ENTRUST CERTIFICATE SERVICES

Certification Practice Statement

Version: 3.9
July 19, 2021

Revision History

Issue	Date	Changes in this Revision
1.0	May 26, 1999	Initial version.
2.0	July 1, 2000	Addition of provisions dealing with subordinate entities (such as third party registration authorities) in the Entrust.net SSL Web Server public key infrastructure. Revision of numerous other terms and conditions.
2.01	May 30, 2001	Minor revisions having no substantive impact.
2.02	January 1, 2002	Minor revisions related to replacement Cross Certificate.
2.03	January 1, 2003	Entrust legal name change.
2.04	August 20, 2003	Minor revisions related to use of certificates on more than one server; permitting use of asterisk in Subject name
2.05	November 28, 2003	Minor revisions to language to handle licensing issues.
2.06	May 14, 2004	Minor revisions to language for export requirements.
2.1	August 1, 2007	Minor revisions to ensure consistency with the CPS for EV SSL Certificates and to add OCSP references.
2.2	August 11, 2008	Minor revisions to terminology to replace references to Entrust SSL Web Server Certificates with Entrust SSL Certificates. Revision to authentication of individuals, routine rekey and key changeover. Other minor revisions having no substantive impact.
2.3	September 8, 2009	Updates for Code Signing and Client Certificates. Added Appendix A with Certificate Profiles. Revisions to add additional application software vendors and relying parties as third party beneficiaries. Deleted Subscriber notice requirements.
2.4	August 16, 2010	Updates for Class 1 and 2 Client Certificates and Document Signing Certificates
2.5	December 1, 2010	Updates for Time-Stamp Certificates and end entity certificate key sizes
2.6	February 28, 2011	Update disaster recovery, time-stamp authority and code signing certificate requirements
2.7	March 1, 2012	Update to restrict use of certificates for MITM transactions or “traffic management”; Update to

		enable Entrust to request additional info from customers
2.8	June 25, 2012	Update for compliance to Baseline Requirements
2.9	May 1, 2013	Update for inclusion of data controls for certificate renewal, Private Key control, and subordinate CA certificates
2.10	December 1, 2013	Support for smartcards and subordinate CA assessment
2.11	March 4, 2014	Change to Loss Limitations
2.12	April 6, 2015	Updated PKI hierarchy, SSL SHA-2 and added Certification Authority Authorization
2.13	February 12, 2016	Update for Document Signing, Security Module and Subscriber obligations
2.14	March 7, 2016	Remove references to 1024-bit root and update approved key sizes
2.15	September 19, 2016	CT logging for SSL certificates, ECC key usage update and Document Signing key usage update
2.16	February 1, 2017	Update for Minimum Requirements for Code Signing, minimum key size and validity period, changes to Definitions, Disclaimers, Loss Limitations and Conflict of Provisions
2.17	July 14, 2017	Update for domain validation methods, inclusion of IP Address validation methods and update for CAA
3.0	May 31, 2018	Change CPS format to RFC 3647, merge the CPS for Extended Validation (EV) Certificates into this CPS, and update to show Baseline Requirements and Mozilla Policy compliance; this CPS supersedes the CPS for Extended Validation (EV) Certificates Version 2.0 dated February 1, 2017.
3.1	August 1, 2018	Update Roots, Subordinate and Cross Certified Cas, list of acronyms, domain validation, email address validation, CA termination, Certificate extensions, Certificate name forms, audit requirements and Certificate profiles
3.2	October 12, 2018	Revocation update, Repository clarification and CPS alignment.
3.3	February 28, 2019	Addition of Verified Mark Certificate (VMC) type TSA requirements and new domain name validation methods. Remove P-521 key size.
3.4	May 31, 2019	Update to IP address validation methods and CPR procedure
3.5	July 25, 2019	Update for Domain Name validation methods, VMC and Third Party RA restrictions.

3.6	September 30, 2019	Update for Baseline Requirements for Code Signing and CAA
3.7	September 30, 2020	Update Entrust brand, email address for CPR, implementation of CAB Forum ballots (SC23, SC24, SC25, SC28, SC30, SC31, SC33, and SC35), update for VMC Guidelines and remove from Appendix, and removal of non-inclusive language
3.8	December 31, 2020	CAB Forum ballot CSC4 and Document Signing Certificate Subscriber key generation
3.9	July 19, 2021	Update for CAB Forum ballots (CSC7, CSC8, SC42, SC44, SC45, SC46 and SC47), update for Mozilla policy 2.7.1, change Client Certificate to S/MIME Certificate, remove references to EV Code Signing Guidelines, update Technical Constraint requirements, update VMC requirements

TABLE OF CONTENTS

1. Introduction

Entrust Limited ("Entrust") uses its award winning suite of software products to provide standards-compliant digital certificates that enable more secure on-line communications.

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

- SSL Certificate(s)
- EV SSL Certificate(s)
- Code Signing Certificate(s)
- EV Code Signing Certificate(s)
- Client Certificate(s)
- Document Signing Certificate(s)
- Time-Stamp Certificates(s)
- Verified Mark 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 makes CA and RA services available in respect to Certificates. This CPS is applicable to all persons, entities, and organizations, including all Applicants, Subscribers, Relying Parties, Resellers, Co-marketers and any other persons, entities, or organizations that have a relationship with (i) Entrust in respect to Certificates and/or any services provided by Entrust 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 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, 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.

In respect to SSL Certificates, Entrust conforms to the current version of the CA/Browser Forum 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.

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

In respect to Code Signing Certificates, Entrust conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates published at http://www.cabforum.org. The Baseline Requirements for Code Signing describe the minimum requirements for Code Signing Certificates. If there is any inconsistency between this document and the Baseline Requirements for Code Signing, the Baseline Requirements for Code Signing take precedence over this document.

In respect to Verified Mark Certificates, Entrust conforms to the current version of the Minimum Security Requirements for Issuance of Verified Mark Certificates published at http://www.entrust.net/CPS. The VMC Requirements describe certain minimum requirements that a CA must meet in order to issue Verified Mark

Certificates. If there is any inconsistency between this document and the VMC Requirements, the VMC Requirements take precedence over this document.

1.2 Document Name and Identification

This document is called the Entrust Certificate Services Certification Practice Statement.

1.3 PKI Participants

1.3.1 Certification Authorities

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

This CPS covers all Certificates issued and signed by the following CAs.

Root
CN: Entrust.net Certification Authority (2048)
Subject Key Identifier: 55E4 81D1 1180 BED8 89B9 08A3 31F9 A124 0916 B970
Thumbprint (SHA-1): 5030 0609 1D97 D4F5 AE39 F7CB E792 7D7D 652D 3431

Subordinate CA(s)
CN: Entrust Class 1 Client CA
Subject Key Identifier: 47 90 a4 a1 0a 43 20 bf d0 74 54 b8 94 fa c4 7b b5 b6 1c 05

CN: Entrust Class 2 Client CA
Subject Key Identifier: 09 91 a5 ba e9 f2 2e 2a 75 df cd 7e fe 77 ca f2 de 6b 9b 24

CN: Entrust Class 3 Client CA - SHA256
Subject Key Identifier: 06 9f 6f 4e a2 29 4e 0f 0c ae 17 bf b6 98 46 ef ad b8 3b 72

CN: Entrust Certification Authority - L1C
Subject Key Identifier: 1e f1 ab 89 06 f8 49 0f 01 33 77 ee 14 7a ee 19 7c 93 28 4d

CN: Entrust Code Signing Certification Authority - L1D
Subject Key Identifier: a7 b1 aa c4 b6 06 ed dd ca 9f 88 94 96 82 d5 e7 43 41 d1 25

CN: Entrust Timestamping CA - TS1
Subject Key Identifier: c3 c2 71 d2 7b d7 68 05 ae 3b 39 9b 34 25 0c 62 03 c7 57 68

CN: Entrust Enterprise Intermediate CA – ICA1
Subject Key Identifier: c8 38 d4 0a 70 dd a3 57 a8 e5 96 59 2d 13 13 c9 20 d5 dc b3

Root
CN: Entrust Root Certification Authority
Subject Key Identifier: 68 90 e4 67 a4 a6 53 80 c7 86 66 a4 f1 f7 4b 43 fb 84 bd 6d
Thumbprint (SHA-1): b3 1e b1 b7 40 e3 6c 84 02 da dc 37 d4 4d f5 d4 67 49 52 f9

Subordinate CA(s)
CN: Entrust Certification Authority – L1E
Subject Key Identifier: 5b 41 8a b2 c4 43 c1 bd bf c8 54 41 55 9d e0 96 ad ff b9 a1

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

Subordinate CA(s)
CN: Entrust Class 1 Client CA – SHA256
Subject Key Identifier: e2 49 b9 ec 25 de b7 0c de e5 50 18 5b 48 cc 0c 8e 15 f2 a6

CN: Entrust Certification Authority – VMC1
Subject Key Identifier: 8b b6 39 76 d0 34 90 a6 3f 62 e1 64 ea 3e bc f4 7c 46 a1 73

CN: Entrust Certification Authority - L1K
Subject Key Identifier: 82 a2 70 74 dd bc 53 3f cf 7b d4 f7 cd 7f a7 60 c6 0a 4c bf

CN: Entrust Certification Authority - L1M
Subject Key Identifier: c3 f7 d0 b5 2a 30 ad af 0d 91 21 70 39 54 dd bc 89 70 c7 3a

CN: Entrust Extended Validation Code Signing CA - EVCS1
Subject Key Identifier: 2a 0a 6f 32 2c 29 20 21 76 6a b1 ac 8c 3c af 93 8e 0e 6b a2

CN: Entrust Code Signing CA - OVCS1
Subject Key Identifier: 7e 1a 1f 1a 11 74 5c 64 c9 0c 1f 94 01 ab fd 81 64 2e a1 2c

CN: CRYPTAS EV Issuing CA
Subject Key Identifier: fc bd 7e 9a 08 c2 54 9d 98 18 5d ba 2d 11 6e 08 61 7e a7 5f

CN: CRYPTAS OV Issuing CA
Subject Key Identifier: b8 d7 08 f5 1c a5 8f a6 45 52 13 f2 f4 d5 05 b7 73 aa 20 4a

CN: Siemens Issuing CA Internet Server 2020
Subject Key Identifier: c9 a7 57 cb 86 c9 61 07 c6 c2 b4 86 65 a9 1e c1 ca e1 02 9b

Root
CN: Entrust Root Certification Authority - EC1
Subject Key Identifier: b7 63 e7 1a dd 8d e9 08 a6 55 83 a4 e0 6a 50 41 65 11 42 49
Thumbprint (SHA-1): 20 d8 06 40 df 9b 25 f5 12 25 3a 11 ea f7 59 8a eb 14 b5 47

Subordinate CA(s)
CN: Entrust Certification Authority - L1F
Subject Key Identifier: 2e 62 f0 14 ee 87 cd b3 35 03 3d ef e4 b9 9e fd 3b b8 a3 c9

CN: Entrust Certification Authority - L1J
Subject Key Identifier: c3 f9 45 03 be c8 f9 0b 3c 45 35 f3 eb 72 ec e7 e8 eb 94 9b

Root
CN: Entrust Root Certification Authority – G4
Key Identifier: 9f 38 c4 56 23 c3 39 e8 a0 71 6c e8 54 4c e4 e8 3a b1 bf 67
SHA-1 Thumbprint: 14 88 4e 86 26 37 b0 26 af 59 62 5c 40 77 ec 35 29 ba 96 01

Subordinate CA(s)
CN: Entrust Certification Authority - L1N
Subject Key Identifier: ee 47 d1 85 71 f1 fd 2d b7 3f bb 3e 63 58 77 17 49 40 0e 95

Root
CN: Entrust Root Certification Authority – CSBR1
Key Identifier: 82 ba d6 3d 97 ce 9f cf 71 e8 92 37 af fd b3 b5 69 35 57 cf
SHA-1 Thumbprint: 89 74 24 05 3a 4a 88 7a c0 98 38 02 91 03 4d 88 5c 87 14 b9

CN: Entrust Extended Validation Code Signing CA – EVCS2
Subject Key Identifier: ce 89 4f 82 51 aa 15 a2 84 62 ca 31 23 61 d2 61 fb f8 fe 78

CN: Entrust Code Signing CA – OVCS2
Subject Key Identifier: ef 9f ba 79 b0 73 f2 25 1e 78 9c 03 52 9c 1b 53 84 de 8d ed

CN: Entrust Timestamping CA – TS2
Subject Key Identifier: 26 0f f0 c4 48 08 1b cd dd 91 f5 54 54 b6 b3 b3 fc 99 f1 08

Root
CN: Entrust Verified Mark Root Certification Authority – VMCR1
Key Identifier: 73 23 56 7b 2b 78 45 80 9a b8 c2 7c cc a5 86 39 8b 26 78 c5
SHA-1 Thumbprint: 4a 04 d5 a6 28 0e 98 e6 5c d4 7f 87 e8 ec a6 4c 8b 4a 9a 43

CN: Entrust Verified Mark CA – VMC2
Subject Key Identifier: ef bc 3c b4 af 3a d0 45 5e 76 54 df c7 64 78 e9 2d 1d 74 3f

Externally Issued Cross Certificates

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

1.3.2 Registration Authorities

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

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

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

1.3.3 Subscribers

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

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

1.4.1 Appropriate Certificate Uses

This CPS is applicable to the following Certificate Types.

SSL and EV SSL Certificates
SSL Certificates and EV SSL Certificates are intended for use in establishing web-based data communication conduits via TLS/SSL protocols. SSL Certificates and EV SSL Certificates conform to the requirements of the ITU-T X.509 v3 standard. The primary purpose of an SSL Certificate or EV 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.

Code Signing and EV Code Signing Certificates
Code Signing Certificates and EV Code Signing Certificates are used by content and software developers and publishers to digitally sign executables and other content. Code Signing and EV Code Signing Certificates conform to the requirements of the ITU-T X.509 v3 standard. The primary purpose of a Code Signing Certificate or EV Code Signing Certificate is to provide a method of ensuring that an executable object has come from an identifiable software publisher and has not been altered since signing.

S/MIME Certificates
S/MIME Certificates are used by individuals to digitally sign and encrypt electronic messages via an S/MIME compliant application. S/MIME Certificates conform to the requirements of the ITU-T X.509 v3 standard. The primary purpose of a S/MIME Certificate is to provide authentication, message integrity and non-repudiation of origin (using digital signatures) and privacy (using encryption).

Document Signing Certificates
Document Signing Certificates are used by individuals to digitally sign electronic documents. Document Signing Certificates conform to the requirements of the ITU-T X.509 v3 standard. Document Signing Certificates help to provide authentication and document integrity.

Time-Stamp Certificates
Time-Stamp Certificates are used by individuals to digitally sign time-stamp responses. Time-Stamp Certificates conform to the requirements of the ITU-T X.509 v3 standard. Time-Stamp Certificates help to provide authentication and time-stamp token integrity.

Verified Mark Certificates
Verified Mark Certificates are used to assert a brand identification for message identification. Verified Mark Certificates conform to the requirements of the ITU-T X.509 v3 standard. Verified Mark Certificates help to provide email messaging integrity.

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 in respect to Certificates are not designed, manufactured, or intended for use in or in conjunction with any application in which failure could lead to death, personal injury or severe physical or property damage, including the monitoring, operation or control of nuclear facilities, mass transit systems, aircraft navigation or communications systems, air traffic control, weapon systems, medical devices or direct life support machines, and all such uses are prohibited.

