2.2.7 Data Source Accuracy	13
3.2.2.8 CAA Records	13
3.2.2.9 Authentication of Email Address	13
3.2.2.10 Authentication of Registered Trademark	13

- 3.2.3 Authentication of Individual Identity..... 13
- 3.2.4 Non-verified Subscriber Information..... 13
- 3.2.5 Validation of Authority..... 13
- 3.2.6 Criteria for Interpretation..... 13
- 3.3 Identification and Authentication for Re-key Requests..... 14**
  - 3.3.1 Identification and Authentication for Routine Re-key ..... 14
  - 3.3.2 Identification and Authentication for Re-key after Revocation..... 14
- 3.4 Identification and Authentication for Revocation Requests..... 14**
- 4. Certificate Life-Cycle Operational Requirements.....15**
  - 4.1 Certificate Application..... 15**
    - 4.1.1 Who Can Submit a Certificate Application..... 15
    - 4.1.2 Enrollment Process and Responsibilities..... 15
  - 4.2 Certificate Application Processing..... 15**
    - 4.2.1 Performing Identification and Authentication Functions ..... 15
    - 4.2.2 Approval or Rejection of Certificate Applications ..... 16
    - 4.2.3 Time to Process Certificate Applications ..... 16
  - 4.3 Certificate Issuance ..... 16**
    - 4.3.1 CA Actions During Certificate Issuance ..... 16
    - 4.3.2 Notification to Subscriber by the CA of Issuance of Certificate..... 16
  - 4.4 Certificate Acceptance..... 16**
    - 4.4.1 Conduct Constituting Certificate Acceptance..... 16
    - 4.4.2 Publication of the Certificate by the CA..... 16
    - 4.4.3 Notification of Certificate Issuance by the CA to Other Entities..... 16
  - 4.5 Key Pair and Certificate Usage..... 16**
    - 4.5.1 Subscriber Private Key and Certificate Usage ..... 16
    - 4.5.2 Relying Party Public Key and Certificate Usage..... 16
  - 4.6 Certificate Renewal ..... 16**
    - 4.6.1 Circumstance for Certificate Renewal..... 16
    - 4.6.2 Who May Request Renewal..... 17
    - 4.6.3 Processing Certificate Renewal Requests..... 17
    - 4.6.4 Notification of New Certificate Issuance to Subscriber..... 17
    - 4.6.5 Conduct Constituting Acceptance of a Renewal Certificate..... 17
    - 4.6.6 Publication of the Renewal Certificate by the CA..... 17
    - 4.6.7 Notification of Certificate Issuance by the CA to Other Entities..... 17
  - 4.7 Certificate Re-key..... 17**
    - 4.7.1 Circumstance for Certificate Re-key ..... 17
    - 4.7.2 Who May Request Certification of a New Public Key..... 17
    - 4.7.3 Processing Certificate Re-keying Requests..... 17
    - 4.7.4 Notification of New Certificate Issuance to Subscriber..... 17
    - 4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate..... 17
    - 4.7.6 Publication of the Re-keyed Certificate by the CA..... 17
    - 4.7.7 Notification of Certificate Issuance by the CA to Other Entities..... 17
  - 4.8 Certificate Modification..... 18**
    - 4.8.1 Circumstance for Certificate Modification..... 18
    - 4.8.2 Who May Request Certificate Modification ..... 18
    - 4.8.3 Processing Certificate Modification Requests ..... 18
    - 4.8.4 Notification of New Certificate Issuance to Subscriber..... 18
    - 4.8.5 Conduct Constituting Acceptance of Modified Certificate..... 18
    - 4.8.6 Publication of the Modified Certificate by the CA..... 18

