ENTRUST CERTIFICATE SERVICES

Certification Practice Statement

for Extended Validation (EV) Certificates

Version: 2.0
July 14, 2017

Revision History

Issue	Date	Changes in this Revision
1.0	November 30, 2006	Initial version.
1.01	January 11, 2007	Initial Release
1.02	August 1, 2007	Update to implement EV Guidelines v1.0 and OCSP data requirements
1.1	September 24, 2008	Revision to routine rekey and key changeover. Other minor revisions having no substantive impact.
1.2	December 3, 2009	Revisions to add additional application software vendors and relying parties as third party beneficiaries. Deleted Subscriber notice requirements. Added Non-Commercial Entities to end-entity types. Added Certificate Profiles. Other minor revisions having no substantive impact.
1.3	February 28, 2011	Updated disaster recovery requirements and other minor changes having no substantive impact.
1.4	June 25, 2012	Update for compliance to Baseline Requirements
1.5	December 1, 2013	Update for inclusion of data controls for certificate renewal, support for smartcards, and subordinate CA certificates
1.6	March 4, 2014	Change to Loss Limitations
1.7	April 6, 2015	Updated PKI hierarchy, SHA-2, added Certificate Transparency and Certification Authority Authorization
1.8	July 6, 2015	Update for EV Code Signing
1.9	February 12, 2016	Updates for HSM criteria
2.0	February 1, 2017	Update PKI hierarchy, roots, ECC key size and certificate profiles, changes to Definitions, Disclaimers, Loss Limitations and Conflict of Provisions
2.1	July 14, 2017	Update for domain validation methods and update for CAA

TABLE OF CONTENTS

1. Introduction

Entrust Datacard Limited ("Entrust") uses Entrust's award winning Entrust Authority™ family of software products to provide standards-compliant digital certificates that enable more secure on-line communications.

The Entrust Certificate Services Certification Practice Statement for Extended Validation (EV) Certificates ("CPS") conforms to the current version of the following CA/Browser Forum documents published at http://www.cabforum.org:

- Guidelines for the Issuance and Management of Extended Validation Certificates ("EV SSL Guidelines")
- Guidelines for the Issuance and Management of Extended Validation Code Signing Certificates ("EV Code Signing Guidelines")
- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("Baseline Requirements")

Note the EV SSL Guidelines and the EV Code Signing Guidelines will be referred to collectively as the EV Guidelines.

The EV Guidelines and the Baseline Requirements describe certain of the minimum requirements that a Certification Authority (CA) must meet in order to issue Extended Validation Certificates ("EV Certificates").

Subject Organization information from valid EV SSL Certificates may be displayed in a special manner by certain relying-party software applications (e.g., browser software) in order to provide users with a trustworthy confirmation of the identity of the entity that controls the website they are accessing.

In the event of any inconsistency between this CPS and the EV Guidelines, the EV Guidelines take precedence over this CPS.

1.1 Overview

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

1.2 Identification

1.2.1 End Entity Entrust Certificates

This document is called the Entrust Certificate Services Certification Practice Statement for Extended Validation Certificates.

Each EV Certificate issued by the EV CA to a Subscriber contains an Object Identifier (OID) defined by the EV CA in the certificate's certificatePolicies extension that:

1. indicates which EV CA policy statement (i.e. this CPS) relates to that certificate,
2. asserts the EV CA's adherence to and compliance with this CPS and the EV Guidelines, and which
3. by pre-agreement with Application Software Vendors, marks the certificate as being an EV Certificate.

The following OID has been registered by the EV CA for inclusion in EV Certificates. The OID indicates the EV Certificates meet the requirements of the EV Guidelines and the Baseline Requirements:

2.16.840.1.114028.10.1.2

1.2.2 Subordinate CA Certificates

Subordinate CA Certificates issued to an Entrust CA will contain either the any policy OID or an OID identifying the specific policy for that CA.

1.3 Community and Application

1.3.1 Certification Authorities

In the EV 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 Entrust-operated RA or by an independent third-party RA operating under an EV CA. If an EV Certificate Application is verified, the verifying RA will send a request to an EV CA for the issuance of an EV Certificate. The EV CA will create an EV Certificate containing the Public Key and identification information contained in the request sent by the RA to that EV CA. The EV Certificate created in response to the request will be digitally signed by the EV CA.

The EV Certificate Authority Hierarchy consists of Roots and Issuing CAs:

Root CA:
Common Name: 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

SSL/TLS Issuing CA:
Common Name: 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
Thumbprint (SHA-1): 17 9a 76 96 db 43 22 81 3f 1c 95 72 b8 50 33 84 1d ec 02 0e

Root CA:
Common Name: 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

SSL/TLS Issuing CA:
Common Name: 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
Thumbprint (SHA-1): 17 9a 76 96 db 43 22 81 3f 1c 95 72 b8 50 33 84 1d ec 02 0e

Root CA (SHA-2):
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
SHA-1 Thumbprint: 8c f4 27 fd 79 0c 3a d1 66 06 8d e8 1e 57 ef bb 93 22 72 d4

SSL/TLS Issuing CA (SHA-2)
Entrust Certification Authority – L1M
Key Identifier: c3 f7 d0 b5 2a 30 ad af 0d 91 21 70 39 54 dd bc 89 70 c7 3a
SHA-1 Thumbprint: cc 13 66 95 63 90 65 fa b4 70 74 d2 8c 55 31 4c 66 07 7e 90

EV Code Signing Issuing CA (SHA-2)
Entrust Extended Validation Code Signing CA – EVCS1
Key Identifier: 2a 0a 6f 32 2c 29 20 21 76 6a b1 ac 8c 3c af 93 8e 0e 6b a2
SHA-1 Thumbprint: 64 b8 f1 ed ef 40 d7 d2 86 02 b6 b9 17 1a ff 11 4e 12 a6 46

Root CA (ECC):
Common Name: 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

SSL/TLS Issuing CA:
Common Name: 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
Thumbprint (SHA-1): 33 ff fe 4a 9a 16 91 e5 3e fa 15 68 eb 74 3a 69 d8 b5 2e ad

Only CAs authorized by Entrust are permitted to issue EV Certificates. In the event that more than one CA is authorized to issue EV Certificates, Entrust will post a list of authorized CAs in the Entrust Repository.

1.3.2 Registration Authorities

In the EV public-key infrastructure, RAs under the EV CAs may accept EV Certificate Applications from Applicants and perform a verification of the information contained in such EV Certificate Applications. The information provided is verified according to the procedures established by the Entrust Policy Authority, which conform to the EV Guidelines published by the CA/Browser Forum. Upon successful verification a RA operating under an EV CA may send a request to such EV CA to issue an EV Certificate to the Applicant.

Only RAs authorized by Entrust are permitted to submit requests to an EV CA for the issuance of EV Certificates.

1.3.3 End Entities

End entities for the Entrust SSL web server public-key infrastructure consist of:

1. **Applicants** - An Applicant is a Private Organization, Government Entity, Business Entity, or Non-Commercial Entity that has applied for, but has not yet been issued, an EV Certificate. Eligible Private Organizations, Government Entities, Business Entities and Non-Commercial Entities are stipulated in the EV Guidelines.
2. **Subscribers** - A Subscriber is a Private Organization, Government Entity, Business Entity, or Non-Commercial Entity that has been issued an EV Certificate.
3. **Relying Parties** – A Relying Party is a person, entity, or organization that relies on or uses an EV Certificate and/or any other information provided in an Entrust 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.

Additionally, Certificate Beneficiaries are express third party beneficiaries of this CPS and all agreements into which it is incorporated.

1.3.4 Applicability

This CPS is applicable to EV Certificates issued by EV CAs.

EV SSL Certificates

EV SSL Certificates are intended for use in establishing Web-based data communication conduits via TLS/SSL protocols. EV SSL Certificates conform to the requirements of the EV SSL Guidelines, which are based on the ITU-T X.509 v3 standard with SSL extensions.

EV Code Signing Certificates
EV Code Signing Certificates are used by content and software developers and publishers to digitally sign executables and other content. EV Code Signing Certificates conform to the requirements of the ITU-T X.509 v3 standard. The primary purpose of an 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.

1.3.4.1 Primary Purposes

EV SSL Certificates
The primary purposes of an EV SSL Certificate are to:

1. Identify the legal entity that controls a website: Provide a reasonable assurance to the user of an Internet browser that the website the user is accessing is controlled by a specific legal entity identified in the EV SSL Certificate by name, address of Place of Business, Jurisdiction of Incorporation or Registration and Registration Number or other disambiguating information; and
2. Enable encrypted communications with a website: 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 website.

EV Code Signing Certificates
EV Code Signing Certificates and signatures are intended to be used to verify the identity of the certificate holder (Subscriber) and the integrity of its code. They provide assurance to a user or platform provider that code verified with the certificate has not been modified from its original form and is distributed by the legal entity identified in the EV Code Signing Certificate by name, Place of Business address, Jurisdiction of Incorporation or Registration, and other information. EV Code Signing Certificates may help to establish the legitimacy of signed code, help to maintain the trustworthiness of software platforms, help users to make informed software choices, and limit the spread of malware. No particular software object is identified by an EV Code Signing Certificate, only its distributor is identified.