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

1.5 Policy Administration

1.5.1 Organization Administering the Document

The CPS is administered by the Policy Authority; it is based on the policies established by Entrust Limited.

1.5.2 Contact Person

The contact information for questions about Certificates is:

Entrust 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@entrust.com

Certificate Problem Reports, such as Certificate misuse, vulnerability reports or external reports of key compromise, must be emailed to ecs.support@entrust.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 with respect to Entrust, a person or entity that directly, or indirectly through one or more intermediaries, controls, is controlled by or is under common control with Entrust, and, with respect to any other party, any corporation or other entity that is directly or indirectly controlled by that party. In this context, a party "controls" a corporation or another entity if it directly or indirectly owns or controls fifty percent (50%) or more of the voting rights for the board of directors or other mechanism of control or, in the case of a non-corporate entity, an equivalent interest.

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

Applicant Representative: as defined in the Baseline Requirements.

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

Attestation Letter: as defined in the Baseline Requirements.

Author Domain: means the domain name of the apparent author of an email, as extracted from the "RFC5322.From field." The "RFC5322.From field" is also known by the names "Visible From field", "Message From field", and "From: field". It is the header field shown to the recipient of the message to represent the sender of the message, and is typically displayed as follows: From: "Friendly Name" <address@domain.com> The Author Domain in this field is the part of the email address between the "@" sign and the right-most angle bracket (i.e., "domain.com" in the example shown).

Authorization Domain Name: as defined in the Baseline Requirements.

Authorized Port: as defined in the Baseline Requirements.

Base Domain Name: as defined in the Baseline Requirements.

Baseline Requirements: means the CA/Browser Forum 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.

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

CA Key Pair: as defined in the Baseline Requirements.

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 the following Certificate types issued by the CA; S/MIME Certificate, Code Signing Certificate, Document Signing Certificate, EV Code Signing Certificate, EV SSL Certificate, SSL Certificate, Subordinate CA Certificate, Time-Stamp Certificate and Verified Mark Certificate.

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

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

Certificate Beneficiaries: means, collectively, all Application Software Vendors with whom Entrust 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 Problem Report: as defined in the Baseline Requirements.

Certificate Profile: as defined in the Baseline Requirements.

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

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

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

Certification Authority: means a certification authority operated by or on behalf of Entrust 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 Authority Authorization: as defined in the Baseline Requirements.

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 or an RA operating under a CA the right to promote Certificates.

Code Signing Baseline Requirements: means Baseline Requirements for Code Signing.

Code Signing Certificate: means a Certificate issued by a CA for use by content and software developers and publishers to digitally sign executables and other content.

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

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

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

Design Mark: as defined in the VMC Requirements.

Document Signing Certificate: means a Certificate issued by a CA for use by individuals or systems to digitally sign documents.

Domain Contact: as defined in the Baseline Requirements.

Domain Name Registrant: as defined in the Baseline Requirements.

Domain Name Registrar: as defined in the Baseline Requirements.

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

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

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

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

Enterprise RA: as defined in the Baseline Requirements.

Entrust: means Entrust Limited.

Entrust Group: means, collectively, Entrust, its Affiliates, its licensors (including for the avoidance of any doubt Microsoft), its resellers, its suppliers, its co-marketers, its subcontractors, its distributors and the directors, officers, employees, agents and independent contractors of any of them.

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

EV Certificate: A means an EV SSL or EV Code Signing Certificate.

EV Code Signing Certificate: means a Code Signing Certificate issued by a CA meeting the requirements of the EV Code Signing Certificate requirements of the Code Signing Baseline Requirements.

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

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

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

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

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

Incorporating Agency: as defined in the EV SSL Guidelines.

Internal Name: as defined in the Baseline Requirements.

IP Address: as defined in the Baseline Requirements.

IP Address Contact: as defined in the Baseline Requirements.

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

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

Key Compromise: as defined in the Baseline Requirements.

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

Mark Representation: as defined in the VMC Requirements.

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 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.

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.

Random Value: as defined in the Baseline Requirements.

Registered Mark: as defined in the VMC Requirements.

Registration Agency: as defined in the EV SSL Guidelines.

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

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

Request Token: as defined in the Baseline Requirements.

Request Value: as defined in the Baseline Requirements.

Required Website Content: as defined in the Baseline Requirements.

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

Reserved IP Address: as defined in the Baseline Requirements.

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

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

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

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

Subject: means the person, entity, or organization identified in the "Subject" field in a Certificate.

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

Subscriber Agreement: means the agreement between a Subscriber and Entrust (or an Affiliate of Entrust) 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. The Subscriber Agreement may consist of one or more parts.

Subsidiary Company: as defined in the Baseline Requirements.

Suspect Code: means any code or set of instructions that contains malicious functionality or serious vulnerabilities, including spyware, malware and other code that installs without the user's consent and/or resists its own removal, and code that can be exploited in ways not intended by its designers to compromise the trustworthiness of the computing environment on which it executes.

S/MIME Certificate: means a Certificate issued by a CA for use by individuals to digitally sign and encrypt electronic messages via an S/MIME compliant application.

Technically Constrained Subordinate CA Certificate: 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.

Time-Stamp Certificate: means a Certificate issued by a CA for use by a time-stamp authority to digitally sign time-stamp tokens.

Trusted Role: as defined in the CA/Browser Forum's Network and Certificate System Security Requirements.

Validation Specialist: as defined in the Baseline Requirements.

Verified Mark Certificate (or VMC): means a certificate that contains subject information and extensions specified in the VMC Requirements and that has been verified and issued by a CA in accordance with the VMC Requirements.

VMC Requirements: means the Minimum Security Requirements for Issuance of Verified Mark Certificates, published at https://bimigroup.org/supporting-documents/ (as such VMC Requirements may be amended from time to time). All Subscribers/Mark Asserting Entities and Consuming Entities (as such terms are defined in the VMC Requirements) are bound by the VMC Terms according to their terms.

VMC Terms: The Terms of Use that apply to a Verified Mark Certificate and to the Mark Representation (as such terms are defined in the VMC Requirements) and related data contained in a Verified Mark Certificate, as set out in Appendix B to the VMC Requirements. The current version of the VMC Terms are presented in this CPS at Appendix D.

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.

Word Mark: as defined in the VMC Requirements.

1.6.2 Acronyms

ADN	Authorization Domain Name
ASV	Application Software Vendor
CA	Certification Authority
CAA	Certification Authority Authorization
CPR	Certificate Problem Report
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CT	Certificate Transparency
DBA	Doing Business As
DN	Distinguished Name
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
ECC	Elliptic Curve Cryptography
EKU	Extended Key Usage
EV	Extended Validation
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
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
TSA	Time-Stamp Authority
URL	Universal Resource Locator
VMC	Verified Mark Certificate

2. Publication and Repository Responsibilities

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

2.1 Repositories

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

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

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

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

2.2 Publication of Certification Information

The CA publishes its CPS, CA Certificates, Subscriber 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. The CPS will be updated with an incremented version number and a new date on an annual basis even if no other changes have been made to this document.

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.

EV SSL and EV Code Signing Certificates

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

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

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

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.

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 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 hostname, the fully qualified hostname or path used in the DNS of the secure server on which the Applicant is intending to install the SSL Certificate;

(v) "Locality" (L), which is the city or locality of the organization's place of business; and

(vi) "State" (ST) (if applicable), which is the state or province of the organization's place of business.

Effective on or before 1 September 2022, the OU field will not be included in SSL Certificates.

EV SSL Certificates

(i) Same as SSL Certificates, plus

(ii) "serialNumber" which is the registration number of Subscriber,

(iii) "businessCategory" which is the applicable business category clause per the EV SSL Guidelines,

(iv) "jurisdictionOfIncorporationLocalityName" (if applicable) which is the jurisdiction of registration or incorporation locality of Subscriber,

(v) "jurisdictionOfIncorporationStateOrProvinceName" (if applicable) which is the jurisdiction of registration or incorporation state or province of Subscriber, and
(vi) "jurisdictionOfIncorporationCountry" which is the jurisdiction of registration or incorporation country of Subscriber.

Effective on or before 1 September 2022, the OU field will not be included in EV SSL Certificates.

Code Signing 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 full legal name of the organization;
(iii) "Organizational Unit Name" (OU) which is an optional field;
(iv) "Common Name" (CN) which is the same value as the "Organization Name";
(v) "Locality" (L), which is the city or locality of the organization's place of business; and
(vi) "State" (ST), which is the state or province of the organization's place of business, if applicable

EV Code Signing Certificates
(i) Same as Code Signing Certificates, plus
(ii) "serialNumber" which is the registration number of Subscriber,
(iii) "businessCategory" which is the applicable business category clause per the Code Signing Baseline Requirements,
(iv) "jurisdictionOfIncorporationLocalityName" (if applicable) which is the jurisdiction of registration or incorporation locality of Subscriber,
(v) "jurisdictionOfIncorporationStateOrProvinceName" (if applicable) which is the jurisdiction of registration or incorporation state or province of Subscriber, and
(vi) "jurisdictionOfIncorporationCountry" which is the jurisdiction of registration or incorporation country of Subscriber.

Class 1 S/MIME Certificates
(i) "Common Name" (CN) which is the e-mail address of the Subscriber;
(ii) "Email" (E), which is the e-mail address of the Subscriber; and
(iii) "Subject Alternative Name" (SAN), which is the e-mail address of the Subscriber.

Class 2 S/MIME 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 or individual, the organization name is not required, but may be the name of the Applicant;
(iii) "Organizational Unit Name" (OU) which is an optional field;
(iv) "Common Name" (CN) which is the name of the Subscriber and is a natural person;
(v) "Email" (E), which is the e-mail address of the Subscriber; and
(vi) "Subject Alternative Name" (SAN), which is the e-mail address of the Subscriber.

Document Signing 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 or individual, the organization name is not required, but may be the name of the Applicant;
(iii) "Organizational Unit Name" (OU) which is an optional field;
(iv) "Email" (E) is an optional field, which is the e-mail address of the Subject;
(v) "Serial Number" is an optional field, which is randomly generated and assigned to the Subject, if the Subject is an individual; and
(vi) "Common Name" (CN) which may be an individual's name, an organization's name or the name of a specific role within an organization.

Time-Stamp 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 full legal name of the organization;
(iii) "Organizational Unit Name" (OU) which is an optional field;
(iv) "Common Name" (CN) which is an optional field;
(v) "Locality" (L), which is the city or locality of the organization's place of business; and
(vi) "State" (ST), which is the state or province of the organization's place of business, if applicable

Verified Mark 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 full legal name of the organization;
(iii) "Organizational Unit Name" (OU), (optional);
(iv) "Common Name" (CN) (optional) which is either the full legal name of the organization or the Word Mark;
(v) "Street Address", which is the number and street address of the organization's place of business;
(vi) "Locality" (L), which is the city or locality of the organization's place of business;
(vii) "State" (ST), (if applicable) which is the state or province of the organization's place of business;
(viii) "Postal Code" which is the postal code of the organization's place of business;
(ix) "serialNumber" which is the registration number of Subscriber;
(x) "businessCategory" which is the applicable business category clause per the VMC Requirements;
(xi) "jurisdictionOfIncorporationLocalityName" (if applicable) which is the jurisdiction of registration or incorporation locality of Subscriber;
(xii) "jurisdictionOfIncorporationStateOrProvinceName" (if applicable) which is the jurisdiction of registration or incorporation state or province of Subscriber;
(xiii) "jurisdictionOfIncorporationCountry" which is the jurisdiction of registration or incorporation country of Subscriber;
(xiv) "trademarkCountryOrRegionName" which is trademark country;
(xv) "trademarkOfficeName" (optional) which is trademark agency office name; and
(xvi) "trademarkRegistration" which is trademark registration number.

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.

SSL Certificates

The value of the Common Name to be used in an SSL Certificate shall be the Applicant's fully qualified hostname or path that is used in the DNS of the secure server on which the Applicant is intending to install the SSL Certificate. Notwithstanding the preceding sentence, the Common Name may include wildcard characters (i.e., an asterisk character).

EV SSL Certificates

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

Code Signing Certificates
The value of the Common Name to be used in a Code Signing Certificate shall be the Applicant's organization name.

EV Code Signing Certificates
The value of the Common Name to be used in an EV Code Signing Certificate shall be the Applicant's organization name.

S/MIME Certificates
The value of the Common Name to be used in a S/MIME Certificate shall be the name or the email address of the Subscriber.

Document Signing Certificates
The value of the Common Name to be used in a Document Signing Certificate shall be the name of the Subscriber, the role of the Subscriber, or the group or organization that the Subscriber represents.

Time-Stamp Certificates
The value of the Common Name to be used in a Time-Stamp Certificate, if present shall be a name of the time-stamp service associated with the Subscriber.

Verified Mark Certificates
The value of the Common Name to be used in a Verified Mark Certificate, if present shall be the Applicant's organization name or Word Mark.

3.1.3 Anonymity or Pseudonymity of Subscribers

No stipulation.

3.1.4 Rules for Interpreting Various Name Forms

No stipulation.

3.1.5 Uniqueness of Names

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

3.1.6 Recognition, Authentication, and Role of Trademarks

The Subject names in Certificates are issued on a "first come, first served" basis. By accepting a Subject name for incorporation into a Certificate, an RA operating under a CA does not determine whether the use of such information infringes upon, misappropriates, dilutes, unfairly competes with, or otherwise violates any intellectual property right or any other rights of any person, entity, or organization. The CAs and any RAs operating under the CAs neither act as an arbitrator nor provide any dispute resolution between Subscribers or between Subscribers and third-party complainants in respect to the use of any information in 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 Subscriber 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 Subscriber 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 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 Subscriber 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

The CA or the RA performs verification of any organizational identities that are submitted by an Applicant or Subscriber in accordance with the practices mandated by the Policy Authority. The CA or the RA determines 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, the CA or the RA uses commercially reasonable efforts to confirm the existence of the organization. Such commercially reasonable efforts may include site visits or third-party attestation letter.

EV SSL, EV Code Signing and Verified Mark Certificates

In accordance with the EV SSL Guidelines or the VMC Requirements, the CA or the RA will determine:

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

Prior to the use of an Incorporating Agency or Registration Agency to fulfill these verification requirements, the agency information about the Incorporating Agency or Registration Agency will be disclosed at https://www.entrust.com/legal-compliance/approved-incorporating-agencies.

This agency information includes the following:

(iv) Sufficient information to unambiguously identify the Incorporating Agency or Registration Agency (such as a name, jurisdiction, and website);
(v) The accepted value or values for each of the subject:jurisdictionLocalityName (OID: 1.3.6.1.4.1.311.60.2.1.1), subject:jurisdictionStateOrProvinceName (OID: 1.3.6.1.4.1.311.60.2.1.2), and subject:jursidictionCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3) fields, when a Certificate is issued using information from that Incorporating Agency or Registration Agency, indicating the jurisdiction(s) that the agency is appropriate for; and,
(vi) A revision history that includes a unique version number and date of publication for any additions, modifications, and/or removals from this list.

3.2.2.2 DBA/Tradename

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

(i) Documentation provided by, or communication with, a government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
(ii) A Reliable Data Source;
(iii) Communication with a government agency responsible for the management of such DBAs or tradenames;
(iv) An Attestation Letter accompanied by documentary support; or
(v) A utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that the CA determines to be reliable.

Verified Mark Certificates

DBA will not be included in a Verified Mark Certificate.

3.2.2.3 Verification of Country

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

3.2.2.4 Validation of Domain Authorization or Control

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

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

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

Verified Mark Certificates
Subscriber must disclose each Author Domain to be supported by a Verified Mark Certificate.