4.8.7 Notification of Certificate Issuance by the CA to Other Entities..... 18

**4.9 Certificate Revocation and Suspension..... 18**

4.9.1 Circumstances for Revocation..... 18

4.9.1.1 Reasons for Revoking a Subscriber Certificate..... 18

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate ..... 19

4.9.2 Who Can Request Revocation..... 19

4.9.3 Procedure for Revocation Request..... 20

4.9.4 Revocation Request Grace Period..... 20

4.9.5 Time within Which CA Must Process the Revocation Request..... 20

4.9.6 Revocation Checking Requirement for Relying Parties ..... 20

4.9.7 CRL Issuance Frequency ..... 20

4.9.8 Maximum Latency for CRLs..... 20

4.9.9 On-line Revocation/Status Checking Availability..... 21

4.9.10 On-line Revocation Checking Requirements ..... 21

4.9.11 Other Forms of revocation Advertisements Available ..... 21

4.9.12 Special Requirements Re Key Compromise ..... 21

4.9.13 Circumstances for Suspension..... 21

4.9.14 Who Can Request Suspension..... 21

4.9.15 Procedure for Suspension Request..... 21

4.9.16 Limits on Suspension Period..... 21

**4.10 Certificate Status Services..... 21**

4.10.1 Operational Characteristics..... 21

4.10.2 Service Availability..... 22

4.10.3 Optional Features ..... 22

**4.11 End of Subscription..... 22**

**4.12 Key Escrow and Recovery..... 22**

4.12.1 Key Escrow and Recovery Policy Practices..... 22

4.12.2 Session Key Encapsulation and Recovery Policy and Practices..... 22

**5. Facility, Management, and Operational Controls ..... 23**

**5.1 Physical Security Controls ..... 23**

5.1.1 Site Location and Construction..... 23

5.1.2 Physical Access..... 23

5.1.3 Power and Air Conditioning..... 23

5.1.4 Water Exposures ..... 23

5.1.5 Fire Prevention and Protection..... 23

5.1.6 Media Storage..... 23

5.1.7 Waste Disposal..... 23

5.1.8 Off-site Backup ..... 23

**5.2 Procedural Controls ..... 23**

5.2.1 Trusted Roles..... 23

5.2.2 Number of Persons Required per Task..... 24

5.2.3 Identification and Authentication for Each Role..... 24

5.2.4 Roles Requiring Separation of Duties..... 24

**5.3 Personnel Controls..... 24**

5.3.1 Qualifications, Experience and Clearance Requirements..... 24

5.3.2 Background Check Procedures ..... 24

5.3.3 Training Requirements ..... 24

5.3.4 Retraining Frequency and Requirements..... 24

5.3.5 Job Rotation Frequency and Sequence..... 24

5.3.6 Sanctions for Unauthorized Actions ..... 24

5.3.7 Independent Contractor Requirements ..... 24

5.3.8 Documentation Supplied to Personnel.....25

**5.4 Audit Logging Procedures..... 25**

5.4.1 Types of Events Recorded.....25

5.4.2 Frequency of Processing Log.....25

5.4.3 Retention Period for Audit Log.....25

5.4.4 Protection of Audit Log.....25

5.4.5 Audit Log Backup Procedures .....26

5.4.6 Audit Collection System.....26

5.4.7 Notification to Event-causing Subject .....26

5.4.8 Vulnerability Assessments .....26

**5.5 Records Archival..... 26**

5.5.1 Types of Records Archived.....26

5.5.2 Retention Period of for Archive.....26

5.5.3 Protection of Archive.....26

5.5.4 Archive Backup Procedures .....26

5.5.5 Requirements for Time-stamping of Records .....26

5.5.6 Archive Collection System.....26

5.5.7 Procedures to Obtain and Verify Archive Information .....27

**5.6 Key Changeover..... 27**

**5.7 Compromise and Disaster Recovery..... 27**

5.7.1 Incident and Compromise Handling Procedures.....27

5.7.2 Computing Resources, Software and/or Data are Corrupted .....27

5.7.3 Entity Private Key Compromise Procedures.....27

5.7.4 Business Continuity Capabilities after a Disaster.....27

**5.8 CA or RA Termination..... 28**

**6. Technical Security Controls.....29**

**6.1 Key Pair Generation and Installation..... 29**

6.1.1 Key Pair Generation.....29

6.1.2 Private Key Delivery to Subscriber .....29

6.1.3 Public Key Delivery to Certificate Issuer.....29

6.1.4 CA Public Key Delivery to Relying Parties .....30

6.1.5 Key Sizes .....30

6.1.6 Public Key Parameters Generation and Quality Checking.....30

6.1.7 Key Usage Purposes.....30

**6.2 Private Key Protection and Cryptographic Module Engineering Controls ..... 30**

6.2.1 Cryptographic Module Standards and Controls.....30

6.2.2 Private Key (N out of M) Multi-person Control.....30

6.2.3 Private Key Escrow.....30

6.2.4 Private Key Backup .....31

6.2.5 Private Key Archival.....31

6.2.6 Private Key Transfer into or from Cryptographic Module.....31

6.2.7 Private Key Storage on Cryptographic Module.....31

6.2.8 Method of Activating Private Key .....31

6.2.9 Method of Deactivating Private Key .....31

6.2.10 Method of Destroying Private Key .....32