1.3.4.2 Secondary Purposes

The secondary purposes of an EV Certificate are to help establish the legitimacy of a business claiming to operate a website or distribute executable code, and to provide a vehicle that can be used to assist in addressing problems related to phishing, malware and other forms of online identity fraud. By providing more reliable third-party verified identity and address information regarding the owner of the business, EV Certificates may help to:

1. Make it more difficult to mount phishing and other online identity fraud attacks using certificates;
2. Assist companies that may be the target of phishing attacks or online identity fraud by providing them with a tool to better identify themselves to users; and
3. Assist law enforcement organizations in investigations of phishing and other online identity fraud, including where appropriate, contacting, investigating, or taking legal action against the Subject.

1.3.4.3 Excluded Purposes

EV SSL Certificates
EV SSL Certificates focus only on the identity of the Subject named in the Certificate, and not on the behavior of the Subject. As such, an EV SSL Certificate is not intended to provide any assurances, or otherwise represent or warrant:

1. That the Subject named in the EV SSL Certificate is actively engaged in doing business;
2. That the Subject named in the EV SSL Certificate complies with applicable laws;
3. That the Subject named in the EV SSL Certificate is trustworthy, honest, or reputable in its business dealings; or

4. That it is “safe” to do business with the Subject named in the EV SSL Certificate.

EV Code Signing Certificates

EV Code Signing Certificates focus only on assuring the identity of the Subscriber and that the signed code has not been modified from its original form. EV Code Signing Certificates are not intended to provide any other assurances, representations, or warranties. Specifically, EV Code Signing Certificates do not warrant that code is free from vulnerabilities, malware, bugs, or other problems. EV Code Signing Certificates do not warrant or represent that:

5. The Subject named in the EV Code Signing Certificate is actively engaged in doing business;
6. The Subject named in the EV Code Signing Certificate complies with applicable laws;
7. The Subject named in the EV Code Signing Certificate is trustworthy, honest, or reputable in its business dealings; or
8. It is “safe” to install code distributed by the Subject named in the EV Code Signing Certificate.

1.4 Contact Details

1.4.1 Specification Administration Organization

The CPS is administered by the Entrust Policy Authority; it is based on the policies established by Entrust Datacard Limited and the EV Guidelines and Baseline Requirements published by the CA/Browser Forum.

1.4.2 Contact Person

The contact information for questions about EV Certificates is:

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

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

2. General Provisions

2.1 Obligations

2.1.1 Certification Authority Obligations

An EV CA shall:

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

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

2.1.2 Registration Authority Obligations

A Registration Authority (RA) operating under an EV CA shall:

(i) receive EV Certificate Applications in accordance with the terms and conditions of the CPS;
(ii) perform, log and secure verification of information submitted by Applicants when applying for EV Certificates, and if such verification is successful, submit a request to an EV CA for the issuance of an EV Certificate, all in accordance with the terms and conditions of the CPS, which conform to the EV Guidelines published by the CA/Browser Forum;
(iii) receive and verify requests from Subscribers for the revocation of EV Certificates, and if the verification of a revocation request is successful, submit a request to an EV CA for the revocation of such EV Certificate, all in accordance with the terms and conditions of the CPS;
(iv) notify Subscribers, in accordance with the terms and conditions of the CPS, that an EV Certificate has been issued to them; and
(v) notify Subscribers, in accordance with the terms and conditions of the CPS that an EV 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-operated RA under the CPS, any Subscription Agreements, or any Relying Party Agreements, provided that Entrust shall remain responsible for the performance of such representatives or agents under the CPS, any Subscription Agreements, or any Relying Party Agreements. Entrust may appoint independent third parties to act as RAs under an EV CA. Such independent third-party RAs shall be responsible for their performance under the CPS, any Subscription Agreements, or any Relying Party Agreements. Independent third-party RAs may use one or more representatives or agents to perform their obligations when acting as a RA under an EV CA. Independent third-party RAs shall remain responsible for the performance of such representatives or agents under the CPS, any Subscription Agreements, or any Relying Party Agreements. Entrust may appoint Resellers and Co-marketers for (i) EV Certificates, and (ii) services provided in respect to EV Certificates. Such Resellers and Co-marketers shall be responsible for their performance under the CPS, any Subscription Agreements, or any Relying Party Agreements. Resellers and Co-marketers may use one or more representatives or agents to perform their obligations under the CPS, any Subscription Agreements, or any Relying Party Agreements. Resellers and Co-marketers shall remain responsible for the performance of such representatives or agents under the CPS, any Subscription Agreements, or any Relying Party Agreements. Independent third-party RAs, Resellers, and Co-marketers shall be entitled to receive all of the benefit of all (i) disclaimers of representations, warranties, and conditions, (ii) limitations of liability, (iii) representations and warranties from Applicants, Subscribers, and Relying Parties, and (iv) indemnities from Applicants, Subscribers, and Relying Parties, set forth in this CPS, any Subscription Agreements, and any Relying Party Agreements.

2.1.3 Subscriber Obligations

Subscribers and Applicants shall:

(i) understand and, if necessary, receive proper education in the use of Public-Key cryptography and Certificates including EV Certificates;
(ii) provide, in any communications with Entrust or an independent third-party RA, correct information with no errors, misrepresentations, or omissions;
(iii) generate a new, secure, and cryptographically sound Key Pair to be used in association with the Subscriber's EV Certificate or Applicant's EV Certificate Application;
(iv) read and agree to all terms and conditions of the CPS and Subscription Agreement;
(v) refrain from modifying the contents of an EV Certificate;
(vi) use EV Certificates exclusively for legal and authorized purposes in accordance with the terms and conditions of the CPS and applicable laws including, without limitation, laws relating to import, export, data protection and the right to include personal information in EV Certificates;
(vii) only use an EV Certificate on behalf of the organization listed as the Subject in such EV Certificate;
(viii) keep confidential and properly protect the Subscriber's or Applicant's Private Keys;
(ix) notify Entrust as soon as reasonably practicable of any change to any information included in the Applicant's EV Certificate Application or any change in any circumstances that would make the information in the Applicant's EV Certificate Application misleading or inaccurate;
(x) notify Entrust as soon as reasonably practicable of any change to any information included in the Subscriber's EV Certificate or any change in any circumstances that would make the information in the Subscriber's EV Certificate misleading or inaccurate;
(xi) immediately cease to use an EV Certificate if any information included in the Subscriber's EV Certificate or if a change in circumstances would make the information in the Subscriber's EV Certificate misleading or inaccurate;
(xii) notify Entrust immediately of any suspected or actual Compromise of the Subscriber's or Applicant's Private Keys and request the revocation of such EV Certificate;
(xiii) immediately cease to use the Subscriber's EV Certificate upon (a) expiration or revocation of such EV Certificate, or (b) any suspected or actual Compromise of the Private Key corresponding to the Public Key in such EV Certificate, and remove such EV Certificate from the devices and/or software in which it has been installed;
(xiv) only install the Subscriber's EV Certificate on one (1) of Subscriber's devices and only use such EV Certificate in connection with such device unless, otherwise expressly permitted by Entrust in writing;
(xv) refrain from using the Subscriber's Private Key corresponding to the Public Key in the Subscriber's EV Certificate to sign other Certificates; and
(xvi) use the Subscriber's or Applicant's own judgment about whether it is appropriate, given the level of security and trust provided by an EV Certificate, to use an EV Certificate in any given circumstance.

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

2.1.3.1 Subscriber and Applicant Representations and Warranties

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

(i) all information provided, and all representations made, by Subscriber in relation to any EV Certificates are and will be complete, accurate and truthful (and Subscriber will promptly update such information and representations from time to time as necessary to maintain such completeness and accuracy);

(ii) the Private Key corresponding to the Public Key submitted to Entrust in connection with an EV Certificate Application was created using sound cryptographic techniques and all measures necessary have been taken to maintain sole control of, keep confidential, and properly protect the Private Key (and any associated access information or device – e.g., password or token) at all times;

(iii) any information provided to Entrust or to any independent third-party RAs in connection with an EV Certificate Application does not infringe, misappropriate, dilute, unfairly compete with, or otherwise violate the intellectual property, or other rights of any person, entity, or organization in any jurisdiction;

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

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

(vi) all use of the EV Certificate and its associated Private Key shall cease immediately, and the Subscriber shall promptly notify Entrust and request the revocation of the EV Certificate, if (1) any information included in the EV Certificate changes, is or becomes incorrect or inaccurate, or if any change in any circumstances would make the information in the EV Certificate Application or EV Certificate incorrect, misleading or inaccurate; or (2) there is any actual or suspected misuse or compromise of the Private Key (or key activation data) associated with the Public Key in the EV Certificate;

(vii) all use of the (1) EV Certificate and (2) Private Key associated with the Public Key in such EV Certificate shall cease upon expiration or revocation of such EV Certificate, and such EV Certificate shall be removed from the devices and/or software in which it has been installed;

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

(ix) the subject named in the EV Certificate corresponds to the Subscriber, and that it legally exists as a valid entity in the Jurisdiction of Incorporation or Registration specified in the EV Certificates;

<u>EV SSL Certificates</u>

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

(x) the EV SSL Certificate shall be installed only on the server accessible at the domain name listed in the EV SSL Certificate, and will only be used in compliance with all applicable laws, solely for authorized company business, and solely in accordance with the Subscription Agreement and the CPS; and

(xi) the Subscriber has the exclusive right to use the domain name listed in the EV SSL Certificate;

<u>EV Code Signing Certificates</u>

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

(xii) The information provided for applications signed using an EV Code Signing Certificate such as, but not limited to, application name, information URL, and application description, shall be truthful, accurate and non-misleading;

(xiii) Subscriber shall not use the EV Code Signing Certificate to digitally sign hostile code, including spyware or other malicious software (malware) that is downloaded without user consent and Subscriber acknowledges that Entrust will revoke such Certificate if Subscriber fails to comply;

(xiv) All use of the EV Code Signing Certificate and its associated Private Key shall cease immediately, and the Subscriber shall immediately notify Entrust and request the revocation of the EV Code Signing Certificate, if there is evidence that the Certificate was used to digitally sign hostile or suspect code, including spyware or other malicious software (malware) or the code has a serious vulnerability;

(xv) Subscriber will, as a best practice, timestamp the digital signature after digitally signing Subscriber's code;

(xvi) Subscriber acknowledges that Application Software Vendor's may independently determine that an EV Code Signing Certificate is being used for malicious purposes or has been compromised and that such Application Software Vendor and Application Software Vendor products may have the ability to modify its customer experiences or "blacklist" an EV Code Signing Certificate without notice to Subscriber or Entrust and without regard to the revocation status of the EV Code Signing Certificate; and

(xvii) Subscriber acknowledges that (a) Entrust will not provide EV Code Signing Certificates with signing keys that are less than 2048 bits, and (b) Subscriber will provide SHA-2 as an option for the hashing algorithm.