3.2.2.4.1 Validating the Applicant as a Domain Contact

This method of domain validation is not used.

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

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

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

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

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

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

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

3.2.2.4.3 Phone Contact with Domain Contact

This method of domain validation is not used.

3.2.2.4.4 Constructed Email to Domain Contact

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

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

The Random Value shall be unique in each email.

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

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

3.2.2.4.5 Domain Authorization Document

This method of domain validation is not used.

3.2.2.4.6 Agreed-Upon Change to Website

This method of domain validation is not used.

3.2.2.4.7 DNS Change

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

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

3.2.2.4.8 IP Address

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

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

3.2.2.4.9 Test Certificate

This method of domain validation is not used.

3.2.2.4.10 TLS Using a Random Number

This method of domain validation is not used.

3.2.2.4.11 Any Other Method

This method of domain validation is not used.

3.2.2.4.12 Validating Applicant as a Domain Contact

This method of domain validation is not used.

3.2.2.4.13 Email to DNS CAA Contact

Confirm the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value will be sent to a DNS CAA Email Contact. The relevant CAA Resource Record Set will be found using the search algorithm defined in RFC 8659 Section 3.

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

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

3.2.2.4.14 Email to DNS TXT Contact

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

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

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

3.2.2.4.15 Phone with Domain Contact

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

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

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

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

3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact

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

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

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

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

3.2.2.4.17 Phone Contact with DNS CAA Phone Contact

Confirm the Applicant's control over the FQDN by calling the DNS CAA Phone Contact's phone number and obtain a confirming response to validate the ADN. Each phone call may confirm control of multiple ADNs provided that the same DNS CAA Phone Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN. The relevant CAA Resource Record Set must be found using the search algorithm defined in RFC 8659 Section 3.

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

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

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

3.2.2.4.18 Agreed Upon Change to Website v2

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

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

The file containing the Request Token or Random Number:

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

The CA follows redirects and the following apply:

(vii) Redirects must be initiated at the HTTP protocol layer .
    a. For validations performed on or after July 1, 2021, redirects will only be the result of a 301, 302, or 307 HTTP status code response, as defined in RFC 7231, Section 6.4, or a 308 HTTP status code response, as defined in RFC 7538, Section 3. Redirects must be to the final value of the Location HTTP response header, as defined in RFC 7231, Section 7.1.2.
    b. For validations performed prior to July 1, 2021, redirects will only be the result of an HTTP status code result within the 3xx Redirection class of status codes, as defined in RFC 7231, Section 6.4.
(viii) Redirects must be to resource URLs with either via the "http" or "https" scheme.
(ix) Redirects must be to resource URLs accessed via Authorized Ports.

If a Random Value is used, then:

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

Note: Once the FQDN has been validated using this method, the CA does NOT also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is NOT suitable for validating Wildcard Domain Names.

3.2.2.4.19 Agreed Upon Change to Website - ACME

This method of domain validation is not used.

3.2.2.4.20 TLS Using ALPN

This method of domain validation is not used.

3.2.2.5 Authentication of an IP Address

This section defines the permitted processes and procedures for validating the Applicant's ownership or control of an IP Address listed in a Certificate.

The CA will confirm that prior to issuance, the CA has validated each IP Address listed in the Certificate using at least one of the methods specified in this section.

Completed validations of Applicant authority may be valid for the issuance of multiple Certificates over time. In all cases, the validation must have been initiated within the time period specified in the relevant requirement (such as Section 4.2.1 of this document) prior to Certificate issuance. For purposes of IP Address validation, the term Applicant includes the Applicant's Parent Company, Subsidiary Company, or Affiliate.

After July 31, 2019, CAs will maintain a record of which IP Address validation method, including the relevant Baseline Requirements version number, was used to validate every IP Address.

3.2.2.5.1 Agreed-Upon Change to Website

This method of IP Address validation is not used.

3.2.2.5.2 Email, Fax, SMS, or Postal Mail to IP Address Contact

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

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

The CA may send the email, fax, SMS, or postal mail identified under this section to more than one recipient provided that every recipient is identified by the IP Address Registration Authority as representing the IP Address Contact for every IP Address being verified using the email, fax, SMS, or postal mail.

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

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

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

3.2.2.5.3 Reverse Address Lookup

Confirm the Applicant's control over the IP Address by obtaining a Domain Name associated with the IP Address through a reverse-IP lookup on the IP Address and then verifying control over the FQDN using a method permitted under Baseline Requirements section 3.2.2.4.

3.2.2.5.4 Any Other Method

This method of IP Address validation is not used.

3.2.2.5.5 Phone Contact with IP Address Contact

This method of IP Address validation is not used.

3.2.2.5.6 ACME "http-01" method for IP Addresses

This method of IP Address validation is not used.

3.2.2.5.7 ACME "tls-alpn-01" method for IP Addresses

This method of IP Address validation is not used.

3.2.2.6 Wildcard Validation

The CAs follow a documented procedure that determines if a wildcard character in a domain name occurs in the first label position to the left of a "registry-controlled" label or "public suffix" (e.g. ".com",".co.uk", see RFC 6454 section 8.2 for further explanation). If a wildcard falls within the label immediately to the left of a registry-controlled or public suffix, the CAs refuse issuance unless the Applicant proves its rightful control of the entire domain namespace.

3.2.2.7 Data Source Accuracy

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

3.2.2.8 CAA Records

Entrust policy on CAA records is stated in §4.2.4.

3.2.2.9 Authentication of Email Address

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

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

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

3.2.2.10 Authentication of Registered Trademark

Verified Mark Certificates

The CA or RA shall verify the following:

(i) Registered Mark
   a. Registered Mark is in good standing with the official database of the applicable trademark office;
   b. Mark Representation matches the Registered Mark as it appears in the official database of the applicable trademark office. ;
   c. Either 1) the owner of the Registered Mark is the same as the Subject organization (or to a Parent, Subsidiary, or Affiliate of the organization) of the Certificate or 2) the Subject organization has obtained the right to use the Registered Mark through a mutually agreed-on license from the entity who is the owner (or a Parent, Subsidiary, or Affiliate of the owner) of record of the Registered Mark and the owner has provided an authorization letter;
   d. Mark Representations are only be in colors if and as permitted by the Registered Mark and the applicable law of the Trademark Office; and
   e. Retain a screenshot or other record of the Mark Representation provided by the Applicant and all information about the Registered Mark obtained from the applicable trademark office.;

(ii) Trademark country or region of the trademark office;

(iii) Trademark registration number provided by the trademark office; and

(iv) Trademark office name is required, if the applicable country/region has regional intellectual property agencies.

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.

SSL Certificates

An individual identity will 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 is inspected for any indication of alteration or falsification.

The Applicant's address will 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 is verified by contacting the Applicant using a reliable method of communication.

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

Class 1 S/MIME Certificates
The Subject identity asserted in Class 1 S/MIME Certificates is an email address that represents the Subscriber.

Class 2 S/MIME Certificates
The Subject identity is authenticated by matching the identity provided by the Applicant or Subscriber to information contained in the business records or databases (e.g. employee or customer directories) of an Enterprise RA approving Certificates to its own affiliated individuals.

Document Signing Certificates
The Subject identity or the Applicant Representative identity is authenticated by face-to-face meeting or by means of a secure video communication where the Subject's valid government-issued photo ID is used to provide identity.

Verified Mark Certificates
The Contract Signer or the Certificate Approver is authenticated by face-to-face based on the requirements of the VMC Requirements.

3.2.4 Non-verified Subscriber Information

No stipulation.

3.2.5 Validation of Authority

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

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

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

EV SSL and EV Code Signing Certificates
The CA or RA verifies the identity and authority of the Contract Signer and Certificate Approver in accordance with EV SSL Guidelines section 11.8.

Verified Mark Certificates
The CA or RA verifies the identity and authority of the Contract Signer and Certificate Approver in accordance with VMC Requirements.

3.2.6 Criteria for Interpretation

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

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

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

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

SSL and EV SSL Certificates
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 Subscriber 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 Subscriber 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. The Applicant may be provided with a URL that can be used to retrieve the Certificate.

EV SSL, EV Code Signing and Verified Mark Certificates

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

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

4.1.1 Who Can Submit a Certificate Application

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

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

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

4.1.2 Enrollment Process and Responsibilities

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

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

The enrollment process includes:

(i) Agreeing to the applicable Subscriber 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.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

4.2.1.1 Validated Information Reuse

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.

SSL Certificates
Effective 2021-10-01, for validation of Domain Names and IP Addresses according to §3.2.2.4 and §3.2.2.5, any reused data, document, or completed validation can be obtained no more than 398 days prior to issuing the Certificate.

EV SSL, EV Code Signing and Verified Mark Certificates
Reuse of previous validation data or documentation obtained from a source specified under §3.2 may be used no more than 398 days after such data or documentation was validated.

4.2.1.2 High Risk Certificate Requests

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

4.2.2 Approval or Rejection of Certificate Applications

The CAs do not issue Certificates containing Internal Names.

4.2.3 Time to Process Certificate Applications

No stipulation.

4.2.4 Certification Authority Authorization (CAA) Records

When CAA record checking is implemented, the CA checks for CAA records for each dNSName in the subjectAltName extension of the Certificate to be issued, according to the procedure in RFC 8659, following the processing instructions set down in RFC 8659 for any records found. If the Certificate is issued, it will be issued within the TTL of the CAA record, or 8 hours, whichever is greater.

When processing CAA records, the CAs process the property tags as specified in RFC 8659. The CA does not act on the contents of the iodef property tag. The CAs respect the critical flag and will not issue a Certificate if they encounter an unrecognized property with this flag set.

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

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

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

(iv) the failure is outside the CA's infrastructure; and
(v) the lookup has been retried at least once; and

(vi) the domain's zone does not have a DNSSEC validation chain to the ICANN root.

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

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

SSL and EV SSL Certificates
The CA performs CAA record checking on issue, issuewild, and iodef property tags prior to issuing SSL and EV SSL Certificates.

Verified Mark Certificate
The CA performs CAA record checking on issuevmc property tag prior to issuing Verified Mark Certificates for Certificates issued on or after 1 January 2022. The sub-syntax of the "issuevmc" property tag value is the processed the same as the "issue" property tag as defined in section 4.2 of RFC 8659.

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. An Enterprise RA can approve issuance of Certificates and submit the certificate request to an RA.

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

4.3.1 CA Actions During Certificate Issuance

Certificate issuance by the Root CA requires 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. Entrust will not issue Certificates with validity period that exceeds the validity period of the corresponding Root Certificate.

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 uses commercially reasonable efforts to notify the Applicant by email that the Applicant's Certificate is available. The email may contain a URL for use by the Applicant to retrieve the Certificate.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

No stipulation.

4.4.2 Publication of the Certificate by the CA

No stipulation.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

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

SSL and EV SSL Certificates
SSL Certificates and EV SSL Certificates may include two or more signed certificate timestamps (SCT) from ASV approved independent Certificate Transparency logs.

Verified Mark Certificates
Verified Mark Certificates will include one or more signed certificate timestamps (SCT) from Certificate Transparency logs as defined in the VMC Requirements.

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 Subscriber Agreement, CAs or RAs will provide a Certificate lifecycle monitoring service which will support Certificate renewal.

4.6.2 Who May Request Renewal

Subscribers or Subscriber agents may request renewal of Certificates.

4.6.3 Processing Certificate Renewal Requests

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

Certificates may be renewed using the previously accepted Public Key, if the Public Key meets the key size requirements of §6.1.5. The Public Key may not be reused if another Certificate with the same Public Key has been revoked due to Key Compromise.

4.6.4 Notification of New Certificate Issuance to Subscriber

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

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

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

No stipulation.

4.6.6 Publication of the Renewal Certificate by the CA

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

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.7 Certificate Re-key

4.7.1 Circumstance for Certificate Re-key
No stipulation.

4.7.2 Who May Request Certification of a New Public Key
No stipulation.

4.7.3 Processing Certificate Re-keying Requests
No stipulation.

4.7.4 Notification of New Certificate Issuance to Subscriber
No stipulation.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate
No stipulation.

4.7.6 Publication of the Re-keyed Certificate by the CA
No stipulation.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities
No stipulation.

4.8 Certificate Modification

4.8.1 Circumstance for Certificate Modification
No stipulation.

4.8.2 Who May Request Certificate Modification
No stipulation.

4.8.3 Processing Certificate Modification Requests
No stipulation.

4.8.4 Notification of New Certificate Issuance to Subscriber
No stipulation.

4.8.5 Conduct Constituting Acceptance of Modified Certificate
No stipulation.

4.8.6 Publication of the Modified Certificate by the CA
No stipulation.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities
No stipulation.

4.9 Certificate Revocation and Suspension
The CA shall revoke a Certificate after receiving a valid revocation request from an RA operating under such CA. An RA operating under a CA shall be entitled to request and may request that a CA revoke a Certificate after such RA receives a valid revocation request from the Subscriber for such Certificate. An RA operating

under a CA shall be entitled to request and shall request that a CA revoke a Certificate if such RA becomes aware of the occurrence of any event that would require a Subscriber to cease to use such Certificate.

CAs do not support the suspension of Certificates.

4.9.1 Circumstances for Revocation

4.9.1.1 Reasons for Revoking a Subscriber Certificate

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

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

(i) The Subscriber requests in writing that the CA revoke the Certificate;
(ii) The Subscriber notifies the CA that the original Certificate request was not authorized and does not retroactively grant authorization;
(iii) The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise;
(iv) The CA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys);or
(v) The CA obtains evidence that the validation of the domain authorization or control for any FQDN or IP Address in the Certificate should not be relied upon.

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

(vi) The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6;
(vii) The CA obtains evidence that the Certificate was misused;
(viii) The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement;
(ix) 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);
(x) The CA is made aware that a Certificate with a Wildcard Domain Name has been used to authenticate a fraudulently misleading subordinate FQDN;
(xi) The CA is made aware of a material change in the information contained in the Certificate;
(xii) The CA is made aware that the Certificate was not issued in accordance with this CPS;
(xiii) The CA determines that any of the information appearing in the Certificate is inaccurate;
(xiv) 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;
(xv) Revocation is required by any other section in this CPS;
(xvi) The CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed;
(xvii) The technical content or format of the Certificate presents an unacceptable risk to ASVs or Relying Parties;
(xviii) A Certificate is used to digitally sign hostile code, including spyware or other malicious software (malware); or
(xix) Any other reason that may be reasonably expected to affect the integrity, security, or trustworthiness of a Certificate or CA.

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

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

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

4.9.2 Who Can Request Revocation

CAs, RAs and Subscribers may initiate revocation.

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

4.9.3 Procedure for Revocation Request

A Subscriber shall request revocation of their Certificate if the Subscriber has a suspicion or knowledge of or a reasonable basis for believing that of any of the following events have occurred:

(i) Compromise of the Subscriber's Private Key;
(ii) Knowledge that the original Certificate request was not authorized and such authorization will not be retroactively granted;
(iii) Change in the information contained in the Subscriber's Certificate;
(iv) Change in circumstances that cause the information contained in Subscriber's Certificate to become inaccurate, incomplete, or misleading.

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

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

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

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

4.9.4 Revocation Request Grace Period

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

4.9.5 Time within Which CA Must Process the Revocation Request

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

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

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

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 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 issue CRLs as follows:

(i) CRLs for Certificates issued to Subordinate CAs are be issued at least once every twelve months or with 24 hours after revoking a Subordinate CA Certificate. The next CRL update will not be more than twelve months from the last update.
(ii) CRLs for SSL Certificates, EV SSL Certificates, Code Signing Certificates, EV Code Signing Certificates, S/MIME Certificates, Document Signing Certificates and Verified Mark

Certificates are issued at least once every 24 hours. The CRL will indicate the next update of 7 days after issuance.