6.2.11 Cryptographic Module Rating.....32

**6.3 Other Aspects of Key Pair Management..... 32**

6.3.1 Public Key Archival.....32

6.3.2 Certificate Operational Periods and Key Pair Usage Periods .....32

**6.4 Activation Data..... 32**

6.4.1 Activation Data Generation and Installation..... 32

6.4.2 Activation Data Protection ..... 32

6.4.3 Other Aspects of Activation Data..... 32

**6.5 Computer Security Controls..... 32**

6.5.1 Specific Computer Security Technical Requirements ..... 32

6.5.2 Computer Security Rating ..... 33

**6.6 Life Cycle Security Controls..... 33**

6.6.1 System Development Controls ..... 33

6.6.2 Security Management Controls..... 33

6.6.3 Life Cycle Security Controls ..... 33

**6.7 Network Security Controls Security Controls ..... 33**

**6.8 Time-stamping..... 33**

**7. Certificate, CRL and OCSP Profiles ..... 34**

**7.1 Certificate Profile..... 34**

7.1.1 Version Number ..... 34

7.1.2 Certificate Extensions ..... 34

7.1.3 Algorithm Object Identifiers ..... 35

7.1.4 Name Forms ..... 35

7.1.5 Name Constraints ..... 36

7.1.6 Certificate Policy Object Identifier..... 36

7.1.7 Usage of Policy Constraints Extension..... 36

7.1.8 Policy Qualifiers Syntax and Semantics..... 36

7.1.9 Processing Semantics for the Critical Certificate Policies Extension..... 36

**7.2 CRL Profile ..... 36**

7.2.1 Version Number..... 36

7.2.2 CRL and CRL Entry Extensions ..... 36

**7.3 OCSP Profile ..... 36**

7.3.1 Version Number..... 37

7.3.2 OCSP Extensions ..... 37

**8. Compliance Audit and Other Assessment..... 38**

**8.1 Frequency or Circumstances of Assessment..... 38**

**8.2 Identity/Qualifications of Assessor..... 38**

**8.3 Assessor’s Relationship to Assessed Entity ..... 38**

**8.4 Topics Covered by Assessment ..... 38**

**8.5 Actions Taken as a Result of Deficiency..... 38**

**8.6 Communication of Results ..... 38**

**8.7 Self-audits..... 38**

**9. Other Business and Legal Matters..... 39**

**9.1 Fees..... 39**

9.1.1 Certificate Issuance or Renewal Fees ..... 39

9.1.2 Certificate Access Fees ..... 39

9.1.3 Revocation or Status Information Access Fees..... 39

9.1.4 Fees for Other Services..... 39

9.1.5 Refund Policy..... 39

<b>9.2</b>	<b>Financial Responsibility.....</b>	<b>39</b>
9.2.1	Insurance Coverage.....	39
9.2.2	Other Assets.....	39
9.2.3	Insurance or Warranty Coverage for End-entities .....	39
<b>9.3</b>	<b>Confidentiality of Business Information .....</b>	<b>40</b>
9.3.1	Scope of Confidential Information .....	40
9.3.2	Information not with the Scope of Confidential Information.....	40
9.3.3	Responsibility to Protect Confidential Information .....	40
<b>9.4</b>	<b>Privacy or Personal Information.....</b>	<b>40</b>
9.4.1	Privacy Plan.....	40
9.4.2	Information Treated as Private.....	40
9.4.3	Information not Deemed Private.....	41
9.4.4	Responsibility to Protect Private Information .....	41
9.4.5	Notice and Consent to Use Private Information.....	41
9.4.6	Disclosure Pursuant to Judicial or Administrative Process .....	41
9.4.7	Other Information Disclosure Circumstances .....	41
<b>9.5</b>	<b>Intellectual Property Rights .....</b>	<b>41</b>
<b>9.6</b>	<b>Representation and Warranties.....</b>	<b>42</b>
9.6.1	CA Representations and Warranties .....	42
9.6.2	RA Representations and Warranties .....	43
9.6.3	Subscriber representations and Warranties.....	43
9.6.4	Relying Parties Representations and Warranties .....	45
9.6.5	Representations and Warranties of Other Participants .....	46
<b>9.7</b>	<b>Disclaimers of Warranties.....</b>	<b>46</b>
<b>9.8</b>	<b>Limitations of Liability .....</b>	<b>47</b>
<b>9.9</b>	<b>Indemnities.....</b>	<b>49</b>
9.9.1	Indemnification by CAs.....	49
9.9.2	Indemnification for Relying Parties.....	49
9.9.3	Indemnification by Subscribers.....	49
<b>9.10</b>	<b>Term and Termination .....</b>	<b>50</b>
9.10.1	Term.....	50
9.10.2	Termination .....	50
9.10.3	Effect of Termination and Survival .....	50
<b>9.11</b>	<b>Individual Notices and Communications with Participants .....</b>	<b>50</b>
<b>9.12</b>	<b>Amendments.....</b>	<b>50</b>
9.12.1	Procedure for Amendment.....	50
9.12.2	Notification Mechanism and Period .....	50
9.12.3	Circumstances Under which OID must be Changed .....	51
<b>9.13</b>	<b>Dispute Resolution Provisions .....</b>	<b>51</b>
<b>9.14</b>	<b>Governing Law .....</b>	<b>51</b>
<b>9.15</b>	<b>Compliance with Applicable Law .....</b>	<b>51</b>
<b>9.16</b>	<b>Miscellaneous Provisions.....</b>	<b>52</b>
9.16.1	Entire Agreement .....	52
9.16.2	Assignment.....	52
9.16.3	Severability.....	52
9.16.4	Enforcement.....	52
9.16.5	Force Majeure.....	52