2.1.3.2 Subscriber Notice Requirements

No stipulation

2.1.4 Relying Party Obligations

Relying Parties shall:

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

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

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

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

(v) make their own judgment and rely on an EV 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 an EV Certificate and the value of any transaction that may involve the use of an EV Certificate.

EV SSL Certificates

Relying Parties shall:

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

EV Code Signing Certificate

Relying Parties shall:

(v) trust and make use of a digital signature created using the Private Key corresponding to the Public Key listed in the EV Certificate only if the EV 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.

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

2.1.4.1 Relying Party Representations and Warranties

Relying Parties represent and warrant to Entrust that:

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

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

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

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

<u>EV SSL Certificates</u>

Relying Parties represent and warrant to Entrust that:

(i) the Relying Party shall not rely on a revoked or expired EV SSL Certificate;

<u>EV Code Signing Certificate</u>

Relying Parties represent and warrant to Entrust that:

(ii) the Relying Party shall not rely on a digital signature created using the Private Key corresponding to the Public Key listed in the EV Certificate if the EV Certificate was expired at the time the digital signature was created or if the Certificate is revoked.

2.1.5 Repository Obligations

An Entrust Repository shall:

(i) make available, in accordance with the terms and conditions of the CPS, EV Certificate revocation information published by an EV CA; and

(ii) make available a copy of the CPS and other information related to the products and services provided by EV CAs and any RAs operating under the EV CAs.

2.2 Liability

THE MAXIMUM CUMULATIVE LIABILITY OF THE ENTRUST GROUP TO ANY APPLICANTS, SUBSCRIBERS, RELYING PARTIES OR ANY OTHER PERSONS, ENTITIES, OR ORGANIZATIONS FOR ANY LOSSES, COSTS, EXPENSES, LIABILITIES, DAMAGES, CLAIMS, OR SETTLEMENT AMOUNTS ARISING OUT OF OR RELATING TO USE OF AN EV CERTIFICATE OR ANY SERVICES PROVIDED IN RESPECT TO ANY EV CERTIFICATES IS LIMITED BY THIS CPS. THIS CPS ALSO CONTAINS LIMITED WARRANTIES, LIMITATIONS ON LIABILITY, AND DISCLAIMERS OF REPRESENTATIONS, WARRANTIES AND CONDITIONS.

2.2.1 CA Liability

2.2.1.1 Warranties and Limitations on Warranties

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

(i) EV CAs shall provide Repository services consistent with the practices and procedures set forth in this CPS;

(ii) EV CAs shall perform EV Certificate issuance consistent with the procedures set forth in this CPS which conform to the EV Guidelines published by the CA/Browser Forum; and

(iii) EV CAs shall provide revocation services consistent with the procedures set forth in this CPS.

Notwithstanding the foregoing, 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 in the generation and storage of the Private Key corresponding to the Public Key in an EV Certificate, including, whether such Private Key has been Compromised or was generated using sound cryptographic techniques, (ii) the reliability of any cryptographic techniques or methods used in conducting any act, transaction, or process involving or utilizing an EV Certificate, (iii) any software whatsoever, or (iv) non-repudiation of any EV Certificate or any transaction facilitated through the use of an EV Certificate, since such determination is a matter of applicable law.

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

2.2.1.2 Disclaimers

EXCEPT AS SPECIFICALLY PROVIDED IN §2.2.1.1, THE ENTRUST GROUP DOES NOT MAKE ANY REPRESENTATIONS OR GIVE ANY WARRANTIES OR CONDITIONS, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND THE ENTRUST GROUP SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, WARRANTIES, AND CONDITIONS OF MERCHANTABILITY, NON-INFRINGEMENT, TITLE, SATISFACTORY QUALITY, AND/OR FITNESS FOR A PARTICULAR PURPOSE.

2.2.1.3 Loss Limitations

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

FOR GREATER CERTAINTY, ENTRUST GROUP'S ENTIRE LIABILITY UNDER THIS CPS TO: (I) AN APPLICANT OR SUBSCRIBER IS SET OUT IN THE SUBSCRIPTION AGREEMENT BETWEEN ENTRUST (OR AN AFFILIATE OF ENTRUST) 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 EV CERTIFICATE.

2.2.1.4 Other Exclusions

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

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

(vii) the EV Certificate is used other than as permitted by the CPS or is used in contravention of applicable law.

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

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

2.2.1.5 Hazardous Activities

EV Certificates and the services provided by Entrust in respect to EV Certificates are not designed, manufactured, or intended for use in or in conjunction with hazardous activities or uses requiring fail-safe performance, including the operation of nuclear facilities, aircraft navigation or communications systems, air traffic control, medical devices or direct life support machines. The Entrust Group specifically disclaims any and all representations, warranties, and conditions with respect to such uses, whether express, implied, statutory, by usage of trade, or otherwise.

2.2.2 RA Liability

The same liability provisions that apply in §2.2.1 with respect to EV CAs shall apply with respect to Entrust-operated RAs and independent third-party RAs operating under EV CAs.

2.3 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 EV Certificates or any services provided in respect to EV Certificates. Entrust makes no representations and gives no warranties or conditions regarding the financial efficacy of any transaction completed utilizing an EV Certificate or any services provided in respect to EV Certificates and the Entrust Group shall have no liability except as explicitly set forth herein in respect to the use of or reliance on an EV Certificate or any services provided in respect to EV Certificates.

2.3.1 Indemnification by Relying Parties

RELYING PARTIES SHALL INDEMNIFY AND HOLD ENTRUST AND ALL INDEPENDENT THIRD-PARTY REGISTRATION AUTHORITIES OPERATING UNDER AN EV CERTIFICATION AUTHORITY, AND ALL RESELLERS, CO-MARKETERS, AND ALL SUBCONTRACTORS, DISTRIBUTORS, AGENTS, SUPPLIERS, EMPLOYEES, AND DIRECTORS OF ANY OF THE FOREGOING (COLLECTIVELY, THE “INDEMNIFIED PARTIES”) HARMLESS FROM AND AGAINST ANY AND ALL LIABILITIES, LOSSES, COSTS, EXPENSES, DAMAGES, CLAIMS, AND SETTLEMENT AMOUNTS (INCLUDING REASONABLE ATTORNEY’S FEES, COURT COSTS, AND EXPERT’S FEES) ARISING OUT OF OR RELATING TO ANY USE OR RELIANCE BY A RELYING PARTY ON ANY EV CERTIFICATE OR ANY SERVICE PROVIDED IN RESPECT TO EV CERTIFICATES, INCLUDING (I) LACK OF PROPER VALIDATION OF AN EV CERTIFICATE BY A RELYING PARTY, (II) RELIANCE BY THE RELYING PARTY ON AN EXPIRED OR REVOKED EV CERTIFICATE, (III) USE OF AN EV CERTIFICATE OTHER THAN AS PERMITTED BY THE CPS, THE SUBSCRIPTION AGREEMENT, ANY RELYING PARTY AGREEMENT, AND APPLICABLE LAW, (IV) FAILURE BY A RELYING PARTY TO EXERCISE REASONABLE JUDGMENT IN THE CIRCUMSTANCES IN RELYING ON AN EV CERTIFICATE, OR (V) ANY CLAIM OR ALLEGATION THAT THE RELIANCE BY A RELYING PARTY ON AN EV CERTIFICATE OR THE INFORMATION

CONTAINED IN AN EV 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.