(iii) CRLs for Time-Stamp Certificates are issued at least once every twelve months or with 24 hours after revoking a Time-stamp Certificate. The next CRL update will not be more than twelve months 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 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 SSL Certificates, EV SSL Certificates, Code Signing Certificates, EV Code Signing Certificates, S/MIME Certificate, Document Signing Certificates and Verified Mark Certificates shall be issued at least once every 24 hours. OCSP responses will have a maximum expiration time of seven days.

(iii) OCSP responses for Time-Stamp Certificates shall be issued at least once every twelve months or within 24 hours after revoking a Subordinate CA Certificate.

Code Signing Certificates that have been revoked due to Key Compromise or issued to unauthorized person will be maintained in the Repository for at least ten years following revocation.

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

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

4.9.11 Other Forms of revocation Advertisements Available

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.

Subscribers, Relying Parties, ASVs, Anti-Malware Organizations and other third parties may advise Entrust of a Private Key Compromise using one of the following demonstration methods:

(i) Submission of a signed CSR with a common name of "Proof of Key Compromise for Entrust", or
(ii) Submission of a Private Key.

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

SSL and EV 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.

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

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

No stipulation.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy Practices

No stipulation.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5. Facility, Management, and Operational Controls

The CA/Browser Forum's Network and Certificate System Security Requirements are incorporated by reference as if fully set forth herein.

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's other systems to restrict access to personnel in Trusted Roles. The security zone is constructed with privacy and secured with slab-to-slab 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. Alarm systems are used to notify security personnel of any violation of the rules for access to a CA.

5.1.3 Power and Air Conditioning

The Security zone is equipped with:

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

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

5.1.4 Water Exposures

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

5.1.5 Fire Prevention and Protection

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

5.1.6 Media Storage

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

5.1.7 Waste Disposal

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

5.1.8 Off-site Backup

As stipulated in §5.5.

5.2 Procedural Controls

5.2.1 Trusted Roles

The CAs have a number of Trusted Roles for sensitive operations of the CA software.

5.2.2 Number of Persons Required per Task

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

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

5.2.3 Identification and Authentication for Each Role

Personnel in Trusted Roles must undergo background investigations and must be trained for their specific role.

5.2.4 Roles Requiring Separation of Duties

No stipulation.

5.3 Personnel Controls

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

5.3.1 Qualifications, Experience and Clearance Requirements

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

5.3.2 Background Check Procedures

No stipulation.

5.3.3 Training Requirements

Personnel in Trusted Roles and Validation Specialists are provided skills-training which is based on industry requirements including the Baseline Requirements, EV SSL Guidelines, Code Signing Baseline Requirements and VMC Requirements.

Validation Specialists perform information verification duties with skills-training that covers basic PKI knowledge, authentication and vetting policies and procedures (including this CPS), and common threats to the information verification process (including phishing and other social engineering tactics). Validation Specialists receive skills-training prior to commencing their job role and are required them to pass an examination on the applicable information verification requirements. The CA maintains 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 Certificate key lifecycle events, including:
- a. Key generation, backup, storage, recovery, archival, and destruction;
- b. Certificate requests, renewal and re-key requests, and revocation;
- c. Approval and rejection of Certificate requests;
- d. Cryptographic device lifecycle management events ;
- e. Generation of CRLs and OCSP entries; and
- f. Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.

(ii) Subscriber Certificate lifecycle management events, including:
- g. Certificate requests, renewal and re-key requests, and revocation;
- h. All verification activities required by this CPS;
- i. Approval and rejection of Certificate requests;
- j. Issuance of Certificates; and
- k. Generation of CRLs and OCSP entries.

(iii) Security events, including:
- l. Successful and unsuccessful PKI system access attempts;
- m. PKI and security system actions performed;
- n. Security profile changes;
- o. System crashes, hardware failures, and other anomalies;
- p. Firewall and router activities; and
- q. Entries to and exits from the CA facility.

Log entries include the following elements:
- r. Date and time of record;
- s. Identity of the person making the journal record; and
- t. Description of record.

5.4.2 Frequency of Processing Log

No stipulation

5.4.3 Retention Period for Audit Log

The CA will retain, for at least two years:

(i) CA Certificate and key lifecycle management event records, as set forth in §5.4.1(i), after either: the destruction of the CA key, or the revocation or expiration of the CA Certificate, whichever occurs later;

(ii) Subscriber Certificate lifecycle management event records, as set forth in Section §5.4.1(ii), after the revocation or expiration of the Subscriber Certificate; and

(iii) Any security event records, as set forth in §5.4.1(iii), after the event occurred.

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 protected by encryption. The archive media is protected through storage in a restricted-access facility to which only Entrust-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 has implemented a secure disaster recovery facility that is greater than 250 km from the primary secure CA facilities.

Entrust 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 as being very unlikely; however, Entrust 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 of CA termination, Entrust will:

(i) Provide notice and information about the CA termination by sending notice to Subscribers with unrevoked unexpired Certificates, Application Software Vendors, and Third Party Subordinate CAs and by posting such information in the Repository; and

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

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

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

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

(v) Destroy all CA Private Keys; and

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

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

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

(i) Prepare and follow a Key Pair generation script;
(ii) Have a qualified auditor witness the CA Key Pair generation process;
(iii) Have a qualified auditor issue a report opining that the CA followed its CA Key Pair generation ceremony during its key generation process and the controls to ensure the integrity and confidentiality of the CA Key Pair;
(iv) Generate the CA Key Pair in a physically secured environment;
(v) Generate the CA Key Pair using personnel in Trusted Roles under the principles of multiple person control and split knowledge;
(vi) Generate the CA Key Pair within cryptographic modules meeting the applicable requirements of §6.2.11;
(vii) Log its CA Key Pair 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 CA Key Pair 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 or initiate a new, secure, and cryptographically sound Key Pair to be used in association with the Subscriber's Certificate or Applicant's Certificate Application.

The CA will reject a Certificate request if one or more of the following conditions are met:

(i) The Key Pair does not meet the requirements set forth in §6.1.5 and/or §6.1.6;
(ii) There is clear evidence that the specific method used to have generate the Private Key was flawed;
(iii) The CA is aware of a demonstrated or proven method that exposes the Private Key to compromise;
(iv) The CA has previously been made aware that the Private Key has suffered a Key Compromise, such as through the provisions of Section 4.9.1.1;
(v) The CA is aware of a demonstrated or proven method to easily compute the Private Key based on the Public Key (such as a Debian weak key, see https://wiki.debian.org/SSLkeys).

SSL and EV SSL Certificates

The CA will not generate a Key Pair on behalf of a Subscriber, and will not accept a Certificate request using a Key Pair previously generated by the CA.

S/MIME Certificates
In order to support key backup, the CA may optionally provide a service to generate the Key Pair on behalf of the Applicant or Subscriber. The Key Pair is generated on a cryptographic module that meets or exceeds the requirements as defined in §6.2.11. The prime number generator is in accordance with FIPS 186-2.

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

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

6.1.2 Private Key Delivery to Subscriber

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

S/MIME Certificates
In the case where the Key Pair is generated on behalf of the Subscriber by the CA, the Private Key will be delivered to the Subscriber in a cryptographically secure manner in a PKCS #12 format.

Managed and Hosted Cryptographic Module
In the case a CA managed and hosted cryptographic module is used, the Private Key will be generated, stored and managed on a cryptographic module which meets the requirements as defined in §6.2.11. The CA enforces multi-factor authentication to allow the Subscriber to enroll to generate the Key Pair or to use the Private Key for signing. The Private Key is not delivered to the Subscriber.

6.1.3 Public Key Delivery to Certificate Issuer

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

6.1.4 CA Public Key Delivery to Relying Parties

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

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

6.1.5 Key Sizes

For RSA Key Pairs the CA will ensure that the modulus size, when encoded, is at least 2048 bits, and that the modulus size, in bits, is evenly divisible by 8.

CA Key Size
For CAs using RSA keys, the size is 2048, 3072 or 4096-bits. For CAs using ECC keys, the size is NIST P-384.

As of July 1, 2017, the minimum key size for a Root CA supporting the Adobe Approved Trust List is 3072-bit RSA or ECC NIST P-384.

As of January 1, 2021, the minimum key size for new CA Certificates which issue Code Signing and Time-stamping Certificates is 3072-bit RSA and ECC NIST P-384.

SSL and EV SSL Certificates
The RSA key size is 2048, 3072 or 4096-bits. The ECC key size is NIST P-256 or P-384.

S/MIME Certificates
The RSA key size is 2048, 3072 or 4096-bits.

Code Signing and EV Code Signing Certificates
The RSA key size is 2048, 3072 or 4096-bits. As of June 1, 2021, the minimum key size is RSA 3072 bits. The ECC key size is NIST P-256 or P-384.

Document Signing Certificates
The RSA key size is 2048, 3072 or 4096-bits. The ECC key size is NIST P-256 or P-384.

Time-Stamp Certificates
The RSA key size is 2048, 3072 or 4096-bits. As of June 1, 2021, the minimum key size is RSA 3072 bits. The ECC key size is NIST P-256 or P-384.

Verified Mark Certificates
The RSA key size is 2048, 3072 and 4096-bits. The ECC key size is NIST P-256 and P-384.

6.1.6 Public Key Parameters Generation and Quality Checking

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

S/MIME and Document Signing Certificates
In the case where the CA has generated the Key Pair on behalf of the Subscriber, the Key Pair is generated in accordance with FIPS 186.

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.

Verified Mark Certificates
Private Keys corresponding to Root Certificates will not sign Subordinate CA or Cross Certificates unless the Certificate to be signed contains id-kp-BrandIndicatorforMessageIdentification (OID: 1.3.6.1.5.5.7.3.31) as the sole KeyPurposeId in the extendedKeyUsage extension.

Private Keys corresponding to Subordinate CA or Cross Certificates will not sign Certificates unless the Certificate to be signed contains id-kp-BrandIndicatorforMessageIdentification (OID: 1.3.6.1.5.5.7.3.31) or id-kp-OCSPSigning (OID: 1.3.6.1.5.5.7.3.9) as the sole KeyPurposeId in the extendedKeyUsage extension.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

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

6.2.1 Cryptographic Module Standards and Controls

CA Private Keys

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

S/MIME Certificates

For cases where the CA has generated the Key Pair on behalf of the Subscriber, the CA use cryptographic modules which meet or exceed the requirements as defined in §6.2.11.

Document Signing Certificates

Subscribers are responsible for protecting the Private Key associated with the Public Key in the Subscriber's Certificate. Subscribers must use cryptographic hardware modules that meet or exceed the requirements as defined in §6.2.11.

Managed and Hosted Cryptographic Module

In the case a CA managed and hosted cryptographic module is used, the cryptographic modules meets or exceeds the requirements as defined in §6.2.11.

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

A minimum of two-person control is 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 are designated as authorized by the CA for this purpose. The names of the parties used for two-person control are maintained on a controlled list.

6.2.3 Private Key Escrow

Entrust does not escrow Private Keys.

6.2.4 Private Key Backup

CA Private Keys

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

S/MIME Certificates

For cases where the CA has generated the Key Pair on behalf of the Subscriber, the CA securely maintains a backup copy of the Private Key during the term of services.

Managed and Hosted Cryptographic Module

In the case a CA managed and hosted cryptographic module is used, the encrypted Private Keys are backed up on a regular basis for disaster recovery purposes.

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 are 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 may 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.

S/MIME Certificates
For cases where the CA has generated the Key Pair on behalf of the Subscriber, the CA may securely maintain an archive of the Subscriber Private Key in the secure long-term backups.

Managed and Hosted Cryptographic Module
In the case a CA managed and hosted cryptographic module is used, the Private Key is not archived.

6.2.6 Private Key Transfer into or from Cryptographic Module

CA Private Keys are 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 will revoke all Certificates corresponding to Private Key.

Managed and Hosted Cryptographic Module
In the case a CA managed and hosted cryptographic module is used, the Private Key will be encrypted using the AES 256 key wrapping functionality of the cryptographic module and stored in a secure database.

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 are activated under two-person control using the methodology provided with the cryptographic module.

Subscriber Private Keys
Subscriber Private Keys should 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.

Managed and Hosted Cryptographic Module
In the case a CA managed and hosted cryptographic module is used, the Private Key activation is performed with the Subject's multi-factor authentication. The Subject shall protect access credentials to the Private Key in accordance with §9.6.3.

6.2.9 Method of Deactivating Private Key

CA Private Keys
CA Private Keys will be deactivated when the CA is not required for active use. Deactivation of the Private Keys is 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.

Subscriber Private Keys
Subscriber Private Keys are deemed to be deactivated when the Private Key is no longer needed or all Certificates associated with the Private Key have expired or been 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.

S/MIME Certificates
For cases where the CA has generated the Key Pair on behalf of the Subscriber, Private Keys which have been archived will be destroyed in accordance with the backup destruction process.

Managed and Hosted Cryptographic Module
In the case a CA managed and hosted cryptographic module is used, the Subject of the Certificate may destroy the Private Key using multi-factor authentication. The CA is authorized to destroy the Private Key when the subscription to the service has terminated.

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.

S/MIME Certificates
For cases where the CA has generated the Key Pair on behalf of the Subscriber, the CA uses cryptographic modules which meet FIPS 140-2 Level 1 certification standards.

Code Signing Certificates
Subscriber Key Pairs must be generated and protected in one of the following options:

(i) A Trusted Platform Module (TPM) that generates and secures a Key Pair and that can document the Subscriber's Private Key protection through a TPM key attestation
(ii) A hardware cryptographic module with a unit design form factor certified as conforming to at least FIPS 140 Level 2 or Common Criteria EAL 4+ certification standards.
(iii) Another type of hardware storage token with a unit design form factor of SD Card or USB token (not necessarily certified as conformant with FIPS 140 Level 2 or Common Criteria EAL 4+). The Subscriber MUST also warrant that it will keep the token physically separate from the device that hosts the code signing function until a signing session is begun.

EV Code Signing Certificates
Subscriber Key Pairs must be generated and protected in a cryptographic module that meets or exceed FIPS 140-2 Level 2 or Common Criteria EAL 4+ certification standards.

Document Signing Certificates
Subscriber Key Pairs must be generated and protected in a cryptographic module that meets or exceed FIPS 140-2 Level 2 certification standards. In the case a CA managed and hosted cryptographic module is used, the Key Pairs will be generated and protected in a cryptographic module that meets FIPS 140-2 Level 3 certification standards.

Time-Stamp Certificates
Subscriber Key Pairs must be generated and protected in a cryptographic module that meets or exceed FIPS 140-2 Level 3 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.

SSL Certificates
SSL Certificates issued on or after 1 March 2018 may have a validity period of up to, but no more than, 825-days. SSL Certificates issued on or after 1 September 2020 may have a validity period of up to, but no more than, 398-days.

EV SSL Certificates
EV SSL Certificates may have a validity period of up to, but no more than, 825-days. EV SSL Certificates issued on or after 1 September 2020 may have a validity period of up to, but no more than, 398-days.

S/MIME Certificates
S/MIME Certificates may have a validity period of up to, but no more than, 39 months.

Code Signing and EV Code Signing Certificates
Code Signing Certificates may have a validity period of up to, but no more than, 39 months.

Document Signing Certificates
Document Signing Certificates may have a validity period of up to, but no more than, 39 months.