<b>9.17</b>	<b>Other Provisions .....</b>	<b>53</b>
9.17.1	Conflict of Provisions .....	53
9.17.2	Fiduciary Relationships .....	53
9.17.3	Waiver.....	53
9.17.4	Interpretation .....	53
<b><i>Appendix A – Subordinate CA Certificates.....</i></b>		<b>54</b>

## 1. Introduction

Entrust Datacard Limited (“Entrust Datacard”) uses its award winning 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:

- Private SSL Certificate(s)
- Mobile Device Certificate(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.

### 1.2 Document Name and Identification

This document is called the Entrust Certificate Services Certification Practice Statement for Private Trust Certificates.

### 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 Shared CAs. This CPS also covers all Certificates issued and signed by Dedicated CAs; however, the Dedicated CAs are not listed for privacy reasons.

#### Root

CN: Entrust Root Certification Authority - G3

Subject Key Identifier: b5 75 01 ee 41 c7 ca 7a 3f f2 fc 5a 56 c7 76 06 0b 06 6c 66

Thumbprint (SHA-1): ae 85 69 d9 4f 4a b1 c4 64 ad 9b 7c fd 78 40 b0 e3 9d af 66

#### Subordinate CA(s)

CN: Entrust Certification Authority - L1G

Subject Key Identifier: 33 e9 d1 9c af 01 53 c3 fd 84 c3 a9 f8 71 b2 3f 7e fc 63 bb

CN: Entrust Certification Authority - L1H  
Subject Key identifier: 90 91 5c fb 52 8f f4 fb bb 37 3e 03 ff 39 63 1e a0 69 1b 81

CN: Entrust Certification Authority - L1R  
Subject Key identifier: d4 36 ff 0e 3c 50 fd 50 71 ca 1c 71 c1 8f f7 be a7 ef 85 34

### 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.

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.

### 1.3.4 Relying Parties

A Relying Party is a person, entity, or organization that relies on or uses a Certificate and/or any other information provided in a Repository to verify the identity and Public Key of a Subscriber and/or use such Public Key to send or receive encrypted communications to or from a Subscriber.

### 1.3.5 Other Participants

No stipulation.

## 1.4 Certificate Usage

Private SSL Certificates are issued to organizations to allow servers, devices and individuals to identify themselves to entities and services of the organization for authorization.

Private SSL Certificates may be issued from a Shared CA to multiple related or unrelated Subscribers. Certificates issued from a Shared CA may unintentionally be trusted by unrelated Subscribers.

Private SSL Certificates may be used from a Dedicated CA to a single Subscriber.

There may be policy differences between a Shared CA and a Dedicated CA, which will be indicated in this CPS.

### 1.4.1 Appropriate Certificate Uses

This CPS is applicable to the following Certificate Types.

#### Private SSL Certificates

Private SSL Certificates are intended for use in establishing web-based data communication conduits via TLS/SSL protocols. Private SSL Certificates conform to the requirements of the ITU-T X.509 v3 standard. The primary purpose of a Private SSL Certificate is to facilitate the exchange of encryption keys in order to enable the encrypted communication of information over the Internet between the user of an Internet browser and a secure server.

### Mobile Device Certificates

Mobile Device Certificates are intended to allow the identification of mobile devices. Mobile Device Certificates conform to the requirements of the ITU-T X.509 v3 standard. The primary purpose of a Mobile Device Certificate is to provide a trusted identity to a service to obtain authorization to use that service.

#### **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.

### **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 Limited.

#### **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](mailto:ecs.support@entrustdatacard.com)

Security issues, such as Certificate misuse, vulnerability reports or external reports of key compromise, may also be reported at <https://www.entrust.net/ev/misuse.cfm> or emailed to [evssl@entrustdatacard.com](mailto:evssl@entrustdatacard.com).

#### **1.5.3 Person Determining CPS Suitability for the Policy**

The Policy Authority determines the suitability and applicability of this CPS.