2.3.1.1 Indemnification by Subscribers

SUBSCRIBERS SHALL INDEMNIFY AND HOLD ENTRUST AND ALL INDEPENDENT THIRD-PARTY REGISTRATION AUTHORITIES OPERATING UNDER AN EV CERTIFICATION AUTHORITY, AND ALL RESELLERS, CO-MARKETERS, AND ALL SUBCONTRACTORS, DISTRIBUTORS, AGENTS, SUPPLIERS, EMPLOYEES, OR DIRECTORS OF ANY OF THE FOREGOING (COLLECTIVELY, THE "INDEMNIFIED PARTIES") HARMLESS FROM AND AGAINST ANY AND ALL LIABILITIES, LOSSES, COSTS, EXPENSES, DAMAGES, CLAIMS, AND SETTLEMENT AMOUNTS (INCLUDING REASONABLE ATTORNEY'S FEES, COURT COSTS, AND EXPERT'S FEES) ARISING OUT OF OR RELATING TO ANY RELIANCE BY A RELYING PARTY ON ANY EV CERTIFICATE OR ANY SERVICE PROVIDED IN RESPECT TO EV CERTIFICATES, INCLUDING ANY (I) ERROR, MISREPRESENTATION OR OMISSION MADE BY A SUBSCRIBER IN USING OR APPLYING FOR AN EV CERTIFICATE, (II) MODIFICATION MADE BY A SUBSCRIBER TO THE INFORMATION CONTAINED IN AN EV CERTIFICATE, (III) USE OF AN EV CERTIFICATE OTHER THAN AS PERMITTED BY THE CPS, THE SUBSCRIPTION AGREEMENT, ANY RELYING PARTY AGREEMENT, AND APPLICABLE LAW, (IV) FAILURE BY A SUBSCRIBER TO TAKE THE NECESSARY PRECAUTIONS TO PREVENT LOSS, DISCLOSURE, COMPROMISE OR UNAUTHORIZED USE OF THE PRIVATE KEY CORRESPONDING TO THE PUBLIC KEY IN SUCH SUBSCRIBER'S EV CERTIFICATE, OR (V) ALLEGATION THAT THE USE OF A SUBSCRIBER'S EV CERTIFICATE OR THE INFORMATION CONTAINED IN A SUBSCRIBER'S EV 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.

2.3.2 Fiduciary Relationships

Nothing contained in this CPS, or in any Subscription Agreement, or any Relying Party Agreement shall be deemed to constitute t 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 Subscription Agreement or any Relying Party Agreement shall confer on any Subscriber, Applicant, Relying Party, or any other third party, any authority to act for, bind, or create or assume any obligation or responsibility, or make any representation on behalf of the Entrust Group.

2.3.3 Administrative Processes

No Stipulation.

2.4 Interpretation and Enforcement

2.4.1 Governing Law

Unless otherwise set out in in a Subscription Agreement or Relying Party Agreement, the laws of the Province of Ontario, Canada, excluding its conflict of laws rules, shall govern the construction, validity, interpretation, enforceability and performance of the CPS, all Subscription Agreements and all Relying Party Agreements. The application of the United Nations Convention on Contracts for the International Sale of Goods to the CPS, any Subscription Agreements, and any Relying Party Agreements is expressly excluded. Any dispute arising out of or in respect to the CPS, any Subscription Agreement, any Relying Party Agreement, or in respect to any EV Certificates or any services provided in respect to any EV 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.

2.4.1.1 Force Majeure

The Entrust Group shall not be in default hereunder or liable for any losses, costs, expenses, liabilities, damages, claims, or settlement amounts arising out of or related to delays in performance or from failure to perform or comply with the terms of the CPS, any Subscription Agreement, or any Relying Party Agreement due to any causes beyond its reasonable control, which causes include acts of God or the public enemy, riots and insurrections, war, accidents, fire, strikes and other labor difficulties (whether or not Entrust is in a position to concede to such demands), embargoes, judicial action, failure or default of any superior CA, lack of or inability to obtain export permits or approvals, necessary labor, materials, energy, utilities, components or machinery, acts of civil or military authorities.

2.4.1.2 Interpretation

All references in this CPS to “Sections” refer to the sections of this CPS. 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.”

2.4.2 Severability, Survival, Merger, Notice

2.4.2.1 Severability

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

FOR GREATER CERTAINTY, IT IS EXPRESSLY UNDERSTOOD AND AGREED THAT EVERY PROVISION OF THE CPS, ANY SUBSCRIPTION AGREEMENTS, OR ANY RELYING PARTY AGREEMENTS THAT DEAL WITH (I) LIMITATION OF LIABILITY OR DAMAGES, (II) DISCLAIMERS OF REPRESENTATIONS, WARRANTIES, CONDITIONS, OR LIABILITIES, OR (III) INDEMNIFICATION, IS EXPRESSLY INTENDED TO BE SEVERABLE FROM ANY

OTHER PROVISIONS OF THE CPS, ANY SUBSCRIPTION AGREEMENTS, OR ANY RELYING PARTY AGREEMENTS AND SHALL BE SO INTERPRETED AND ENFORCED.

2.4.2.2 Survival

The provisions of the section entitled "Definitions" and sections 2.1.3.1, 2.1.4.1, 2.2, 2.3, 2.4, 2.8, 2.9, 3.1.5, 3.1.6, 4.6 and 8.1 shall survive termination or expiration of the CPS, any Subscription Agreements, and any Relying Party Agreements. All references to sections that survive termination of the CPS, any Subscription Agreements, and any Relying Party Agreements, shall include all sub-sections of such sections. All payment obligations shall survive any termination or expiration of the CPS, any Subscription Agreements, and any Relying Party Agreements.

2.4.2.3 Merger

The CPS, the Subscription 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.

2.4.2.4 Conflict of Provisions

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

2.4.2.5 Waiver

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

2.4.2.6 Notice

Any notice to be given by a Subscriber, Applicant, or Relying Party to Entrust under this CPS, a Subscription Agreement, or a Relying Party Agreement shall be given in writing to the address specified in §1.4 by prepaid receipted mail, facsimile, or overnight courier, and shall be effective as follows (i) in the case of facsimile or courier, on the next Business Day, and (ii) in the case of receipted mail, five (5) Business Days following the date of deposit in the mail. Any notice to be given by Entrust under the CPS, any Subscription Agreement, or any Relying Party Agreement shall be given by email or by facsimile or courier to the last address, email address or facsimile number for the Subscriber on file with Entrust. In the event of notice by email, the notice shall become effective on the next Business Day. In the event of notice by prepaid receipted mail, facsimile, or overnight courier, notice shall become effective as specified in (i) or (ii), depending on the means of notice utilized.

2.4.2.7 Assignment

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

2.4.3 Dispute Resolution Procedures

Any disputes between a Subscriber or an Applicant and Entrust or any third-party RAs operating under the Entrust CAs, or a Relying Party and Entrust or any third-party RAs operating under the Entrust CAs, shall be submitted to mediation in accordance with the Commercial Mediation Rules of the American Arbitration Association which shall take place in English in Ottawa, Ontario. In the event that a resolution to such dispute cannot be achieved through mediation within thirty (30) days, the dispute shall be submitted to binding arbitration. The arbitrator shall have the right to decide all questions of arbitrability. The dispute shall be finally settled by arbitration in accordance with the rules of the American Arbitration Association, as modified by this provision. Such arbitration shall take place in English in Ottawa, Ontario, before a sole arbitrator appointed by the American Arbitration Association (AAA) who shall be appointed by the AAA from its Technology Panel and shall be reasonably knowledgeable in electronic commerce disputes. The arbitrator shall apply the laws of the Province of Ontario, without regard to its conflict of laws provisions, and shall render a written decision within thirty (30) days from the date of close of the arbitration hearing, but no more than one (1) year from the date that the matter was submitted for arbitration. The decision of the arbitrator shall be binding and conclusive and may be entered in any court of competent jurisdiction. In each arbitration, the prevailing party shall be entitled to an award of all or a portion of its costs in such arbitration, including reasonable attorney's fees actually incurred. Nothing in the CPS, or in any Subscription Agreement, or any Relying Party Agreement shall preclude Entrust or any third-party RAs operating under the Entrust CAs from applying to any court of competent jurisdiction for temporary or permanent injunctive relief, without breach of this §2.4.3 and without any abridgment of the powers of the arbitrator, with respect to any (i) alleged Compromise that affects the integrity of an EV Certificate, or (ii) alleged breach of the terms and conditions of the CPS, any Subscription Agreement, or any Relying Party Agreement. The institution of any arbitration or any action shall not relieve an Applicant, Subscriber or Relying Party of its obligations under the CPS, any Subscription Agreement, or any Relying Party Agreement.

2.4.3.1 Limitation Period on Arbitrations and Actions

Any and all arbitrations or legal actions in respect to a dispute that is related to an EV Certificate or any services provided in respect to an EV Certificate shall be commenced prior to the end of one (1) year after (i) the expiration or revocation of the EV Certificate in dispute, or (ii) the date of provision of the disputed service or services in respect to the EV Certificate in dispute, whichever is sooner. If any arbitration or action in respect to a dispute that is related to an EV Certificate or any service or services provided in respect to an EV 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.

2.5 Fees

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

2.5.1 Certificate Issuance or Renewal Fees

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

2.5.2 Certificate Access Fees

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

2.5.3 Revocation or Status Information Access Fees

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

2.5.4 Fees for Other Services such as Policy Information

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

2.5.5 Refund Policy

Neither Entrust nor any RAs operating under the Entrust CAs nor any Resellers or Co-Marketers provide any refunds for EV Certificates or services provided in respect to EV Certificates.

2.6 Publication and Repositories

Entrust maintains the Entrust Repository to store various information related to EV Certificates and the operation of EV CAs, Entrust RAs, and third-party RAs operating under the EV CAs. The CPS and various other related information is published in the Entrust Repository. The CPS is also available from Entrust in hard copy upon request.