Time-Stamp Certificates
Time-Stamp Certificates may have a validity period of up to, but no more than 135 months. Private Key usage period is 15 months.

Verified Mark Certificates
Verified Mark Certificates may have a validity period of up to, but no more than, 398-days. If the Applicant is a licensee of a Registered Mark rather than the Registrant, the expiration date of the certificate will have an expiration date that is no later than the final expiration date of the license held by the Applicant to use the Registered Mark.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

No stipulation.

6.4.2 Activation Data Protection

No stipulation.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

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

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

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

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Security Controls

6.6.1 System Development Controls

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

In the case a CA managed and hosted cryptographic module is used, the Subject of the Certificate controls the life cycle of the Key Pair. The Subject may destroy the Private Key in accordance with §6.2.10.

6.7 Network Security Controls Security Controls

The CA has implemented security controls to comply with the CA/Browser Forum's Network and Certificate System Security Requirements..

6.8 Time-stamping

Entrust provides a TSA service for use with specific products such as Code Signing and Document Signing Certificates. The TSA supports RFC 3161 "Internet X.509 Public Key Infrastructure Time-Stamp Protocol" and Microsoft Authenticode™ time-stamp requests.

Code Signing, EV Code Signing and Document Signing Certificates

Subscribers of Code Signing, EV Code Signing or Document Signing Certificates are recommended to time-stamp digital signatures when signing code or data.

Time-stamp Certificates

Times-stamp authorities (TSA), used with a Time-stamp Certificates, must meet the requirements specified in Appendix C.

7. Certificate, CRL and OCSP Profiles

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

7.1 Certificate Profile

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

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

Subscriber Certificates are issued from dedicated Subordinate CAs based on the policy identifiers listed in §7.1.6.4.

7.1.1 Version Number

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

7.1.2 Certificate Extensions

7.1.2.1 Root CA Certificate

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

7.1.2.2 Subordinate CA Certificate

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

Effective January 1, 2019, the extension requirements for extended key usage are:

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

7.1.2.3 Subscriber Certificate

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

Verified Mark Certificate

Logotype Extension (OID: 1.3.6.1.5.5.7.1.12) contains the subjectLogo with a LogotypeData element [RFC3709] containing the Mark Representation asserted by the Subject of the Verified Mark Certificate. The Mark Representation must be an embedded secured SVG image [RFC6170]. More specifically the extension must embed the image element in “data:” URL as defined in RFC6170 section 4. Further, to secure the SVG, it must use the SVG tiny profile (W3C Recommendation, "Scalable Vector Graphics (SVG) Tiny 1.2 Specification", December 2008), must not contain <script> tags, must be compressed, and must follow other requirements set forth in [RFC6170 section 5.2].

7.1.2.4 All Certificates

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

7.1.2.5 Application of RFC 5280

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

7.1.3 Algorithm Object Identifiers

7.1.3.1 SubjectPublicKeyInfo

For RSA, the CA will indicate an RSA key using the rsaEncryption (OID: 1.2.840.113549.1.1.1) algorithm identifier. The parameters must be present and must be explicit NULL.
For ECDSA, the CA must indicate an ECDSA key using the id-ecPublicKey (OID: 1.2.840.10045.2.1) algorithm identifier. The parameters must use the namedCurve encoding:

(i) For P-256 keys, the namedCurve must be secp256r1 (OID: 1.2.840.10045.3.1.7), or
(ii) For P-384 keys, the namedCurve must be secp384r1 (OID: 1.3.132.0.34).

7.1.3.2 SignatureAlgorithmIdentifier

All objects signed by a CA Private Key must conform to these requirements on the use of the AlgorithmIdentifier or AlgorithmIdentifier-derived type in the context of signatures.

For RSA, the CA must use one of the following signature algorithms and encodings.

(i) RSASSA-PKCS1-v1_5 with SHA-256
(ii) RSASSA-PKCS1-v1_5 with SHA-384
(iii) RSASSA-PKCS1-v1_5 with SHA-512

For ECDSA, the CA must use the appropriate signature algorithm and encoding based upon the signing key used.

(iv) If the signing key is P-256, the signature MUST use ECDSA with SHA-256.
(v) If the signing key is P-384, the signature MUST use ECDSA with SHA-384.
(vi) If the signing key is P-521, the signature MUST use ECDSA with SHA-512.

7.1.4 Name Forms

7.1.4.1 Name Encoding

For every valid Certification Path (as defined by RFC 5280, Section 6) for all Certificate and Subordinate CA Certificate, the following must be met:

(i) For each Certificate in the Certification Path, the encoded content of the issuer distinguished name field of a Certificate shall be byte-for-byte identical with the encoded form of the Subject distinguished name field of the issuing CA certificate.
(ii) For each CA Certificate in the Certification Path, the encoded content of the Subject distinguished name field of a Certificate shall be byte-for-byte identical among all Certificates whose Subject distinguished names can be compared as equal according to RFC 5280, Section 7.1, and including expired and revoked Certificates

7.1.4.2 Subject Information – Subscriber Certificates

Subject information must meet the requirements stated in Appendix A.

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

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

SSL, EV SSL and Verified Mark Certificates
CAs shall not issue a Certificate with a domain name containing a Reserved IP Address or Internal Name.

7.1.4.3 Subject Information – Root Certificates and Subordinate CA Certificates

Subject information must meet the requirements stated in Appendix A.

7.1.5 Name Constraints

Technically Constrained Subordinate CA Certificates are issued with an extended key usage extension. The extension will not include the anyExtendedKeyUsage key usage purpose. The extension will include one of, but will not combine the following key usage purposes: serverAuth, codesigning, emailProtection and timeStamping.

The Technically Constrained Subordinate CA Certificate will be restricted to only permit values in accordance with the included extended key usages and policies.

If the Technically Constrained Subordinate CA Certificate includes the serverAuth key usage purpose, the nameConstraints extension will include dNSName, iPAddress, DirectoryName and otherName:SRVName (1.3.6.1.5.5.7.8.7 as defined in rfc4985) as described in section 7.1.5 of the Baseline Requirements.

If the Technically Constrained Subordinate CA Certificate includes the emailProtection key usage purpose, the nameConstraints extension will include rfc882Name, with at least one name on permittedSubtrees, each name having control validated according to §3.2.2.4. The extension may include constraints on dNSName, iPAddress and DirectoryName as described in section 7.1.5 of the Baseline Requirements. The extension may include additional constraints.

7.1.6 Certificate Policy Object Identifier

7.1.6.1 Reserved Certificate Policy Identifiers

Subscriber Certificates must include one of the following reserved Certificate Policy Identifiers, if the CA is asserting the Certificate meets the associated certificate policy:

SSL Certificates	**2.23.140.1.2.2**
EV SSL Certificates	**2.23.140.1.1**
Code Signing Certificates	**2.23.140.1.4.1**
EV Code Signing Certificates	**2.23.140.1.3**
Timestamp Certificates	**2.23.140.1.4.2**
Verified Mark Certificates	**1.3.6.1.4.1.53087.1.1**

7.1.6.2 Root CA Certificates

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

7.1.6.3 Subordinate CA Certificates

Subordinate CA

Subordinate CA Certificates must include either the "any policy" certificate policy object identifier or one or more explicit certificate policy object identifiers that indicates compliance with a specific certificate policy. Certificate policy object identifiers are listed in §7.1.6.1 and §7.1.6.4.

Third Party Subordinate CA

Subordinate CA Certificates issued to a Third Party Subordinate CA must include one or more explicit certificate policy object identifiers that indicates the Third Party Subordinate CA's adherence to and compliance with the requirements documented in its CP and/or CPS. For Third Party Subordinate CAs which issue SSL Certificates, these requirements must include adherence and compliance to the Baseline Requirements.

7.1.6.4 Subscriber Certificates

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

SSL Certificates:	**2.16.840.1.114028.10.1.5**
EV SSL Certificates:	**2.16.840.1.114028.10.1.2**

Code Signing Certificates:	**2.16.840.1.114028.10.1.3**
EV Code Signing Certificates:	**2.16.840.1.114028.10.1.2**
S/MIME Certificates:	
Class 1:	**2.16.840.1.114028.10.1.4.1**
Class 2:	**2.16.840.1.114028.10.1.4.2**
Document Signing Certificates:	**2.16.840.1.114028.10.1.6**
Time-Stamp Certificates:	**2.16.840.1.114028.10.3.5**
Verified Mark Certificates	**2.16.840.1.114028.10.1.11**

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

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

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Certificate policies extension is marked Not Critical.

7.2 CRL Profile

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

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

7.2.1 Version Number

No stipulation.

7.2.2 CRL and CRL Entry Extensions

reasonCode (OID 2.5.29.21)

The CRLReason code extension is used for all revoked Certificates. The CRLReason indicated must not be unspecified (0) or certificateHold (6). This extension must not be marked critical. The most appropriate reason must be selected by the Subscriber or the CA from one the following:

(i) keyCompromise (1), if the key to the certificate has been or is suspected to be compromised
(ii) cACompromise (2), if the CA has been or is suspected to be compromised
(iii) affiliationChanged (3), if verified information in the Certificate has changed and as such the Relying Parties should no longer trust the Certificate
(iv) superseded (4), if the Certificate has been reissued, rekeys or renewed by another Certificate
(v) cessationOfOperation (5), if the application or device is no longer in service

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.

Effective 2020-09-30, if an OCSP response is for a Root CA or Subordinate CA Certificate, including Cross Certificates, and that certificate has been revoked, then the revocationReason field within the RevokedInfo of the CertStatus shall be present.

Effective 2020-09-30, the CRLReason indicated shall contain a value permitted for CRLs, as specified in §7.2.2.

7.3.1 Version Number

No stipulation.

7.3.2 OCSP Extensions

The singleExtensions of an OCSP response shall not contain the reasonCode (OID 2.5.29.21) CRL entry extension.

8. Compliance Audit and Other Assessment

8.1 Frequency or Circumstances of Assessment

CAs with unconstrained Certificates are audited for compliance with the practices and procedures set forth in the CPS in which the CA operates. 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.

CAs with Technically Constrained Subordinate CA Certificates will be audited for compliance with the practices and procedures set forth in the CPS in which the CA operates.

A CA implementation will no longer need to be audited, if all CA Certificates for the CA have expired or have been revoked before commencement of the audit period.

8.2 Identity/Qualifications of Assessor

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

i. Independence from the subject of the audit;
ii. Ability to conduct an audit that addresses the criteria of the audit schemes specified in §8.4;
iii. Employs individuals who have proficiency in examining PKI technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
iv. Licensed by WebTrust;
v. Bound by law, government regulation, or professional code of ethics; and
vi. Maintains professional liability/errors and omissions insurance policy limits of at least one million US dollars coverage.

8.3 Assessor's Relationship to Assessed Entity

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

8.4 Topics Covered by Assessment

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

i. This CPS;
ii. WebTrust Program for Certification Authorities;
iii. WebTrust Program for Baseline Requirements and Network Security;
iv. WebTrust Program for Extended Validation SSL;
v. WebTrust Program for Code Signing Baseline Requirements; and
vi. WebTrust Program for Verified Mark Certificates.

8.5 Actions Taken as a Result of Deficiency

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

8.6 Communication of Results

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

The results of the most recent compliance audit will be posted within three months from the end of the audit period to the Repository. In the event of a delay greater than three months, the CA will provide an explanatory letter signed by the qualified auditor.

The audit report will contain at least the following information:

(i) name of the organization being audited;

(ii) name and address of the organization performing the audit;
(iii) the SHA-256 fingerprint of all Roots and Subordinate CA Certificates, including Cross Certificates, that were in-scope of the audit, where the fingerprint uses uppercase letters and does not contain colons, spaces or line feeds;
(iv) audit criteria, with version number(s), that were used to audit each of the certificates (and associated keys);
(v) a list of the CA policy documents, with version numbers, referenced during the audit;
(vi) whether the audit assessed a period of time or a point in time;
(vii) the start date and end date of the Audit Period, for those that cover a period of time;
(viii) the point in time date, for those that are for a point in time; and
(ix) the date the report was issued, which will necessarily be after the end date or point in time date.

The authoritative version of the audit report must be English language, available as a PDF and text searchable for all required information.

SSL and EV SSL Certificates
For CAs which issue SSL or EV SSL Certificates, the audit results will also be posted to the CA Common Database (i.e., https://ccadb.force.com).

8.7 Self-audits

Subscriber Certificates are self-audited using post-issuance linting software limited to the linter coverage to monitor adherence to the applicable items of this CPS.

SSL and EV SSL Certificates
SSL Certificates and EV SSL Certificates are self-audited using pre-issuance linting software to monitor adherences to this CPS, the Baseline Requirements and the EV SSL Guidelines limited to the linter coverage.

Technically Constrained Subordinate CA Certificates
Entrust will monitor CAs which have been issued a Technically Constrained Subordinate CA Certificate to ensure adherence to the Subordinate CA's CPS. In addition, Entrust will review a randomly selected sample of at least three percent of the Certificates issued by the Subordinate CA on a quarterly basis.

9. Other Business and Legal Matters

9.1 Fees

Unless otherwise set out in a Subscriber Agreement, the fees for services provided by Entrust with respect to Certificates are set forth on the websites (including e-commerce sites)operated by Entrust. Unless otherwise set out in a Subscriber Agreement, these fees are subject to change, and any such changes shall become effective immediately after posting on such websites (including e-commerce sites). The fees for services provided by independent third-party RAs, Resellers and Co-marketers in respect to Certificates are set forth on the websites operated by such RAs, Resellers and Co-marketers. These fees are subject to change, and any such changes shall become effective immediately after posting on such websites.

9.1.1 Certificate Issuance or Renewal Fees

No stipulation.

9.1.2 Certificate Access Fees

No stipulation.

9.1.3 Revocation or Status Information Access Fees

No stipulation.

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

Except for a formal written Entrust refund policy, if any, neither Entrust nor any RAs operating under the CAs 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.

9.2.1 Insurance Coverage

Entrust 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

9.3.1 Scope of Confidential Information

The following information is considered confidential information of Entrust and is protected against disclosure using a reasonable degree of care:

- Private Keys;

- Activation data used to access Private Keys or to gain access to the CA system;
- Business continuity, incident response, contingency, and disaster recovery plans;
- Other security practices used to protect the confidentiality, integrity, or availability of information;
- Information held by Entrust as private information in accordance with 9.4;
- Audit logs and archive records; and
- Transaction records, financial audit records, and external or internal audit trail records and any audit reports (with the exception of an auditor's letter confirming the effectiveness of the controls set forth in this CPS).

9.3.2 Information not with the Scope of Confidential Information

Information that is included in a Certificate or a Certificate Revocation List are considered public.

9.3.3 Responsibility to Protect Confidential Information

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

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

Entrust follows the policies, statements and practices available at https://www.entrust.com/legal-compliance/privacy ("Privacy Plan") when handling personal information.

9.4.2 Information Treated as Private

Entrust 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 Plan.

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 personnel are required to protect personal information in accordance with the Privacy Plan.

9.4.5 Notice and Consent to Use Private Information

Unless otherwise stated in the CPS, Privacy Plan or other agreement (such as a Subscriber 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, 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, 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, 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, independent third-party RAs under a CA, Resellers, and Co-marketers may disclose information provided to Entrust, 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, the Certificate status will be provided by the CRL and OCSP response.