#### **1.5.4 CPS Approval Procedures**

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

### **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.

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

**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 Ottawa, Ontario, Canada.

**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; Private SSL Certificate and/or Mobile Device Certificates.

**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 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.

**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.

**Cross Certificate(s):** shall mean a Certificate(s) 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.

**Dedicated CA:** means a CA which is dedicated to one Subscriber. The CA hierarchy shall be trusted by a Root CA which is also dedicated to the same Subscriber.

**Domain 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 Limited.

**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.

**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.

**IP Address:** 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.

**Mobile Device Certificate:** means a Certificate issued by a Certification Authority for use to identify a mobile device.

**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.

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

**Private SSL Certificate:** means an SSL Certificate issued by a Certification Authority for use on secure servers. The Certification Authority root certificate is not distributed to any ASV for public trust. The Private SSL Certificate may contain domain names which are not publicly registered.

**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.

**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.

**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.

**Shared CA:** means a CA which issues Certificates to one or more Subscribers.

**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. and/or Third Party Subordinate CAs.

**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.

**Third Party Subordinate CA:** means a certification authority owned by a third party which has been issued a Subordinate CA Certificate.

**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**

ASV	Application Software Vendor
CA	Certification Authority
CAA	Certification Authority Authorization
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DBA	Doing Business As
DN	Distinguished Name

---

DNS	Domain Name System
ECC	Elliptic Curve Cryptography
EKU	Extended Key Usage
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
NIST	(US Government) National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PA	Policy Authority
PIN	Personal Identification Number
PKI	Public-Key Infrastructure
RA	Registration Authority
RFC	Request for Comment
RSA	Rivest–Shamir–Adleman cryptosystem
SAN	Subject Alternative Name
SSL	Secure Sockets Layer
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)
TLS	Transport Layer Security
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>.

### **2.2 Publication of Certification Information**

The CA publishes its CPS, CA Certificates, Subscription Agreements, 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 a 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.

##### 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.

###### Private SSL 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 Private SSL 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 fully qualified hostname or path used in the DNS of the secure server on which the Applicant is intending to install the Private SSL Certificate;
- (v) “State” (ST), which is the state or province of the organization’s place of business, if applicable; and
- (vi) “Subject Alternative Name” (SAN), which is the fully qualified hostname or path used in the DNS of the secure server on which the Applicant is intending to install the Private SSL Certificate. There may be multiple SANs in each Private SSL Certificate.

###### Mobile Device Certificates

- (i) “Country Name” (C) which is the two-letter ISO 3166 code for the country in which the Applicant is located;
- (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 a unique alpha-numeric identifier, Subscriber name, or a unique alpha-numeric identifier plus Subscriber name which has been approved by the Subscriber administration contact; and
- (v) Optionally, “Subject Alternative Name” (SAN) which is the email address of the Subscriber.

##### 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.

### 3.13 Anonymity or Pseudonymity of Subscribers

No stipulation.

### 3.14 Rules for Interpreting Various Name Forms

No stipulation.

### 3.15 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.

### 3.16 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 a 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 a 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**

Private SSL Certificates (Shared CA) and Mobile Device Certificates

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.

Private SSL Certificates (Dedicated CA)

RAs operating under the Dedicated CAs are not required to confirm any organization identities that are submitted by an Applicant or Subscriber.

**3.2.2.2 DBA/Tradename**

No stipulation.

**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**

**3.2.2.4.1 Fully-Qualified Domain Names**

Private SSL Certificates (Shared CA)

RAs operating under the CAs shall use reasonable means to confirm the Applicant or Subscriber has control of the FQDN to be included in the Certificate. The RA shall use one of the following methods as defined in Section 3.2.2.4 of the Baseline Requirements:

- 1) Method not used
- 2) Email, Fax, SMS, or Postal Mail to Domain Contact
- 3) Method not used
- 4) Constructed Email to Domain Contact
- 5) Method not used
- 6) Agreed-Upon Change to Website
- 7) DNS Change
- 8) IP Address
- 9) Method not used
- 10) Method not used
- 11) Method not used
- 12) Method not used
- 13) Email to DNS CAA Contact
- 14) Email to DNS TXT Contact
- 15) Phone with Domain Contact
- 16) Phone Contact with DNS TXT Record Phone Contact
- 17) Phone Contact with DNS CAA Phone Contact

Private SSL Certificates (Dedicated CA)

RAs operating under the Dedicated CAs are not required to confirm the Applicant or Subscriber has control of the FQDN to be included in the Private SSL Certificate.

**3.2.2.4.2 Non-Fully-Qualified Domain Names**

RAs operating under the CAs shall allow non-FQDN to be used.

Private SSL Certificates (Shared CA)

Non-FQDNs must be multi-label name or reserved IP Address. Each non-FQDN shall be reserved for one Subscriber for each CA used to issue Private SSL Certificates.