2.6.1 Publication of CA Information

The following EV Certificate information is published in the Entrust Repository:

(i) the CPS;
(ii) information and agreements regarding the subscription for and reliance on EV Certificates; and
(iii) revocations of EV Certificates performed by an EV CA, published in a Certificate Revocation List (CRL).

The data formats used for EV Certificates and for Certificate Revocation Lists in the Entrust Repository are in accordance with the associated definitions in §7.

2.6.2 Frequency of Publication

The CPS may be re-issued and published in accordance with the policy set forth in §8.

2.6.3 Access Controls

The CPS is published in the Entrust Repository. The CPS will be available to all Applicants, Subscribers and Relying Parties, but may only be modified by the Entrust Policy Authority.

2.6.4 Repositories

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

2.7 Compliance Audit

This sub-section describes the stipulations with respect to audit by an independent third party. In addition to these audits, the EV CAs strictly control service quality by performing ongoing self-audits as prescribed in the EV Guidelines.

2.7.1 Frequency of Entity Compliance Audit

EV CAs, Entrust-operated RAs, and independent third-party RAs operating under the EV CAs shall be audited once per calendar year for compliance with the practices and procedures set forth in the CPS. If the results of an audit report recommend remedial action, Entrust or the applicable independent third-party RA shall initiate corrective action within thirty (30) days of receipt of such audit report.

2.7.2 Identity/Qualifications of Auditor

The compliance audit of Entrust CAs shall be performed by a certified public accounting firm with a demonstrated competency in the evaluation of CAs and RAs and that meets the requirements of the EV Guidelines.

2.7.3 Auditor’s Relationship to Audited Party

The certified public accounting firm selected to perform the compliance audit for the EV CAs, Entrust-operated RAs, or independent third-party operated RAs under the Entrust CAs shall be independent from the entity being audited.

2.7.4 Topics Covered by Audit

The compliance audit shall test compliance of EV CAs, Entrust-operated RAs, or independent third-party operated RAs under the Entrust CAs against the policies and procedures set forth in:

i. the CPS;
ii. the WebTrust Program for CAs; and
iii. the WebTrust EV Program.

2.7.5 Actions Taken as a Result of Deficiency

Upon receipt of a compliance audit that identifies any deficiencies, the audited EV CA, Entrust-operated RA, or independent third-party operated RA under an EV CA shall use commercially reasonable efforts to correct any such deficiencies in an expeditious manner.

2.7.6 Communication of Results

The results of all compliance audits shall be communicated, in the case of EV CAs, to the Entrust Policy Authority, and, in the case of any Entrust-operated RAs under an EV CAs, to the Entrust Policy Authority, and in the case of third-party RAs operating under an EV CA, to the operational authority for such RA.

The results of the most recent compliance audit will be posted to the Repository.

2.8 Confidentiality

Neither Entrust nor any independent third-party RAs operating under the Entrust CAs, nor any Resellers or Co-Marketers shall disclose or sell Applicant or Subscriber names (or other information submitted by an

Applicant or Subscriber when applying for an EV Certificate), except in accordance with this CPS, a Subscription Agreement, or a Relying Party Agreement. Entrust and all independent third-party RAs operating under the Entrust CAs, and all Resellers and Co-Marketers shall use a commercially reasonable degree of care to prevent such information from being used or disclosed for purposes other than those set forth in the CPS, a Subscription Agreement, or a Relying Party Agreement. Notwithstanding the foregoing, Applicants and Subscribers acknowledge that some of the information supplied with an EV Certificate Application is incorporated into EV Certificates and that Entrust and all independent third-party RAs operating under the Entrust CAs, and all Resellers and Co-Marketers shall be entitled to make such information publicly available.

2.8.1 Types of Information to be Kept Confidential

Information that is supplied by Applicants, Subscribers, or Relying Parties for the subscription for, use of, or reliance upon an EV Certificate, and which is not included in the information described in §2.8.2 below, shall be considered to be confidential. Entrust and independent third-party RAs under the Entrust CAs shall be entitled to disclose such information to any subcontractors or agents that are assisting Entrust in the verification of information supplied in EV Certificate Applications or that are assisting Entrust in the operation of the EV CAs or Entrust-operated RAs. Information considered to be confidential shall not be disclosed unless compelled pursuant to legal, judicial, or administrative proceedings, or otherwise required by law. Entrust and independent third-party RAs under the Entrust CAs shall be entitled to disclose information that is considered to be confidential to legal and financial advisors assisting in connection with any such legal, judicial, administrative, or other proceedings required by law, and to potential acquirors, legal counsel, accountants, banks and financing sources and their advisors in connection with mergers, acquisitions, or reorganizations.

2.8.2 Types of Information not Considered Confidential

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

2.8.3 Disclosure of Certificate Revocation/Suspension Information

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

2.8.4 Release to Law Enforcement Officials

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

2.8.5 Release as Part of Civil Discovery

Entrust, independent third-party RAs under an EV 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.

2.8.6 Disclosure Upon Owner's Request

Entrust, independent third-party RAs under an EV 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.

2.8.7 Other Information Release Circumstances

No stipulation.

2.9 Intellectual Property Rights

Entrust retains all right, title, and interest (including all intellectual property rights), in, to and under all EV Certificates, except for any information that is supplied by an Applicant or a Subscriber and that is included in an EV Certificate, which information shall remain the property of the Applicant or Subscriber. All Applicants and Subscribers grant to Entrust and any RAs operating under the Entrust CAs a non-exclusive, worldwide, paid-up, royalty-free license to use, copy, modify, publicly display, and distribute such information, by any and all means and through any and all media whether now known or hereafter devised for the purposes contemplated under the CPS, the Subscriber's Subscription Agreement, and any Relying Party Agreements. Entrust and any RAs operating under the Entrust CAs shall be entitled to transfer, convey, or assign this license in conjunction with any transfer, conveyance, or assignment as contemplated in §2.4.2.7. Entrust grants to Subscribers and Relying Parties a non-exclusive, non-transferable license to use, copy, and distribute EV Certificates, subject to such EV Certificates being used as contemplated under the CPS, the Subscriber's Subscription Agreement, and any Relying Party Agreements, and further provided that such EV Certificates are reproduced fully and accurately and are not published in any publicly available database, repository, or directory without the express written permission of Entrust. Except as expressly set forth herein, no other right is or shall be deemed to be granted, whether by implication, estoppel, inference or otherwise. Subject to availability, Entrust may in its discretion make copies of one or more Cross Certificate(s) available to Subscribers for use solely with the EV Certificate issued to such Subscribers. Entrust retains all right, title, and interest (including all intellectual property rights), in, to and under the Cross Certificate(s).

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

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

3 Identification and Authentication

3.1 Initial Registration

Before issuing an EV Certificate, the EV CAs ensure that all Subject organization information in the EV Certificate conforms to the requirements of, and has been verified in accordance with, the procedures prescribed in this CPS and the EV Guidelines published by the CA/Browser Forum and matches the information confirmed and documented by the RA pursuant to its verification processes. Such verification processes are intended 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 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 Subscription Agreement; and
  c. Verify that a Certificate Approver has signed or otherwise approved the EV Certificate Request.

<u>EV SSL Certificate</u>

(iii) Verify the Applicant is a registered holder or has exclusive control of the domain name to be included in the EV SSL Certificate.

3.1.1 Types of Names

The Subject names in an EV Certificate comply with the X.500 Distinguished Name (DN) form. EV CAs shall use a single naming convention as set forth in the EV Guidelines and the Baseline Requirements published by the CA/Browser Forum.

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, and/or URL 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.

Application Note: Above general prohibition naturally also covers the case when the certificate can be used for Man in the Middle insertion or Traffic Interception and Management.

<u>EV SSL Certificates</u>

The value of the Common Name to be used in an EV 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 EV SSL Certificate.

<u>EV Code Signing Certificates</u>

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

3.1.3 Rules for Interpreting Various Name Forms

Subject names for EV Certificates shall be interpreted as set forth in §3.1.1 and §3.1.2.

3.1.4 Uniqueness of Names

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

3.1.5 Name Claim Dispute Resolution Procedure

The Subject names in EV Certificates are issued on a "first come, first served" basis. By accepting a Subject name for incorporation into an EV Certificate, a RA operating under an EV 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 Entrust CAs and any RAs operating under the Entrust CAs neither act as an arbitrator nor provide any dispute resolution between Subscribers or between Subscribers and third-party complainants in respect to the use of any information in an EV Certificate. The CPS does not bestow any procedural or substantive rights on any Subscriber or third-party complainant in respect to any information in an EV Certificate. Neither the Entrust CAs nor any RAs operating under the Entrust 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 an EV CA or a RA operating under an EV CA or between a third-party complainant and an EV CA or a RA operating under an EV CA arising out of any information in an EV Certificate. EV CAs and RAs operating under EV CAs shall respectively have the right to revoke and the right to request revocation of EV Certificates upon receipt of a properly authenticated order from an arbitrator or court of competent jurisdiction requiring the revocation of an EV Certificate.