9.5 Intellectual Property Rights

Entrust retains all right, title, and interest (including all intellectual property rights), in, to and under the CPS and 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. Subject to availability, Entrust may in its discretion make copies of one or more Subordinate CA Certificate(s) available to Subscribers for use solely with the Certificate issued to such Subscribers. Entrust retains all right, title, and interest (including all intellectual property rights), in, to and under the Subordinate CA Certificate(s). Except as expressly set forth herein in Subscriber Agreement no right is or shall be deemed to be granted, whether by implication, estoppel, inference or otherwise.

9.6 Representation and Warranties

9.6.1 CA Representations and Warranties

Entrust makes the following limited warranties with respect to the operation of the CAs. A CA shall:

(i) provide CA services in accordance with the CPS;
(ii) upon receipt of a request from an RA operating under such CA, issue a Certificate in accordance with the practices and procedures set forth in the CPS;
(iii) make available Certificate revocation information by issuing Certificates and by issuing and making available Certificate CRLs and OCSP responses in a Repository in accordance with the CPS;
(iv) issue and publish Certificate CRLs and OCSP responses on a regular schedule in accordance with the CPS;
(v) provide revocation services consistent with the procedures set forth in the CPS; and
(vi) provide Repository services consistent with the practices and procedures set forth in the CPS.

In operating the CAs, Entrust may use one or more representatives or agents to perform its obligations under the CPS, any Subscriber Agreements, or any Relying Party Agreements, provided that Entrust shall remain responsible for its performance.
In no event does the Entrust 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 by any party other than Entrust 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, or (iii) non-repudiation of any Certificate or any transaction facilitated through the use of a Certificate, since such determination is a matter of applicable law.

9.6.2 RA Representations and Warranties

RAs operating under a CA shall:

(i) receive Certificate Applications in accordance with 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 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 CPS;

(iv) notify Subscribers, in accordance with the CPS, that a Certificate has been issued to them; and
(v) notify Subscribers, in accordance with the CPS that a Certificate issued to them has been revoked or will soon expire.

Entrust may use one or more representatives or agents to perform its obligations in respect of an Entrust RA under the CPS, any Subscriber Agreements, or any Relying Party Agreements, provided that Entrust shall remain responsible for the performance of such representatives or agents under the CPS, any Subscriber Agreements, or any Relying Party Agreements. Entrust 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 Subscriber Agreements, or any Relying Party Agreements. Entrust 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 Subscriber Agreements, or any Relying Party Agreements. Entrust 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 Subscriber Agreements, or any Relying Party Agreements. Entrust 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 Subscriber 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 Subscriber 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 Subscriber Agreements, and any Relying Party Agreements.

9.6.3 Subscriber representations and Warranties

As a condition of having any Certificate issued to or for Subscriber, each Subscriber (in this section, "Subscriber" includes "Applicant" when referring to any time prior to issuance of the Certificate) makes, on its own behalf and if applicable on behalf of its principal or agent under a subcontractor or hosting service relationship, the following representations, commitments, affirmations and warranties for the benefit of Certificate Beneficiaries, Entrust and any of Entrust's Affiliates that will issue Certificates to or for Subscriber:

9.6.3.1 For all Certificates:

(i) If Subscriber is applying for a Certificate to be issued to or for another Person, such Person has authorized Subscriber to act on its behalf, including to request Certificates on behalf of such Person, and to make the representations, commitments, affirmations and warranties in this §9.6.3 on behalf of such Person as well as on Subscriber's own behalf.

(ii) For clarity, Key Pairs for Code Signing and EV Code Signing Certificates, Document Signing Certificates, and Time-Stamp Certificates are required to be generated in a cryptographic module that prevents exportation or duplication and that meets or exceed the requirements as defined in §6.2.11.

(iii) All information provided, and all representations made, at all times, by Subscriber in relation to any Certificate Services, including in the Certificate request and otherwise in connection with Certificate issuance, are and will be complete, correct and accurate, including that any legal entity Subject legally exists as a valid entity in the jurisdiction of incorporation or registration specified in the Certificate (and such information and representations will be promptly updated from time to time as necessary to maintain such completeness, correctness and accuracy), and 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. For clarity, in submitting any request for a Certificate using pre-qualified information, a Subscriber is deemed to be making anew the representations, commitments, affirmations and warranties set out in this §9.6.3, and Entrust will have no obligation to issue any Certificate containing pre-qualified information if such information is subsequently found to have changed or to be in any way inaccurate, incorrect, or misleading.

(iv) The Private Key corresponding to the public key submitted to Entrust with the Certificate request was created using sound cryptographic techniques and all reasonable measures have been taken to, at all times, assure control of (and, in the case of Code Signing Certificates and EV Code Signing Certificates, sole control of), keep confidential, properly protect, and prohibit unauthorized use of, the Private Key (and any associated access or activation data or device, e.g., password or token), including, in the case of Code Signing Certificates and EV Code Signing Certificates, in accordance with the "Data Security and Private Key Protection" provisions of the Code Signing Baseline Requirements.

(v) Any device storing Private Keys will be operated and maintained in a secure manner.

(vi) A Certificate will not be installed or used until Subscriber (or, in the case of Code Signing Certificates, Subscriber's Agent) has reviewed and verified that the content of the Certificate is accurate and correct.

(vii) In the case of all Entrust SSL Certificates and EV SSL Certificates the Certificate will be installed only on servers that are accessible at the domain name (subjectAltName(s)) listed in the Certificate.

(viii) Certificates and the Private Key corresponding to the public key listed in such Certificate will only be used in compliance with all applicable laws and solely in accordance with the Subscriber Agreement, and will only be used on behalf of the organization listed as the Subject in such Certificates.

(ix) The contents of Certificates will not be improperly modified.

(x) Subscriber will notify Entrust, cease all use of the Certificate and the Private Key corresponding to the public key in the Certificate, and request the revocation of the Certificate,

a. promptly, if any information included in the Certificate or the application for a Certificate changes, is or becomes incorrect or inaccurate, or if any change in any circumstances would make the information in the Certificate misleading.
b. immediately, if there is any actual or suspected Key Compromise, or if control over the Private Key has been lost for other reasons.
c. in the case of a Code Signing Certificate or EV Code Signing Certificate, immediately, if there is evidence that the Certificate was used to sign Suspect Code.

(xi) Subscriber will promptly cease all use of the Certificate and the Private Key corresponding to the public key in such Certificate upon expiration or revocation of such Certificate.

(xii) Subscriber will immediately respond to Entrust's instructions concerning any Key Compromise or misuse or suspected misuse of a Certificate.

(xiii) Subscriber acknowledges and agrees that Entrust is entitled to revoke a Certificate immediately if:

a. Subscriber breaches the Subscriber Agreement.
b. Entrust discovers that there has been a Key Compromise of the Certificate's Private Key.
c. Revocation is required under the CPS, the Baseline Requirements, the EV SSL Guidelines, the Code Signing Baseline Requirements or the VMC Requirements.
d. Entrust discovers that the Certificate is compromised or being used for Suspect Code or the Private Key corresponding to the public key in the Certificate has been used to digitally sign Suspect Code.

(xiv) Where the Subject named in the Certificate(s) is a separate entity from the Subscriber, the Subject has authorized the inclusion of the Subject's information in the Certificate.

(xv) Subscriber owns, controls, or has the exclusive right to use the domain name or email address listed in Certificate.

(xvi) Subscriber acknowledges and agrees that Entrust is entitled to modify the Agreement when necessary to comply with any changes in Industry Standards as defined in the Subscriber Agreement.

(xvii) Subscriber will use appropriate judgment about whether it is appropriate, given the level of security and trust provided by Certificate, to use the Certificate in any given circumstance.

9.6.3.2 In addition, in the case of Code Signing Certificates and EV Code Signing Certificates,

(i) Subscriber will use commercially reasonable efforts to employ the code signing practices set out in the Code Signing Best Practices document made available https://www.entrust.com/-/media/documentation/whitepapers/code-signing-best-practices-v2.pdf or by contacting Entrust ("Code Signing Best Practices"). Without limiting the foregoing, Subscriber will as a best practice, timestamp the digital signature after digitally signing Subscriber's code.

(ii) Subscriber will generate and operate any device storing Private Keys in a secure manner, as described in the Code Signing Best Practices, and will use passwords that are randomly generated with at least 16 characters containing uppercase letters, lowercase letters, numbers, and symbols to transport Private Keys.

(iii) Subscriber will not request a Code Signing Certificate or EV Code Signing Certificate containing a public key that is, or will be used with any other type of Certificate.

(iv) The Certificate and the Private Key corresponding to the public key in such Certificate will only be used for authorized and legal purposes, and will not be used to digitally sign Suspect Code.

(v) An adequate network and other security controls will be provided to protect against misuse of the Private Key corresponding to the public key in the Certificate.

(vi) Subscriber acknowledges and agrees that Entrust is authorized to share information about the Subscriber, signed application, Certificate, and surrounding circumstances with other certification authorities or industry groups, including the CA/Browser Forum, if:

a. the Certificate or Subscriber is identified as a source of Suspect Code,
b. the authority to request the Certificate cannot be verified, or
c. the Certificate is revoked for reasons other than at Subscriber's request (e.g. as a result of Private Key compromise, discovery of malware, etc.).

(vii) Subscriber acknowledges that ASVs may independently determine that a Certificate is malicious or compromised and that ASVs and ASV products may have the ability to modify its customer experiences or "blocklist" a Code Signing Certificate or EV Code Signing Certificate without notice to Subscriber or Entrust and without regard to the revocation status of the Code Signing Certificate or EV Code Signing Certificate.

(viii) Subscriber acknowledges that (a) the CA will not provide Certificates with signing keys that are less than 2048 bits, and (b) the CA will hash the Certificate with the SHA-2 algorithm.

9.6.3.3 In addition, in the case of VMCs:

(i) Subscriber will apply for and use VMCs in accordance with and subject to the VMC Requirements.

(ii) The trademarks submitted in a VMC application represent registered trademarks that the Subscriber owns or for which it has obtained sufficient license to be able to grant the limited license in the VMC Terms, and that it will immediately revoke the VMC if it no longer owns or has a sufficient license to the applicable trademarks.

9.6.3.4 In addition, in the case of Time-Stamp Certificates, Subscriber shall use the Time-Stamp Certificate for time-stamping services only. All time-stamps must be accurate and the Subscriber accepts responsibility for any inaccuracies.

9.6.4 Relying Parties Representations and Warranties

Each Relying Party makes the following representations, commitments, affirmations and warranties:

(i) The Relying Party shall understand and, if necessary, receive proper education in the use of Public-Key cryptography and Certificates including Certificates.

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

(iii) The Relying Party shall 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) The Relying Party shall 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.

(v) 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.

(vi) the Relying Party shall not rely on a Certificate that cannot be validated back to a trustworthy root.

(vii) The Relying Party shall make its 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.

(viii) 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 an Certificate and the value of any transaction that may involve the use of a Certificate.

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

(x) With respect to SSL and EV SSL Certificates, the Relying Party shall 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 the Relying Party shall not rely on a revoked or expired Certificate.

(xi) With respect to Code Signing, EV Code Signing, S/MIME and Document Signing Certificates, the Relying Party shall trust and make use of a digital signature created using the Private Key corresponding to the Public Key listed in the Certificate only if the Certificate was not expired or revoked at the time the digital signature was created and if a proper chain of trust can be established to a trustworthy root.

(xii) With respect to Code Signing, EV Code Signing, S/MIME, Document Signing and Time-Stamp Certificates, the Relying Party shall not rely on a digital signature created using the Private Key corresponding to the Public Key listed in the Certificate if the Certificate was expired at the time the digital signature was created or if the Certificate is revoked.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

EXCEPT FOR THE LIMITED WARRANTY DESCRIBED IN §9.6.1 ABOVE, AND EXCEPT AS OTHERWISE PROVIDED IN THE SUBSCRIBER AGREEMENT, ENTRUST AND ENTRUST 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 AND ENTRUST 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, 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 AND RELIED UPON BY A RELYING PARTY. ENTRUST AND ENTRUST 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 AND ENTRUST 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 ENTRUST GROUP'S ENTIRE LIABILITY UNDER THIS CPS TO: (I) AN APPLICANT OR SUBSCRIBER IS SET OUT IN THE SUBSCRIBER AGREEMENT BETWEEN ENTRUST (OR AN ENTRUST GROUP AFFILIATE) 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.THE ENTRUST GROUP'S ENTIRE LIABILITY TO ANY OTHER PARTY IS SET OUT IN THE AGREEMENT(S) BETWEEN ENTRUST AND SUCH OTHER PARTY.

9.8.2 SUBJECT TO THE FOREGOING AND IF §9.8.1 ABOVE DOES NOT APPLY:

9.8.2.1 TO THE EXTENT ENTRUST HAS ISSUED THE CERTIFICATE(S) IN COMPLIANCE WITH THE CPS, THE ENTRUST GROUP SHALL HAVE NO LIABILITY TO ANY PERSON FOR ANY CLAIMS, DAMAGES OR LOSSES SUFFERED AS THE RESULT OF THE USE OF OR RELIANCE ON SUCH CERTIFICATE. IN NO EVENT WILL ENTRUST GROUP BE LIABLE FOR, AND CUSTOMER WAIVES ANY RIGHT IT MAY HAVE TO, ANY CONSEQUENTIAL, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE OR EXEMPLARY DAMAGES OR FOR ANY LOSS OF BUSINESS, OPPORTUNITIES, CONTRACTS, REVENUES, PROFITS, SAVINGS, GOODWILL, REPUTATION, USE, OR DATA, OR COSTS OF REPROCUREMENT OR BUSINESS INTERRUPTION, OR ANY LOSS OR DAMAGE THAT IS NOT DIRECTLY ATTRIBUTABLE TO THE USE OR RELIANCE ON A CERTIFICATE OR THE CERTIFICATE SERVICES PROVIDED UNDER THIS AGREEMENT AND THE CPS INCLUDING ANY LOSS OR DAMAGE RESULTING FROM THE COMBINATION OR INTEGRATION OF THE CERTIFICATE OR CERTIFICATE SERVICES WITH ANY SOFTWARE OR HARDWARE NOT PROVIDED BY ENTRUST IF THE LOSS OR DAMAGE WOULD NOT HAVE OCCURRED AS A RESULT OF USE OF THE CERTIFICATE OR CERTIFICATE SERVICES ALONE.

9.8.2.2 IN NO EVENT WILL ENTRUST GROUP'S TOTAL AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THE SUBCRIPTION AGREEMENT, THE CPS AND THE USE AND PERFORMANCE OF ANY PRODUCTS AND SERVICES PROVIDED HEREUNDER EXCEED THE GREATER OF ONE THOUSAND UNITED STATES DOLLARS ($1,000.00 U.S.), OR (2) THE FEES PAID BY SUCH PARTY TO ENTRUST UNDER THIS CPS DURING THE TWELVE MONTHS PRIOR TO THE INITIATION OF THE CLAIM TO A MAXIMUM OF ONE HUNDRED THOUSAND DOLLARS ($100,000.00) (EXCEPT THAT FOR ANY EV CERTIFICATES ISSUED UNDER THIS CPS, ENTRUST AND ITS ENTITIES' AGGREGATE LIABILITY TO ANY SUBSCRIBER OR RELYING PARTY IS LIMITED TO TWO THOUSAND U.S. DOLLARS (US$2,000.00) PER EV CERTIFICATE, UP TO A MAXIMUM OF ONE HUNDRED THOUSAND U.S. DOLLARS (US$100,000.00).