Private SSL Certificates (Dedicated CA)

Non-FQDNs may be minimum single-label or a reserved IP Address.

**3.2.2.5 Authentication of an IP Address**

Private SSL Certificates may use registered or Reserved IP Addresses.

RAs operating under the CAs shall use one of the methods defined in Section 3.2.2.5 of the Baseline Requirements to confirm the Applicant or Subscriber has control of the registered IP Address to be included in the Certificate.

Private SSL Certificates (Shared CA)

Reserved IP Addresses must be reserved for one Subscriber for each Shared CA used to issue Private SSL Certificates.

**3.2.2.6 Wildcard Validation**

Wildcard validation for an FQDN follows the requirements as defined in Section 3.2.2.6 of the Baseline Requirements.

**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**

No stipulation.

**3.2.2.9 Authentication of Email Address**

No stipulation.

**3.2.2.10 Authentication of Registered Trademark**

No stipulation.

**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.

An individual identity shall be verified by using a legible copy, which discernibly shows the Applicant’s face, of at least one currently valid government-issued photo ID (passport, driver’s license, military ID, national ID, or equivalent document type). The copy shall be inspected for any indication of alteration or falsification.

The Applicant’s address shall be verified using a trusted form of identification such as a government ID, utility bill, or bank or credit card statement. The same government-issued ID that was used to verify the Applicant’s name may be relied upon.

The request shall be verified by contacting the Applicant using a reliable method of communication.

**3.2.4 Non-verified Subscriber Information**

Non-verified Subscriber information may be organization identities per §3.2.2.1, non-FQDNs per §3.2.2.4.2 or Reserved IP Addresses per §3.2.2.5.

**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.

**3.2.6 Criteria for Interpretation**

No stipulation.

### **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.

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.

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 by email once a Certificate has been issued by the CA.

#### 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.

#### 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.

## 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, or may reuse previous validations themselves provided the data or documentation was obtained from a source specified under §3.2 or completed the validation itself no more than 825 days after such data or documentation was validated.



**4.2.2 Approval or Rejection of Certificate Applications**

No stipulation.

**4.2.3 Time to Process Certificate Applications**

No stipulation.

**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 a Certificate in accordance with the Certificate profile described in §7.

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.

**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.

**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**

No stipulation.

**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.

Certificates may be reissued 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 any of the events listed in this section have occurred.

The CA may revoke a Certificate 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.
- (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 may 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 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 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 a 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 Certificate Problem Reports 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 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.

**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**

No stipulation.

**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 with 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 Private SSL Certificates Mobile Device Certificates shall be issued at least once every seven days. The next CRL update is 7 days from the last update.

**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 Private SSL Certificates and Mobile Device Certificates issued to end entities shall be issued at least once every four days. OCSP responses will have a maximum expiration time of ten days.

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.

**4.9.11 Other Forms of revocation Advertisements Available**

No stipulation.

**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.

**4.10 Certificate Status Services**

**4.10.1 Operational Characteristics**

Private SSL Certificates

Revocation entries on a CRL or OCSP response are not removed until after the expiry date of the revoked Certificate.

**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.

**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

### 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 dry wall and wire mesh. The security zone is protected by electronic control access systems, alarmed doors and is monitored via a 24x7 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. Alarms 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.

#### 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 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 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.

The time for the CAs computer systems is synchronized with the service provided by the National Research Council Canada.

**5.4.1 Types of Events Recorded**

The CAs and all RAs operating under a CA record in detail every action taken to process a Certificate request and to issue a Certificate, including all information generated or received in connection with a 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. Firewall and router activities; and
  - n. Entries to and exits from the CA facility.
- (iv) Log entries include the following elements:
  - o. Date and time of entry;
  - p. Identity of the person making the journal entry; and
  - q. 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**

No stipulation.

**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.

**5.7 Compromise and Disaster Recovery**

**5.7.1 Incident and Compromise Handling Procedures**

CAs have a disaster recovery plan to provide for timely recovery of services in the event of a system outage. The disaster recovery plan addresses 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 24 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.

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 and ASVs shall be informed as soon as practicable of such a Compromise and information shall be posted in the Repository.

**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 that a CA ceases operation, all Certificates issued by such CA shall be revoked and the CRL lifetime will be set to a period that meets any Entrust Datacard obligations.

## **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).

CA Key Pairs must be generated on a cryptographic module that meets or exceeds the requirements as defined in §6.2.11.

#### **6.12 Private Key Delivery to Subscriber**

CAs do not generate, archive or deliver the Key Pair on behalf of the Subscriber.