3.1.6 Recognition, Authentication and Role of Trademarks

An EV CA or a RA operating under an EV CA may, in certain circumstances, take action in respect to an EV Certificate containing information that possibly violates the trademark rights of a third-party complainant. In the event that a third-party complainant provides an EV CA or a RA operating under an EV 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 EV Certificate in dispute, stating that the complainant believes that information in the Subscriber's EV 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 EV Certificate in dispute, an EV CA or a RA operating under an EV CA may initiate the following actions. The EV CA or the RA operating under an EV CA may determine whether the issue date of the Subscriber's EV Certificate predates the registration date on the trademark registration provided by the complainant. If the date of issuance of the Subscriber's EV Certificate predates the trademark registration date, the EV CA or the RA operating under the EV 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 EV Certificate is after the registration date on the trademark registration provided by the complainant, the EV CA or the RA operating under the EV 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 EV CA or the RA operating under the EV 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 EV CA and the RAs operating under that EV CA respectively may revoke or may request revocation of the disputed EV 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 EV Certificate, and if the party instigating the litigation provides an EV CA or a RA operating under an EV CA with a copy of the file-stamped complaint or statement of claim, the EV CA will maintain the current status of the EV Certificate or the RA operating under the EV CA will request that the EV CA maintain the current status of the EV Certificate, subject to any requirements to change the status of such EV Certificate otherwise provided or required under this CPS, a Subscription Agreement, or any Relying Party Agreement. During any litigation, an EV CA will not revoke and a RA operating under an EV CA will not request revocation of an EV Certificate that is in dispute unless ordered by an arbitrator or a court of competent jurisdiction or as otherwise provided or required under this CPS, a Subscription Agreement, or any Relying Party Agreement. In the event of litigation as contemplated above, EV CAs and RAs operating under the EV CAs will comply with any directions by a court of competent jurisdiction in respect to an EV 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 an EV Certificate, Entrust and/or any third party operating a RA under an EV 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 an EV Certificate shall remain subject to all of the terms and conditions of the CPS, the Subscriber's Subscription Agreement, and the Relying Party's Relying Party Agreement.

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

3.1.7 Method to Prove Possession of Private Key

RAs 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 EV Certificate Application.

3.1.8 Authentication of Organizational Identity

RAs operating under the EV CAs shall perform a verification of any organizational identities that are submitted by an Applicant or Subscriber. RAs operating under the EV CAs shall determine whether the organizational identity, legal existence, physical existence, operational existence, and domain name provided with an EV Certificate Application are consistent with the requirements set forth in the EV Guidelines published by the CA/Browser Forum. The information and sources used for the verification of EV Certificate Applications may vary depending on the jurisdiction of the Applicant or Subscriber.

The Entrust Policy Authority may, in its discretion, update verification practices to improve the organization identity verification process. Any changes to verification practices shall be published pursuant to the standard procedures for updating the CPS.

3.1.9 Authentication of Individual Identity

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

The Entrust Policy Authority may, in its discretion, update verification practices to improve the individual identity verification process. Any changes to verification practices shall be published pursuant to the standard procedures for updating the CPS.

3.1.10 Authentication of Domain Name

EV CAs shall confirm that, as of the date the EV SSL Certificate issues, either the CA or the RA validated each Fully-Qualified Domain Name (FQDN) listed in the 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 EV SSL Certificates over time. For purposes of domain validation, the term Applicant includes the Applicant's Parent Company, Subsidiary Company, or Affiliate.

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

3.1.10.1 Validating the Applicant as a Domain Contact

Confirming the Applicant's control over the FQDN by validating the Applicant is the Domain Contact directly with the Domain Name Registrar. This method may only be used if:

1. The EV CA authenticates the Applicant's identity under § 3.1.8 or 3.1.9 and the authority of the Applicant Representative through a reliable method of communication, OR
2. The EV CA is also the Domain Name Registrar, or an Affiliate of the Registrar, of the Base Domain Name.

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

Confirming 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 Authorization Domain Names.

The EV 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 shall be unique in each email, fax, SMS, or postal mail.

The EV 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.

3.1.10.3 Phone Contact with Domain Contact

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

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

3.1.10.4 Constructed Email to Domain Contact

Confirming 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 Authorization Domain Name, (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 Authorization Domain Name used in the email is an Authorization Domain Name 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.

3.1.10.5 Domain Authorization Document

No stipulation.

3.1.10.6 Agreed-Upon Change to Website

Confirming the Applicant's control over the FQDN by confirming one of the following under the "/.well-known/pki-validation" directory, or another path registered with IANA for the purpose of Domain Validation, on the Authorization Domain Name that is accessible by the CA via HTTP/HTTPS over an Authorized Port:

1) The presence of Required Website Content contained in the content of a file or on a web page in the form of a meta tag. The entire Required Website Content must not appear in the request used to retrieve the file or web page, or
2) The presence of the Request Token or Request Value contained in the content of a file or on a webpage in the form of a meta tag where the Request Token or Random Value must not appear in the request.

If a Random Value is used, the EV CA or RA shall provide a Random Value unique to the EV Certificate request and shall not use the Random Value after the longer of (i) 30 days or (ii) if the Applicant submitted the Certificate request, the timeframe permitted for reuse of validated information relevant to the EV Certificate (such as in Section 11.14.3 of the EV Guidelines).

3.1.10.7 DNS Change

Confirming the Applicant's control over the requested FQDN by confirming the presence of a Random Value in a DNS TXT record for an Authorization Domain Name or an Authorization Domain Name that is prefixed with a label that begins with an underscore character.

If a Random Value is used, the EV 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.

3.1.10.8 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 Section 3.2.2.5 of the Baseline Requirements.

Once the FQDN has been validated using this method, the EV CA may not also issue EV 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.

3.1.10.9 Test Certificate

No stipulation

3.1.10.10 TLS Using a Random Number

No stipulation

3.1.11 Accuracy of Information

To ensure the accuracy of the information and to ensure that no misleading information is included in the Certificate, each verification shall be validated by a verification manager before the information can be used to issue a Certificate.

3.2 Routine Rekey

Each EV 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 EV Certificate Application, Entrust recommends that a new Key Pair be generated and that the new Public Key of this Key Pair be submitted with the Applicant's EV Certificate Application. If a Subscriber wishes to continue to use an EV Certificate beyond the expiry date for the current EV Certificate, the Subscriber must obtain a new EV Certificate and replace the EV Certificate that is about to expire. Subscribers submitting a new EV Certificate Application will be required to complete the initial application process, as described in §4.1. The RA will perform verification of the information submitted with the EV Certificate Application as described in §3.1.8 and §3.1.9 only if verification has not been performed for that Subscriber within the previous 1-year period. The Subscriber may request a replacement certificate using an existing key pair.

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

3.3 Rekey After Revocation

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

3.4 Revocation Request

A Subscriber may request revocation of their EV Certificate at any time provided that the Subscriber can validate to the RA that processed the Subscriber's EV Certificate Application that the Subscriber is the organization to whom the EV Certificate was issued. The RA shall authenticate a request from a Subscriber for revocation of their EV 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 §4.4.

Subscribers, Relying Parties, Application Software Suppliers, Anti-Malware Organizations and other third parties may report Certificate misuse or other types of fraud, compromise misuse or inappropriate conduct related to Certificates by contacting the Registration Authority or submitting notification through the online form, https://www.entrust.net/ev/misuse.cfm.

4 Operational Requirements

4.1 Certificate Application

To obtain an EV Certificate, an Applicant must:

(i) generate a secure and cryptographically sound Key Pair,
(ii) agree to all of the terms and conditions of the CPS and the Subscription Agreement, and
(iii) complete and submit an EV Certificate Application, providing all information requested by an Entrust-operated RA or by an independent third-party RA under an EV CA (a "Registration Authority") without any errors, misrepresentation, or omissions.

The following Applicant roles (refer to the EV Guidelines for a definition of each role) are required for the issuance of an EV Certificate:

Certificate Requester – The EV certificate request must be signed and submitted by an authorized Certificate Requester.
Certificate Approver – The EV certificate request must be reviewed and approved by an authorized Certificate Approver.
Contract Signer – A Subscription Agreement applicable to the requested EV 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.

Upon an Applicant's completion of the EV Certificate Application and acceptance of the terms and conditions of this CPS and the Subscription Agreement, an Entrust-operated RA or an independent third-party RA operating under an EV CA shall follow the procedures described in Sections 3.1.8 and 3.1.9 to perform verification of the information contained in the EV Certificate Application. If the verification performed by a RA is successful, the RA may, in its sole discretion, request the issuance to the Applicant of an EV Certificate from an EV CA. If a RA refuses to request the issuance of an EV 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 EV Certificate Application.

In the event of successful verification of an EV Certificate Application, the RA shall submit a request to an EV CA for the issuance of an EV Certificate and shall notify the Applicant by email once an EV Certificate has been issued by the EV CA. The Applicant will be provided with a URL that can be used to retrieve the EV Certificate.

4.1.1 Certification Authority Authorization

This section is effective as of September 8, 2017.

Prior to issuing Entrust EV SSL Certificates, EV CAs will check for certification authority authorization (CAA) records for each dNSName in the subjectAltName extension of the Entrust EV SSL Certificate to be issued, according to the procedure in RFC 6844, following the processing instructions set down in RFC 6844 for any records found. If the EV SSL Certificate is issued, it will be issued within the TTL of the CAA record, or 8 hours, whichever is greater.

When processing CAA records, Entrust Certification Authorities must process the issue, issuewild, and iodef property tags as specified in RFC 6844. Entrust Certification Authority may not act on the contents of the iodef property tag. Entrust Certification Authorities shall respect the critical flag and will not issue an EV SSL Certificate if they encounter an unrecognized property with this flag set.