9.8.2.3 THE EXCLUSIONS AND LIMITS IN THIS SECTION (LIMITATIONS OF LIABILITY) APPLY: (A) REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT (INCLUDING FUNDAMENTAL BREACH), TORT (INCLUDING NEGLIGENCE), WARRANTY, BREACH OF STATUTORY DUTY, MISREPRESENTATION, STRICT LIABILITY, STRICT PRODUCT LIABILITY, OR OTHERWISE; (B) ON AN AGGREGATE BASIS, REGARDLESS OF THE NUMBER OF CLAIMS, TRANSACTIONS, DIGITAL SIGNATURES OR CERTIFICATES; (C) EVEN IF THE POSSIBILITY OF

THE DAMAGES IN QUESTION WAS KNOWN OR COMMUNICATED IN ADVANCE AND EVEN IF SUCH DAMAGES WERE FORESEEABLE; AND (D) EVEN IF THE REMEDIES FAIL OF THEIR ESSENTIAL PURPOSE. ENTRUST HAS SET ITS PRICES AND PROVIDES CERTIFICATES IN RELIANCE ON THE EXCLUSIONS AND LIMITS IN THIS SECTION (LIMITATIONS OF LIABILITY), WHICH FORM AN ESSENTIAL BASIS OF THE PROVISION OF THE SERVICES DESCRIBED IN THIS CPS.

9.8.2.4 In no event will Entrust or its Affiliates be liable to 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 related to the use or misuse of, or reliance on any Certificate issued under this CPS that: (i) has expired or been revoked; (ii) has been used for any purpose other than as set forth in this CPS or an applicable Subscriber Agreement; (iii) has been tampered with; (iv) with respect to which the key pair underlying such Certificate or the cryptography algorithm used to generate such Certificate's key pair, has been compromised by the action of any party other than Entrust or its Affiliates (including without limitation the Subscriber or Relying Party); or (v) is the subject of misrepresentations or other misleading acts or omissions of any other party, including but not limited to Subscribers and Relying Parties. Except to the extent expressly provided in this CPS or an applicable Subscriber Agreement or Relying Party Agreement, in no event shall Entrust or its Affiliates be liable to the Subscriber, Relying Party or other party for damages arising out of any claim that the content of a Certificate (including any verified marks in a VMC) infringes any patent, trademark, copyright, trade secret or other intellectual property right of any party.

9.8.2.5 Notwithstanding anything to the contrary in this Section (Limitation of Liability) or elsewhere in the Subscriber Agreement, to the extent required by applicable law Entrust neither excludes nor limits its liability for: (i) death or bodily injury caused by its own negligence; (ii) its own fraud or fraudulent misrepresentation; or (iii) other matters for which liability cannot be excluded or limited under applicable law.

9.9 Indemnities

9.9.1 Indemnification by CAs

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

9.9.2 Indemnification for Relying Parties

RELYING PARTIES SHALL INDEMNIFY AND HOLD ENTRUST GROUP AND ALL INDEPENDENT THIRD-PARTY REGISTRATION AUTHORITIES OPERATING UNDER A CERTIFICATION AUTHORITY, AND APPLICATION SOFTWARE VENDORS(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 SUBSCRIBER 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

UNLESS OTHERWISE SET OUT IN IN A SUBSCRIBER AGREEMENT SUBSCRIBERS SHALL INDEMNIFY AND HOLD ENTRUST AND ALL INDEPENDENT THIRD-PARTY REGISTRATION AUTHORITIES OPERATING UNDER A CERTIFICATION AUTHORITY, AND ALL APPLICATION SOFTWARE VENDORS(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 SUBSCRIBER 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 Subscriber Agreements, and any Relying Party

Agreements. All references to sections that survive termination of the CPS, any Subscriber 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 Subscriber Agreements, and any Relying Party Agreements.

9.11 Individual Notices and Communications with Participants

Unless otherwise set out in in a Subscriber Agreement or Relying Party Agreement, any notice to be given to Entrust under this CPS, a Subscriber Agreement, or a Relying Party Agreement shall be given in writing to the address specified in §1.5.2 by prepaid receipted mail, or overnight courier, and shall be effective as follows (i) in the case of 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 under the CPS or any Subscriber Agreement shall be given by email or by prepaid receipted mail or courier to the last address, email address for the Subscriber on file with Entrust. 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, 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 may, in its discretion, modify the CPS and the terms and conditions contained herein from time to time. Entrust shall modify the CPS to stay concurrent with the latest version of the Baseline Requirements, EV SSL Guidelines and Code Signing Baseline Requirements.

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 withdraws such modified CPS prior to such effective date. In the event that Entrust 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

No stipulation.

9.13 Dispute Resolution Provisions

Unless otherwise set out in in a Subscriber Agreement or Relying Party Agreement, any disputes between a Subscriber or an Applicant and Entrust or any third-party RAs operating under the CAs, or a Relying Party and Entrust 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 Subscriber Agreement, or any Relying Party Agreement shall preclude Entrust 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 Subscriber 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 Subscriber 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 in a Subscriber 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 Subscriber 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 Subscriber Agreements, and any Relying Party Agreements is expressly excluded. Any dispute arising out of or in respect to the CPS, any Subscriber 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

Certificates and related information may be subject to export, import, and/or use restrictions. Subscribers and Relying Parties
will comply in all respects with any and all applicable laws, rules and regulations and obtain all permits, licenses and authorizations or certificates that may be required in connection with their exercise of their rights and obligations under any part of the CPS, Subscriber Agreement, and/or Relying Party Agreement, including use or access by any of Subscriber or Relying Party's users. Without limiting the foregoing, Subscribers and Relying Parties will comply with all applicable trade control laws, including but not limited to any sanctions or trade controls of the European Union ("E.U."), Canada, the United Kingdom ("U.K."), and United Nations ("U.N."); the Export Administration Regulations administered by the U.S. Department of Commerce's Bureau of Industry and Security; U.S. sanctions regulations administered by the U.S. Treasury Department's Office of Foreign Assets Control ("OFAC"); or on the U.S. Department of Commerce Entities List ("Entities List"); and any import or export licenses required pursuant to any of the foregoing; and all applicable anti-money laundering laws, including the U.S. Bank Secrecy Act, Money Laundering Control Act, and Patriot Act, the Canadian Proceeds of Crime (Money Laundering) and Terrorist Financing Act, the U.K. Proceeds of Crime Act, and legislation implementing the International Convention on the Suppression of the Financing of Terrorism or the money laundering provisions of the U.N. transnational Organized Crime Convention. Each Subscriber and Relying Party represents and warrants that: (a) neither it nor any of its users is located in, under the control of, or a national or resident of any country to which the export of any software or technology licensed under the Agreement, or related information, would be prohibited by the applicable laws, rules or regulations of the U.S., Canada, U.K., E.U., or other applicable jurisdiction; (b) neither it nor any of its users is a Person to whom the export of any software or technology licensed under the Agreement, or related information, would be prohibited by the laws of the U.S., Canada, U.K., E.U., or other applicable jurisdiction; (c) it and each of its users has and will comply with applicable laws, rules and regulations of the U.S., Canada, U.K., E.U., or other applicable jurisdiction(s) and of any state, province, or locality or

applicable jurisdiction governing exports of any product or service provided by or through Entrust; (d) it and all its users will not use any product or service for any purposes prohibited by applicable laws, rules or regulations on trade controls, including related to nuclear, chemical, or biological weapons proliferation, arms trading, or in furtherance of terrorist financing; (e) neither it nor any of its users nor any of its affiliates, officers, directors, or employees is (i) an individual listed on, or directly or indirectly owned or controlled by, a Person (whether legal or natural) listed on, or acting on behalf of a Person listed on, any U.S, Canadian, E.U., U.K., or U.N. sanctions list, including OFAC's list of Specially Designated Nationals or the Entities List; or (ii) located in, incorporated under the laws of, or owned (meaning 50% or greater ownership interest) or otherwise, directly or indirectly, controlled by, or acting on behalf of, a person located in, residing in, or organized under the laws of any of the countries listed at https://www.entrust.com/legal-compliance/denied-parties (each of (i) and (ii), a "Denied Party"); and (f) it and each of its users is legally distinct from, and not an agent of any Denied Party. In the event any of the above representations and warranties is incorrect or the Subscriber, Relying Party or any their users engages in any conduct that is contrary to sanctions or trade controls or other applicable laws, regulations, or rules, any agreements, purchase orders, performance of services, or other contractual obligations of Entrust are immediately terminated.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

Certificates and the rights granted under the CPS, any Subscriber Agreement, or any Relying Party Agreement are personal to the Applicant, Subscriber, or Relying Party that entered into the Subscriber 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 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 Subscriber Agreement, or any Relying Party Agreement. Entrust may assign, sell, transfer, or otherwise dispose of the CPS, any Subscriber Agreements, or any Relying Party Agreements together with all of its rights and obligations under the CPS, any Subscriber 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 to which the CPS, the Subscriber 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, any third-party RAs operating under the CAs, Applicants, Subscribers, and Relying Parties, as the case may be.

The CPS, the Subscriber Agreements, and the Relying Party Agreements state all of the rights and obligations of the Entrust 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 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.

9.16.3 Severability

Whenever possible, each provision of the CPS, any Subscriber 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 Subscriber 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 Subscriber 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

In no event shall the Entrust Group be deemed in default or liable for any loss or damage resulting from the failure or delay in the performance of its obligations under the CPS, any Subscriber Agreement, or any Relying Party Agreement, arising out of or caused by, directly or indirectly, a Force Majeure Event. "Force Majeure Event" means any event or circumstance beyond Entrust Group's reasonable control, including but not limited to, floods, fires, hurricanes, earthquakes, tornados, epidemics, pandemics, other acts of God or nature, strikes and other labor disputes, failure of utility, transportation or communications infrastructures, riots or other acts of civil disorder, acts of war, terrorism (including cyber terrorism), malicious damage, judicial action, lack of or inability to obtain export permits or approvals, acts of government such as expropriation, condemnation, embargo, changes in applicable laws or regulations, and shelter-in-place or similar orders, and acts or defaults of third party suppliers or service providers.

9.17 Other Provisions

9.17.1 Conflict of Provisions

In the event of any conflict between the provisions of this CPS and the provisions of any Subscriber 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 Subscriber Agreement, or any Relying Party Agreement shall be deemed to constitute the Entrust 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 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 Subscriber 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 Group.

9.17.3 Waiver

The failure of Entrust to enforce, at any time, any of the provisions of this CPS, a Subscriber Agreement with Entrust, or a Relying Party Agreement with Entrust or the failure of Entrust 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 Subscriber Agreement with Entrust, or a Relying Party Agreement with Entrust, 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 to enforce each and every such provision thereafter. The express waiver by Entrust of any provision, condition, or requirement of this CPS, a Subscriber Agreement with Entrust, or a Relying Party Agreement with Entrust shall not constitute a waiver of any future obligation to comply with such provision, condition, or requirement.

9.17.4 Interpretation

All references in this CPS to "section" or "§" refer to the sections of this CPS unless otherwise stated. As used in this CPS, neutral pronouns and any variations thereof shall be deemed to include the feminine and masculine and all terms used in the singular shall be deemed to include the plural, and vice versa, as the context may require. The words "hereof", "herein", and "hereunder" and other words of similar import refer to this CPS as a whole, as the same may from time to time be amended or supplemented, and not to any subdivision contained in this CPS. The word "including" when used herein is not intended to be exclusive and means "including, without limitation".

Appendix A – Certificate Profiles

Root Certificate

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

Subordinate CA Certificate

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

Technically Constrained Subordinate CA Certificate

Field	Critical Extension	Content
Validity: notAfter		Not later than the notAfter of the signing certificate
Subject		Must contain countryName, organizationName and commonName
Extension: subjectKeyIdentifier	Not critical	160-bit SHA-1 hash of subjectPublicKey per RFC 5280
Extension: authorityKeyIdentifier	Not critical	Matches subjectKeyIdentifier of signing certificate
Extension: certificatePolicies	Not critical	Must contain at least one set of policyInformation containing at least a policyIdentifier
Extension: basicConstraints	Critical	cA is TRUE
Extension: keyUsage	Critical	keyCertsign and cRLSign bits are set
Extension: extKeyUsage	Not critical	Must be present per §7.1.5
Extension: nameConstraint	Critical	Must contain constraints per §7.1.5
Extension: authorityInfoAccess	Not critical	Must contain one AccessDescription with an accessMethod of ocsp and a Location of type uniformResourceIdentifier
Extension: cRLDistributionPoints	Not critical	Must have at least one DistributionPoint containing a fullName of type uniformResourceIdentifier

SSL Certificate

Field	Critical Extension	Content
Subject		Must contain countryName, localityName organizationName and commonName
Extension: subjectKeyIdentifier	Not critical	160-bit SHA-1 hash of subjectPublicKey per RFC 5280
Extension: authorityKeyIdentifier	Not critical	Matches subjectKeyIdentifier of signing certificate
Extension: certificatePolicies	Not critical	Must contain at least one set of policyInformation containing at least a policyIdentifier
Extension: basicConstraints	Critical	Empty or not present
Extension: subjectAltName	Not critical	Must contain at least one name and all names must either be of type dNSName or iPAddress
Extension: keyUsage	Critical	digitalSignature bit must be set, keyExchange may be set, other bits should not be set
Extension: extKeyUsage	Not critical	Must include serverAuth and/or clientAuth
Extension: authorityInfoAccess	Not critical	Must contain one AccessDescription with an accessMethod of caIssuers and a Location of type uniformResourceIdentifier and one AccessDescription with an accessMethod of ocsp and a Location of type uniformResourceIdentifier
Extension: cRLDistributionPoints	Not critical	Must have at least one DistributionPoint containing a fullName of type uniformResourceIdentifier

EV SSL Certificate

Field	Critical Extension	Content
Subject		Must contain countryName, localityName jurisdiction country, organizationName business category, serial number of subscriber and commonName
Extension: subjectKeyIdentifier	Not critical	160-bit SHA-1 hash of subjectPublicKey per RFC 5280
Extension: authorityKeyIdentifier	Not critical	Matches subjectKeyIdentifier of signing certificate
Extension: certificatePolicies	Not critical	Must contain at least one set of policyInformation containing at least a policyIdentifier
Extension: basicConstraints	Critical	Empty or not present
Extension: subjectAltName	Not critical	Must contain at least one name and all names must either be of type dNSName
Extension: keyUsage	Critical	digitalSignature bit must be set, keyExchange may be set, other bits should not be set
Extension: extKeyUsage	Not critical	Must include serverAuth and/or clientAuth
Extension: authorityInfoAccess	Not critical	Must contain one AccessDescription with an accessMethod of caIssuers and a Location of type uniformResourceIdentifier and one AccessDescription with an accessMethod of ocsp and a Location of type uniformResourceIdentifier
Extension: cRLDistributionPoints	Not critical	Must have at least one DistributionPoint containing a fullName of type uniformResourceIdentifier

Code Signing Certificate

Field	Critical Extension	Content
Subject		Must contain countryName, organizationName and commonName
Extension: subjectKeyIdentifier	Not critical	160-bit SHA-1 hash of subjectPublicKey per RFC 5280
Extension: authorityKeyIdentifier	Not critical	Matches subjectKeyIdentifier of signing certificate
Extension: certificatePolicies	Not critical	Must contain at least one set of policyInformation containing at least a policyIdentifier
Extension: basicConstraints	Critical	Empty or not present
Extension: keyUsage	Critical	digitalSignature bits must be set, other bits must not be set
Extension: extKeyUsage	Not critical	Must include codeSigning, other values must not be set
Extension: authorityInfoAccess	Not critical	Must contain one AccessDescription with an accessMethod of caIssuers and a Location of type uniformResourceIdentifier and one AccessDescription with an accessMethod of ocsp and a Location of type uniformResourceIdentifier
Extension: cRLDistributionPoints	Not critical	Must have at least one DistributionPoint containing a fullName of type uniformResourceIdentifier