#### **6.13 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 Certification Authority Certificate(s) containing the Root CAs Public Key are made available to Subscribers with the Certificate or may be obtained from the Entrust Datacard support team. The Subordinate CA Certificate is provided to the Subscriber with the Certificate.

The Subordinate CA Certificate for the CA is provided to the Relying Parties by the Subscriber.

#### 6.1.5 Key Sizes

For CA, Private SSL Certificates and Mobile Device Certificates, the key sizes supported are:

- (i) RSA 2048-bit, 3072 bit and 4096-bit
- (ii) Elliptic curve cryptography (ECC) NIST P-384

#### 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.

For ECC public keys, CAs shall confirm the validity of all keys using either the ECC Full Public Key Validation Routine or the ECC Partial Public Key Validation Routine.

#### 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 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.

#### 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 controls 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.

**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.

Private SSL Certificates

Private SSL Certificates contain a validity period of up to, but no more than, 39 months.

Mobile Device Certificates

Mobile Device Certificates contain a validity period of up to, but no more than, 39 months.

**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.

**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 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.

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, Subordinate CA, and end entity Certificates are described in 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**

Certificate extensions are as set as stipulated in IETF RFC 5280.

**7.1.2.1 Root CA Certificate**

Extension	Critical	Description
basicConstraints	Yes	CA field is set to be true pathLenConstraint field not present
keyUsage	Yes	Bit positions for keyCertSign and cRLSign are set
certificatePolicies		Not present
extendedKeyUsage		Not present

**7.1.2.2 Subordinate CA Certificate**

Extension	Critical	Description
basicConstraints	Yes	CA field is set to be true pathLenConstraint field not present
keyUsage	Yes	Bit positions for keyCertSign and cRLSign are set
certificatePolicies	No	Policy Identifier, Qualifier ID of CPS and URI for CPS are required
extendedKeyUsage	No	As applicable from the following: None present Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)
cRLDistributionPoints	No	HTTP URL of the CA's CRL service
authorityInformationAccess	No	HTTP URL of the Issuing CA's OCSP responder

**7.1.2.3 Subscriber Certificate**

Extension	Critical	Description
basicConstraints		Not present
keyUsage	Yes	As applicable from the following: Digital Signature Key Encipherment
certificatePolicies	No	Policy Identifier, Qualifier ID of CPS and URI for CPS are required
extendedKeyUsage	No	As applicable from the following: None present Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)
cRLDistributionPoints	No	HTTP URL of the CA’s CRL service
authorityInformationAccess	No	HTTP URL of the Issuing CA’s OCSP responder HTTP URL of the Issuing CA’s certificate

**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**

No stipulation.

**7.1.3 Algorithm Object Identifiers**

Algorithm object identifiers are as specified in IETF RFC 3279 and RFC 4005.

Private SSL Certificates

SHA-1 or SHA-256 hash algorithm may be used.

Mobile Device Certificates

SHA-256 hash algorithm shall be used.

**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**

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.

**7.1.4.3 Subject Information – Root Certificates and Subordinate CA Certificates**

No stipulation.

**7.1.5 Name Constraints**

No stipulation.

**7.1.6 Certificate Policy Object Identifier**

**7.1.6.1 Reserved Certificate Policy Identifiers**

No stipulation.

**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 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 of the following certificate policy identifiers :

Private SSL Certificates (Shared CA):	<b>2.16.840.1.114028.10.1.9.1</b>
Private SSL Certificates (Dedicated CA):	<b>2.16.840.1.114028.10.1.9.5</b>
Mobile Device Certificates:	<b>2.16.840.1.114028.10.1.9.4</b>

**7.1.7 Usage of Policy Constraints Extension**

No stipulation.

**7.1.8 Policy Qualifiers Syntax and Semantics**

No stipulation.

**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**

Compliance audits will be performed on Shared CAs. Compliance audits may be performed on Dedicated CAs.

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; and
- iv. Bound by law, government regulation, or professional code of ethics.

### **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; and
- ii. WebTrust Program for Certification Authorities;

### **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.

### **8.7 Self-audits**

No stipulation.

## **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 a 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 a 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 a 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 acquirors, 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 Privacy Plan**

Entrust Datacard follows the Privacy Policy available at [www.entrustdatacard.com](http://www.entrustdatacard.com) when handling personal information.

#### **9.4.2 Information Treated as Private**

Entrust Datacard treats all personal information about an individual that is not publicly available in the contents of a Certificate, CRL or OCSP as personal information in accordance with the Privacy Policy.

#### **9.4.3 Information not Deemed Private**

Subject to applicable law, Certificates, CRLs, and OCSP and the personal or corporate information appearing in them are not considered personal or private information.