Entrust Certification Authorities may not check CAA records for the following exceptions:

(i) CAA checking is optional 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) CAA checking is optional for Certificates issued by a Technically Constrained Subordinate CA Certificate as set out in Baseline Requirements section 7.1.5, where the lack of CAA checking is an explicit contractual provision in the contract with the Applicant.
(iii) CAA checking is optional if the CA or an Affiliate of the CA is the DNS Operator (as defined in RFC 7719) of the domain's DNS.

Entrust Certification Authority may treat a record lookup failure as permission to issue if:

(iv) the failure is outside the CA's infrastructure;
(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.

Entrust Certification Authority shall document 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. Entrust Certification Authorities will support mailto: and https: URL schemes in the iodef record.

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

4.2 Certificate Issuance

Upon receipt of a request from a RA operating under an EV CA, the EV 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 EV 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 EV CA may generate and digitally sign an EV Certificate in accordance with the Certificate profile described in §7.

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

4.2.1 Circumstances for Certificate Renewal

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

4.2.2 Who May Request Renewal

Subscribers or Subscriber agents may request renewal of Entrust Certificates.

4.2.3 Processing Certificate Renewal Requests

Entrust CAs or RAs will process certificate renewal requests with validated verification data. Verification data which was validated within the last twelve months may be used.

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

4.2.4 Notification of New Certificate Issuance to Subscriber

Entrust CAs or RAs will provide Entrust 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 Entrust Certificates.

4.2.5 Conduct Constituting Acceptance of a Renewal Certificate

No stipulation.

4.2.6 Publication of the Renewal Certificate by the CA

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

4.2.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.3 Certificate Acceptance

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

4.4 Certificate Suspension and Revocation

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

EV CAs do not allow the suspension of EV Certificates.

4.4.1 Circumstances for Revocation

An EV CA shall be entitled to revoke and may revoke, and a RA operating under an EV CA shall be entitled to request revocation of and shall request revocation of, a Subscriber's EV Certificate if such EV CA or RA has knowledge of or a reasonable basis for believing that of any of the following events have occurred:

(i) Compromise of such EV CA's Private Key or Compromise of a superior CA's Private Key;

(ii) breach by the Subscriber of any of the terms of the CPS or the Subscriber's Subscription Agreement;

(iii) any change in the information contained in an EV Certificate issued to a Subscriber;

(iv) non-payment of any EV Certificate fees or service fees;

(v) a determination that an EV Certificate was not issued in accordance with the requirements of the CPS or the Subscriber's Subscription Agreement;

(vi) the EV CA receives notice or otherwise becomes aware that a court or arbitrator has revoked a Subscriber's right to use the domain name listed in the EV Certificate, or that the Subscriber has failed to renew its domain name;

(vii) the EV CA receives notice or otherwise becomes aware that a Subscriber has been added as a denied party or prohibited person to a blacklist, or is operating from a prohibited destination under the laws of the EV CA's jurisdiction of operation as described in §2.4;

(viii) the EV CA ceases operations for any reason or the EV CA's right to issue EV Certificates expires or is revoked or terminated and the EV CA has not arranged for another EV CA to provide revocation support for the EV Certificates;

(ix) an EV Code Signing Certificate is used to digitally sign hostile code, including spyware or other malicious software (malware); or

(x) any other reason that may be reasonably expected to affect the integrity, security, or trustworthiness of an EV Certificate or an EV CA.

A Subscriber shall request revocation of their EV 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 EV Certificate request was not authorized and such authorization will not be retroactively granted;
(iii) change in the information contained in the Subscriber's EV Certificate;
(iv) change in circumstances that cause the information contained in Subscriber's EV Certificate to become inaccurate, incomplete, or misleading.

Such revocation request shall be submitted by the Subscriber to the RA that processed the Subscriber's EV Certificate Application. If a Subscriber's EV Certificate is revoked for any reason, the RA that processed the Subscriber's EV Certificate Application shall make a commercially reasonable effort to notify such Subscriber by sending an email to the technical and security contacts listed in the EV Certificate Application. Revocation of an EV Certificate shall not affect any of the Subscriber's contractual obligations under this CPS, the Subscriber's Subscription Agreement, or any Relying Party Agreements.

4.4.2 Who Can Request Revocation

A Subscriber may request revocation of their EV Certificate at any time for any reason. If a Subscriber requests revocation of their EV Certificate, the Subscriber must be able to validate themselves as set forth in §3.4 to the RA that processed the Subscriber's EV Certificate Application. The EV CAs shall not be required to revoke and the RAs operating under the EV CAs shall not be required to request revocation of an EV Certificate until a Subscriber can properly validate themselves as set forth in §3.4 and §4.4.3.

Subscribers, Relying Parties, Application Software Vendors, and other third parties may report complaints or suspected Private Key compromise, EV Certificate misuse, or other types of fraud, compromise, misuse or inappropriate conduct related to EV Certificates by completing the form at https://www.entrust.net/ev/misuse.cfm.

An EV CA shall be entitled to revoke and shall revoke, and a RA operating under an EV CA shall be entitled to request revocation of and shall request revocation of, a Subscriber's EV Certificate at any time for any of the reasons set forth in §4.4.1.

4.4.3 Procedure for Revocation Request

A RA operating under an EV CA shall authenticate a request by a Subscriber for revocation of their EV Certificate by verifying (i) Subscriber authentication credentials, or (ii) authorization of the Subscriber through a reliable method of communication. Upon receipt and confirmation of such information, the RA shall send a revocation request to the EV CA that issued such EV Certificate. The EV CA shall make all reasonable efforts to post the serial number of the revoked EV Certificate to a CRL in an Entrust Repository within one (1) business days of receiving such revocation request.

For EV Certificate problems reported through the form at https://www.entrust.net/ev/misuse.cfm, an EV CA should begin an investigation within twenty-four hours and decide whether revocation or other appropriate action is warranted on a least the following criteria:

(i) The nature of the alleged problem;
(ii) The number of certificate problem reports received about a particular EV Certificate or website;
(iii) The identity of the complainants (for example, complaints from a law enforcement official that a Web site is engaged in illegal activities carry more weight than a complaint from a consumer alleging that they didn't receive the goods they ordered); and
(iv) Relevant legislation.

For Certificate revocation that is not initiated by the Subscriber, the RA that requested revocation of the Subscriber's EV Certificate shall make a commercially reasonable effort to notify the Subscriber by sending an email to the technical and security contacts specified in the Subscriber's EV Certificate Application.

4.4.4 Revocation Request Grace Period

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

4.4.5 Circumstances for Suspension

EV CAs do not suspend EV Certificates.

4.4.6 Who Can Request Suspension

EV CAs do not suspend EV Certificates.

4.4.7 Procedure for Suspension Request

EV CAs do not suspend EV Certificates.

4.4.8 Limits on Suspension Period

EV CAs do not suspend EV Certificates.

4.4.9 CRL Issuance Frequency

EV CAs shall issue CRLs as follows:

(i) CRLs for Entrust Certificates issued to subordinate CAs shall be issued at least once every twelve months or with 24 hours after revoking a subordinate CA. The next CRL update shall not be more than twelve months from the last update.

(ii) CRLs for EV Certificates shall be issued at least once every seven days.

4.4.10 CRL Checking Requirements

A Relying Party shall check whether the EV 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 EV 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 an EV Certificate, or (ii) any reliance by a Relying Party on an EV Certificate that has been revoked or that has expired.

4.4.11 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).

Entrust CAs shall sign and make available OCSP as follows:

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

(ii) OCSP responses for Entrust Certificates issued to end entities shall be issued at least once every four days. OCSP responses will have a maximum expiration time of ten days.

EV 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 twenty (20) years following revocation.

The on-line location of the CRL and the OCSP response are included in the EV 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 www.entrust.net/CPS.

4.4.12 On-line Revocation Checking Requirements

Refer to §4.4.10.

4.4.13 Other Forms of Revocation Advertisements Available

No stipulation.

4.4.14 Checking Requirements For Other Forms of Revocation Advertisements

No stipulation.

4.4.15 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 EV Certificate has been Compromised, the Subscriber shall immediately notify the RA that processed the Subscriber’s EV Certificate Application, using the procedures set forth in §4.4.3, of such suspected or actual Compromise. The Subscriber shall immediately stop using such EV Certificate and shall remove such EV Certificate from any devices and/or software in which such EV Certificate has been installed. The Subscriber shall be responsible for investigating the circumstances of such Compromise or suspected Compromise and for notifying any Relying Parties that may have been affected by such Compromise or suspected Compromise.

4.5 Security Audit Procedures

Significant security events in the EV 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. Authentication codes are used in conjunction with the audit trail files to protect against modification of audit logs. 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 EV CAs and all RAs operating under an EV CA record in detail every action taken to process an EV certificate request and to issue an EV Certificate, including all information generated or received in connection with an EV 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) EV CA key lifecycle management events, including:
  a. Key generation, backup, storage, recovery, archival, and destruction; and
  b. Cryptographic device lifecycle management events.

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

(iii) 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 EV CA facility.

(iv) Log entries include the following elements:
  a. Date and time of entry;
  b. Identity of the person making the journal entry; and
  c. Description of entry.

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

4.6 Records Archival

The audit trail files, databases and revocation information for EV CAs are both archived. The archive of an EV CAs' database and the archive of revocation information are retained for at least three (3) years. Archives of audit trail files are retained for at least seven (7) year(s) after any EV Certificate based on that documentation ceases to be valid. The databases for EV CAs are encrypted and protected by Entrust software master keys. 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 an EV CA system. Backup files are stored at a secure and separate geographic location.