EV Code Signing Certificate

Field	Critical Extension	Content
Subject		Must contain countryName, localityName jurisdiction country, organizationName business category, serial number of subscriber and commonName
Extension: subjectKeyIdentifier	Not critical	160-bit SHA-1 hash of subjectPublicKey per RFC 5280
Extension: authorityKeyIdentifier	Not critical	Matches subjectKeyIdentifier of signing certificate
Extension: certificatePolicies	Not critical	Must contain at least one set of policyInformation containing at least a policyIdentifier
Extension: basicConstraints	Critical	Empty or not present
Extension: keyUsage	Critical	digitalSignature bits must be set, other bits must not be set
Extension: extKeyUsage	Not critical	Must include codeSigning, other values must not be set
Extension: authorityInfoAccess	Not critical	Must contain one AccessDescription with an accessMethod of caIssuers and a Location of type uniformResourceIdentifier and one AccessDescription with an accessMethod of ocsp and a Location of type uniformResourceIdentifier
Extension: cRLDistributionPoints	Not critical	Must have at least one DistributionPoint containing a fullName of type uniformResourceIdentifier

S/MIME Class 1 Certificate

Field	Critical Extension	Content
Subject		Must include rfc822Name email address in the commonName and/or emailAddress fields
Extension: subjectKeyIdentifier	Not critical	160-bit SHA-1 hash of subjectPublicKey per RFC 5280
Extension: authorityKeyIdentifier	Not critical	Matches subjectKeyIdentifier of signing certificate
Extension: certificatePolicies	Not critical	Must contain at least one set of policyInformation containing at least a policyIdentifier
Extension: basicConstraints	Critical	Empty or not present
Extension: subjectAltName	Not critical	Must include rfc822Name email address
Extension: keyUsage	Critical	digitalSignature bit must be set, keyExchange may be set, other bits should not be set
Extension: extKeyUsage	Not critical	Must include clientAuth and/or emailProtection, may include Document Signing, other values should not be set
Extension: authorityInfoAccess	Not critical	Must contain one AccessDescription with an accessMethod of caIssuers and a Location of type uniformResourceIdentifier and one AccessDescription with an accessMethod of ocsp and a Location of type uniformResourceIdentifier
Extension: cRLDistributionPoints	Not critical	Must have at least one DistributionPoint containing a fullName of type uniformResourceIdentifier

S/MIME Class 2 Certificate

Field	Critical Extension	Content
Subject		Must contain countryName, localityName organizationName, commonName and emailAddress with rfc822Name
Extension: subjectKeyIdentifier	Not critical	160-bit SHA-1 hash of subjectPublicKey per RFC 5280
Extension: authorityKeyIdentifier	Not critical	Matches subjectKeyIdentifier of signing certificate
Extension: certificatePolicies	Not critical	Must contain at least one set of policyInformation containing at least a policyIdentifier
Extension: basicConstraints	Critical	Empty or not present
Extension: subjectAltName	Not critical	Must include rfc822Name email address
Extension: keyUsage	Critical	digitalSignature bit must be set, keyExchange may be set, other bits should not be set
Extension: extKeyUsage	Not critical	Must include clientAuth and/or emailProtection, may include Document Signing, other values should not be set
Extension: authorityInfoAccess	Not critical	Must contain one AccessDescription with an accessMethod of caIssuers and a Location of type uniformResourceIdentifier and one AccessDescription with an accessMethod of ocsp and a Location of type uniformResourceIdentifier
Extension: cRLDistributionPoints	Not critical	Must have at least one DistributionPoint containing a fullName of type uniformResourceIdentifier

Document Signing Certificate

Field	Critical Extension	Content
Subject		Must contain countryName, organizationName, and commonName
Extension: subjectKeyIdentifier	Not critical	160-bit SHA-1 hash of subjectPublicKey per RFC 5280
Extension: authorityKeyIdentifier	Not critical	Matches subjectKeyIdentifier of signing certificate
Extension: certificatePolicies	Not critical	Must contain at least one set of policyInformation containing at least a policyIdentifier
Extension: basicConstraints	Critical	Empty or not present
Extension: subjectAltName	Not critical	May contain rfc822Name email address
Extension: keyUsage	Critical	digitalSignature bit must be set, keyExchange and nonRepudiation may be set, other bits should not be set
Extension: extKeyUsage	Not critical	Must include Document Signing (Entrust) and/or Document Signing (Microsoft), other values should not be set
Extension: authorityInfoAccess	Not critical	Must contain one AccessDescription with an accessMethod of caIssuers and a Location of type uniformResourceIdentifier and one AccessDescription with an accessMethod of ocsp and a Location of type uniformResourceIdentifier
Extension: cRLDistributionPoints	Not critical	Must have at least one DistributionPoint containing a fullName of type uniformResourceIdentifier
Extension: timeStamping	Not critical	Must have at least one accessLocation containing a fullName of type uniformResourceIdentifier
Extension: Archive Rev Info	Not critical	May be provided

Time-Stamp Certificate

Field	Critical Extension	Content
Subject		Must contain countryName, organizationName and commonName
Extension: subjectKeyIdentifier	Not critical	160-bit SHA-1 hash of subjectPublicKey per RFC 5280
Extension: authorityKeyIdentifier	Not critical	Matches subjectKeyIdentifier of signing certificate
Extension: certificatePolicies	Not critical	Must contain at least one set of policyInformation containing at least a policyIdentifier
Extension: basicConstraints	Critical	Empty or not present
Extension: keyUsage	Critical	digitalSignature bits must be set, other bits must not be set
Extension: extKeyUsage	Critical	Must include timeStamping, other values must not be set
Extension: authorityInfoAccess	Not critical	Must contain one AccessDescription with an accessMethod of caIssuers and a Location of type uniformResourceIdentifier and one AccessDescription with an accessMethod of ocsp and a Location of type uniformResourceIdentifier
Extension: cRLDistributionPoints	Not critical	Must have at least one DistributionPoint containing a fullName of type uniformResourceIdentifier

Verified Mark Certificate

Field	Critical Extension	Content
Subject		Must contain countryName, localityName, streetAddress, postalCode, trademark country or region name, trademark registration number, jurisdiction country, organizationName, business category and serial number of subscriber
Extension: subjectKeyIdentifier	Not critical	160-bit SHA-1 hash of subjectPublicKey per RFC 5280
Extension: authorityKeyIdentifier	Not critical	Matches subjectKeyIdentifier of signing certificate
Extension: certificatePolicies	Not critical	Must contain at least one set of policyInformation containing at least a policyIdentifier
Extension: basicConstraints	Critical	Empty or not present
Extension: subjectAltName	Not critical	Must contain at least one name and all names must either be of type dNSName
Extension: certificate transparency	Not critical	Must include signed certificate timestamp(s)
Extension: subjectLogo	Not critical	Must contain subjectLogo per RFC 3709
Extension: keyUsage	Critical	digitalSignature bit may be set, other bits should not be set
Extension: extKeyUsage	Not critical	Must include id-kp-BrandIndicatorforMessageIdentification
Extension: authorityInfoAccess	Not critical	Must contain one AccessDescription with an accessMethod of caIssuers and a Location of type uniformResourceIdentifier and one AccessDescription with an accessMethod of ocsp and a Location of type uniformResourceIdentifier
Extension: cRLDistributionPoints	Not critical	Must have at least one DistributionPoint containing a fullName of type uniformResourceIdentifier

Appendix B – Subordinate CA Certificates

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

Subordinate CAs

Entrust 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 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 Appendix A.

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 and the Subordinate Third Party CA.

Certificate Revocation

Entrust 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 may also revoke any Subordinate CA Certificate in accordance with the agreement between Entrust 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.

Appendix C – Time-stamp Authority Requirements

Time-stamp Authorities (TSAs) used with Time-stamp Certificates must meet the requirements in the following table.

Requirement	Description
Standard	TSA must be RFC 3161 compliant
Private Key Protection	HSM meeting the minimum of FIPS 140-2 Level 3 or Common Criteria EAL 4+ (ALC_FLR.2)
Time-stamp Token Digest Algorithm	SHA-256, SHA-384 or SHA-512
Signing Process	TSA signing operations must be physically and logically protected. Any changes to its signing process must be an auditable event.
Clock Synchronization	TSA must: 1. Ensure that clock synchronization is maintained when a leap second occurs. 2. Synchronize its timestamp server at least every 24 hours with a UTC(k) time source. 3. Automatically detect and report on clock drifts or jumps out of synchronization with UTC. 4. Ensure clock adjustment of one second or greater are auditable events.
Logging	TSA must log the following information: 1. All data related to the creation of a time-stamp, including all requests for a time-stamp, the connecting IP, and results of the timestamp, 2. Physical or remote access to a time-stamp server, including the time of the access and the identity of the individual accessing the server, 3. History of the time-stamp server configuration, 4. Any attempt to delete or modify time-stamp logs, 5. Security events, including: a. Successful and unsuccessful PKI system access attempts; b. PKI and security system actions performed; c. Security profile changes; d. System crashes, hardware failures, and other anomalies; e. Firewall and router activities; and f. Entries to and exits from the CA facility 6. Revocation of a time-stamp certificate, 7. Major changes to the time-stamp server's time, 8. System startup and shutdown, and 9. Equipment failures or malfunctions. Data MUST be retained for at least seven years, except for item number 1 above which MUST be retained for a minimum of 5 days.

Time-stamp Certificate Usage	Time-Stamp Certificate shall be used for time-stamping services only. All timestamps must be accurate and the certificate subscriber accepts responsibility for any inaccuracies.
Compliance Audit	TSA may be subject to annual third-party compliance audit to ensure the TSA meets the specified requirements.

Appendix D – VMC Terms of Use ("VMC Terms")

All Mark Asserting Entities (MAEs) are required, as a condition of being issued a Verified Mark Certificate, to agree to these VMC Terms. Any and all use, display, or reliance on any Verified Mark Certificate (and any Design Mark Representation and any other data or information therein) by Consuming Entities, Relying Parties, and any other person, is subject to and conditional upon acceptance of these VMC Terms. The OID 1.3.6.1.4.1.53087.1.1 in the Verified Mark Certificate incorporates by reference these VMC Terms. If any person does not agree to these VMC Terms, such person may not obtain, use, publish, or rely upon any Verified Mark Certificate or on any Design Mark Representation or any other data or information in a Verified Mark Certificate.

1. Definitions. In addition to the other definitions included in the Baseline Requirements, EV Guidelines, and VMC Guidelines, the following capitalized words will have the meanings set out below.
   1.1. Mark Asserting Entity (MAE): An Applicant for/Subscriber of a Verified Mark Certificate.
   1.2. VMC Marks: the Design Mark Representation and Word Mark, if any, contained in a MAE's Verified Mark Certificate application.

2. Limited Right to Reproduce and Display. The MAE hereby grants, subject to the terms, conditions and restrictions in the VMC Guidelines and these VMC Terms:
   2.1. to the Issuing CA, a limited, non-exclusive, worldwide license to issue a Verified Mark Certificate that contains the VMC Marks and to log said certificate in a limited number of Certificate Transparency Logs as required by the VMC Guidelines; and
   2.2. to Consuming Entities, a limited, non-exclusive, worldwide license to reproduce, display, and modify as permitted by section 3.1 the VMC Marks only in direct visual association with communications, correspondence, or services authored or provided by the MAE from or through one of the same domains included within the Verified Mark Certificate's Subject Alternative Name field; and
   2.3. to certificate transparency log operators if different from the Issuing CA, a limited, non-exclusive, worldwide license to retain a copy of and to reproduce the Verified Mark Certificate to support a durable public record of those issued certificates, and for the purpose of permitting members of the public to audit the verification of Verified Mark Certificates.

3. License Restrictions and Conditions. Any Consuming Entity that incorporates or intends to incorporate the VMC Marks obtained through an issued and published Verified Mark Certificate into its products and services, agrees that its license to do so is subject to and conditional on the following:
   3.1. Quality Control, Same Treatment. The Consuming Entity may not distort at display time any Design Mark Representation obtained from a published Verified Mark Certificate, change its colors or background, modify its transparency, or alter it in any way other than to adjust its size or scale, or to crop it in a manner consistent with cropping performed on other Design Mark Representations displayed in the same context and where after such cropping the entire Design Mark remains visible. If a Consuming Entity displays a Word Mark obtained from a published Verified Mark Certificate, it must do so in a neutral manner applied consistently to all Word Marks from all Verified Mark Certificates that are shown in the same visual context. The Consuming Entity may display a Design Mark included in a Verified Mark Certificate without also displaying a Word Mark included in the same Verified Mark Certificate, but the Consuming Entity may not display a Word Mark included in a Verified Mark Certificate without also displaying the Design Mark included in the same Verified Mark Certificate.
   3.2. No Partnership or Relationships implied. Subject to an express agreement to the contrary between the Consuming Entity and the MAE, neither the VMC Marks nor any other content of the Verified Mark Certificate may be used or displayed in any way that reasonably implies any relationship between the Consuming Entity and the MAE, beyond the bare licensor-licensee relationship created by these VMC Terms.
   3.3. CRL or OCSP Checks. Consuming Entities must check the Certificate Revocation Lists maintained by the CA or perform an on-line revocation status check using OCSP to determine whether a Verified Mark Certificate has been revoked no less frequently than every 7 days.

3.4. Lawful Use. Consuming Entities may only use the Design Mark Representation in a Verified Mark Certificate in accordance with applicable law.

4. Sufficient Ownership or License. The MAE warrants that the VMC Marks published via a Verified Mark Certificate represent a Registered Design Mark (and Word Mark, if any) that the MAE owns or for which the MAE has obtained sufficient license to be able to grant the limited license in these VMC Terms, and that it will immediately revoke the Verified Mark Certificate if it no longer owns or has a sufficient license to the applicable Registered Design Mark (or Word Mark, if any). The MAE will defend and will be liable for any intellectual property or other claims against any Consuming Entity, Relying Party or CA that arise from the content of the MAE's application for a Verified Mark Certificate.

5. No obligation to display. The MAE acknowledges that Consuming Entities are under no obligation to display the VMC Marks in connection with content the MAE publishes that is associated with the domains the MAE owns or controls as a Domain Registrant, even if a communication or message is confirmed to be from the MAE and a suitable VMC Mark can be obtained and safely displayed from the applicable Verified Mark Certificate. Instead, Consuming Entities may choose to display the VMC Marks in accordance with these VMC Terms, or not display them, at their option.

6. Termination. Immediately upon revocation or expiration of the Verified Mark Certificate, the MAE will cease publishing or using the Verified Mark Certificate, and the license granted to Consuming Entities in Section 2.2 above shall terminate. The license to a Consuming Entity in Section 2.2 above also terminates automatically and immediately upon breach of any provision of these VMC Terms by the Consuming Entity. Consuming Entities must immediately cease any and all use of the VMC Marks upon termination of the applicable license.

7. Updates to VMC Guidelines and VMC Terms. The VMC Guidelines and VMC Terms may be updated from time to time. All parties agree that the version of the VMC Guidelines and VMC Terms in effect at the time of issuance of a Verified Mark Certificate shall apply through the date of expiration or revocation of the Verified Mark Certificate (and, for those provisions that by their nature extend beyond the date of expiration or revocation, until the provisions no longer would apply by their terms). It is the responsibility of each entity who obtains, uses, publishes or relies upon a Verified Mark Certificate to review and familiarize itself from time to time with any updated versions of the VMC Guidelines and VMC Terms.