#### **9.4.4 Responsibility to Protect Private Information**

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

#### **9.4.5 Notice and Consent to Use Private Information**

Unless otherwise stated in the CPS, Privacy 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 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 a 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 is sued 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 a 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 a 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
- (iii) 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 a 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 a Certificate, (iii) any software whatsoever, or (iv) non-repudiation of any Certificate or any transaction facilitated through the use of a 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 a 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 a 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 a 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 a 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 a Certificate, to use a 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, 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 a 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 a 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 a 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;

#### 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.

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 a 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 a Certificate, 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;
- (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

#### 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 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).

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 a Certificate or any services provided in respect to a 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 a Certificate after the information contained 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 as 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 a Certificate or any information contained in a 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

No stipulation.

### 9.9.2 Indemnification for Relying Parties

RELYING PARTIES 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, 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 A CERTIFICATE BY A RELYING PARTY, (II) RELIANCE BY THE RELYING PARTY ON AN EXPIRED OR REVOKED CERTIFICATE, (III) USE OF A 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 A CERTIFICATE, OR (V) ANY CLAIM OR ALLEGATION THAT THE RELIANCE BY A RELYING PARTY ON A CERTIFICATE OR THE INFORMATION CONTAINED IN A 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, 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 A CERTIFICATE, (II) MODIFICATION MADE BY A SUBSCRIBER TO THE INFORMATION CONTAINED IN A CERTIFICATE, (III) USE OF A 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 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, facsimile, or overnight courier, and shall be effective as follows (i) in the case of facsimile or courier, 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 by facsimile or courier to the last address, email address or facsimile number for the Subscriber on file with Entrust Datacard. In the event of notice by email, the notice shall become effective on the next Business Day. In the event of notice by prepaid receipted mail, facsimile, or overnight courier, notice shall become effective as specified in (i) or (ii), depending on the means of notice utilized.

## **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.

### **9.12.2 Notification Mechanism and Period**

Modifications to the CPS shall be published in the Repository and shall become effective fifteen (15) days after publication in the Repository unless Entrust Datacard withdraws such modified CPS prior to such effective date. In the event that Entrust Datacard makes a significant modification to CPS, the version number of the CPS shall be updated accordingly. 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**

#### **9.13 Dispute Resolution Provisions**

Unless otherwise set out 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 a 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 a Certificate or any services provided in respect to a 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 a Certificate or any service or services provided in respect to a 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 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.

## **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 RA under a CA with which such Applicant, Subscriber, or Relying Party has contracted. 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 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 include 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 – Subordinate CA Certificates**

Entrust Datacard issues Subordinate CA Certificates to Entrust Datacard CAs and third party operated certification authorities.

**Subordinate CAs**

Entrust Datacard operated subordinate CAs are managed in accordance with this CPS or are operated in accordance with their own CP and/or CPS which meets the minimum requirements of this CPS.

**Third Party Subordinate CAs****Registration**

Entrust Datacard specifies requirements to Third Party Subordinate CAs through written agreement. The Third Party Subordinate CAs must make use of a CP and/or CPS which meets the minimum requirements of this CPS.

The generation of the certificate authority key pair for the Third Party Subordinate CAs is to be witnessed by a third party security auditor.

A request for a Subordinate CA Certificate is started by the Third Party Subordinate CAs submitting a CSR. The CSR is authenticated by contacting the authorization contact for the Third Party Subordinate CAs.

**Certificate Renewal**

Subordinate CA Certificates issued to a third party may be renewed through mutual agreement. The Subordinate CA Certificate may be renewed using the original CSR which was submitted for the initial registration. If the renewal is performed with a new CSR, then the CSR is authenticated by contacting the authorization contact of the Third Party Subordinate CAs.

**Certificate Rekey**

Third Party Subordinate CA Certificates issued to a third party are rekeyed using a new CSR. The new CSR is authenticated by the authorization contact of the Third Party Subordinate CAs.

**Certificate Issuance**

The Subordinate CA Certificate issued to a third party is issued in accordance with the Subordinate CA Certificate profile defined in §7.1.

**Certificate Distribution**

The Subordinate CA Certificate issued to a third party may be distributed in accordance with license set out in the written agreement between Entrust Datacard and the Subordinate Third Party CA.

**Certificate Revocation**

Entrust Datacard confirms Third Party Subordinate CA Certificate revocation requests by contacting the authorization contact of the Third Party Subordinate CAs.

In addition to §4.9.1.2, Entrust Datacard may also revoke any Subordinate CA Certificate in accordance with the agreement between Entrust Datacard and the Third Party Subordinate CA.

The revocation status will be provided by CRL and/or OCSP.

**CA Assessment**

Third Party Subordinate CAs are assessed to meet the requirements of the CP and/or CPS on an annual basis using one of the audit criteria specified in §8.4.