4.7 Key Changeover

EV CAs' key pairs will be retired from service at the end of their respective lifetimes as defined in §6.3. New CAs with new key pairs will be created as required to support the continuation of EV CA Services. Each EV 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.

4.8 Compromise and Disaster Recovery

EV 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 issuance, certificate revocation, and issuance of certificate revocation status; and
(viii) testing of recovery plans.

In order to mitigate the event of a disaster, Entrust has 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 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 EV CAs. The Compromise of the Private Key used by an EV 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 shall be informed as soon as practicable of such a Compromise and information shall be posted in the Entrust Repository.

4.9 CA Termination

In the event that an EV CA ceases operation, all EV Certificates issued by such EV CA shall be revoked and the CRL life-time will be set to a period that meets any Entrust obligations.

5 Physical, Procedural, and Personnel Security Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

The computing facilities that host the Entrust Certificate Authority services are located within the Entrust Ottawa, Canada facility. The CA equipment is located in a Security zone that is physically separated from Entrust's other systems so that only authorized CA personnel can access it. The Security zone is constructed slab-to-slab with drywall and wire mesh. The Security zone is protected by electronic control access systems, alarmed doors and is monitored via a 24x7 recorded security camera and motion detector system.

5.1.2 Physical Access

The room containing the Entrust Authority 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 an EV Certificate Authority.

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 Entrust 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 §4.6.

5.2 Procedural Controls

An EV CA has a number of trusted roles for sensitive operations of the EV CA software. To gain access to the Entrust/Authority software used in an EV CA, operational personnel must undergo background investigations. EV CA operations related to adding administrative personnel or changing CA policy settings require more than one (1) person to perform the operation.

5.3 Personnel Controls

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

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The signing Key Pair for an EV CA is created during the initial startup of the Entrust Master Control application and is protected by the master key for such EV CA.

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

Entrust Certification Authority Administrators

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

6.1.2 Private Key Delivery to Entity

Not applicable.

6.1.3 Public Key Delivery to Certificate Issuer

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

6.1.4 CA Public Key Delivery to Users

The Public-Key Certificate for EV 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 issuing CAs is provided to the Subscriber with the Subscriber certificate.

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

6.1.5 Key Sizes

For Entrust EV CAs, the minimum key size shall be no less than 2048 bit RSA or shall be elliptic curve cryptography (ECC) NIST P-384 or P-521.

The minimum RSA key size for EV Certificates if 2048-bit. The ECC keys supported are NIST P-256, P-384 and P-521.

6.1.6 Public-Key Parameters Generation

No stipulation.

6.1.7 Parameter Quality Checking

No stipulation.

6.1.8 Hardware/Software Key Generation

CA Key Pairs must be generated on a cryptographic module that meets or exceeds the requirements as defined in §6.8.

Root CA

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

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.

<u>EV Code Signing Certificates</u>
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 §6.8.

6.1.9 Key Usage Purposes

EV Certificates issued by an EV CA contain the keyUsage and the extendkeyUsage Certificate extensions restricting the purpose for which an EV Certificate can be used. Subscribers and Relying Parties shall only use EV Certificates in compliance with this CPS and applicable laws.

6.2 Private Key Protection

6.2.1 Standards for Cryptographic Module

Entrust CAs Private Keys must be stored and protected on cryptographic modules that meet or exceed the requirements as defined in §6.8. 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 §6.8.

<u>EV Code Signing Certificates</u>
Subscribers are responsible for protecting the Private Key associated with the Public Key in the Subscriber's EV Code Signing Certificate. Subscribers must use cryptographic hardware modules that meet or exceed the requirements as defined in §6.8.

6.2.2 Private Key Multi-Person Control

A minimum of two person control shall be established on any Entrust 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 Entrust CA Private Keys shall be designated as authorized by the Entrust CA for this purpose. The names of the parties used for two-person control shall be maintained on a controlled list.

6.2.3 Private Key Escrow

Entrust does not escrow the Entrust CAs' Private Keys.

6.2.4 Private Key Backup

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

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

6.2.5 Private Key Archival

Upon retirement of an Entrust CA, the Private Keys will be archived securely using hardware cryptographic modules that meet the requirements §6.8. The Key Pairs shall not be used unless the CA has been removed from retirement or the keys are required temporarily to validate historical data. Private Keys required for temporary purposes shall be removed from archive for a short period of time.

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

6.2.6 Private Key Entry into Cryptographic Module

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

6.2.7 Private Key Storage on Cryptographic Module

Private Keys are stored on a cryptographic module are secured in accordance with the requirements specified in FIPS 140.

6.2.8 Method of Activating Private Keys

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

Subscriber Private Keys shall be activated by the Subscriber to meet the requirements of the security software used for their applications. Subscribers shall protect their Private Keys corresponding to the requirements in §2.1.3.

6.2.9 Private Key Deactivation Methods

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

<u>Entrust Certification Authority Administrators</u>
The administrator’s identity is deactivated in the Entrust CA and the administrator’s certificate is revoked.

6.2.10 Private Signature Key Destruction Method

Entrust 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 Entrust CA Private Keys must be authorized by the Entrust Policy Authority.

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

<u>Entrust Certification Authority Administrators</u>
The administrator’s private is destroyed by reinitializing the cryptographic module.

6.3 Other Aspects of Key Pair Management

The maximum validity for Entrust CAs’ RSA 2048 bit Key Pairs is 31 December 2030.

<u>EV SSL Certificates</u>
EV SSL Certificates contain a validity period of up to, but no more than, 27 months.

<u>EV Code Signing Certificates</u>
EV Code Signing Certificates contain a validity period of up to, but no more than, 39 months.

6.4 Activation Data

No stipulation.

6.5 Computer Security Controls

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

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

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

6.6.2 Security Management Controls

The configuration of the EV 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 Ratings

No stipulation.

6.7 Network Security Controls

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

6.8 Cryptographic Module Engineering Controls

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.

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

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 certification standards.

6.9 Time-Stamping

Entrust provides a Time-Stamp Authority (TSA) service for use with specific Entrust products such as EV Code Signing Certificates. The TSA authority supports RFC 3161 “Internet X.509 Public Key Infrastructure Time-Stamp Protocol” time-stamp requests.

As a best practice, Subscribers of EV Code Signing Certificates should time-stamp the digital signature after signing of the code.

Entrust time-stamping certificates contain a validity period of up to, but no more than, 135 months.

Details of any acceptable use policy or limitations are included in the Subscription Agreement.

7 Certificate and CRL Profiles

The profile for the EV Certificates and Certificate Revocation List (CRL) issued by an EV CA conform to the specifications contained in the EV Guidelines published by the CA/Browser Forum, which themselves conform to IETF RFC 5280 Internet X.509 PKI Certificate and Certificate Revocation List (CRL) Profile.

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

7.1 Certificate Profile

EV CAs issue certificates in accordance with the X.509 version 3. Certificate profiles for Entrust Root CA certificate, Subordinate CA certificates, and end entity certificates are described in Appendix A and the sections below.

7.1.1 Version Number(s)

All certificates issued by Entrust CAs are X.509 version 3 certificates.

7.1.2 Certificate Extensions

Certificate extensions are as stipulated in EV Guidelines. See Appendix A.

7.1.3 Algorithm Object Identifiers

Algorithm object identifiers are as specified in IETF RFC 3279 Algorithms and Identifiers for the Internet X.509 PKI Certificate and Certificate Revocation List (CRL) Profile. See Appendix A.

7.1.4 Name Forms

Name forms are as stipulated in §3.1.1.

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

Certificate policy object identifiers (OIDs) are listed in §1.2 and in the Certificate Profile attached as Appendix A.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

Entrust includes the following policy qualifiers in all end entity certificates:
CPSUri: http://www.entrust.net/rpa

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 EV 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

7.3 OCSP Profile

The profile for the EV Online Certificate Status Protocol (OCSP) messages issued by an EV CA conform to the specifications contained in the IETF RFC 2560 Internet X.509 PKI Online Certificate Status Protocol (OCSP) Profile.

7.4 Certificate Transparency

EV SSL Certificates may include two or more signed certificate timestamps (SCT) from Google approved independent certificate transparency logs. Information on certificate transparency may be found in IETF RFC 6962.

8 Specification Administration

8.1 Specification Change Procedures

Entrust may, in its direction, 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 EV Guidelines and the Baseline Requirements.

Modifications to the CPS shall be published in the Entrust Repository and shall become effective fifteen (15) days after publication in the Entrust 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 EV 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.

8.2 Publication and Notification Policies

Prior to major changes to this CPS, notification of the upcoming changes will be posted in the Entrust Repository.

8.3 CPS Approval Procedures

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

9 Acronyms

ASV	Application Software Vendor
CA	Certification Authority
CAA	Certification Authority Authorization
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CT	Certificate Transparency
DN	Distinguished Name
DNS	Domain Name Server
DSA	Digital Signature Algorithm
ECC	Elliptic Curve Cryptography
EV	Extended Validation
FQDN	Fully-Qualified Domain Name
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
MAC	Message Authentication Code
OA	Operational Authority
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PA	Policy Authority
PIN	Personal Identification Number
PKI	Public-Key Infrastructure
RA	Registration Authority
RDN	Relative Distinguished Name
RFC	Request for Comment
SEP	Secure Exchange Protocol
SSL	Secure Sockets Layer
URL	Universal Resource Locator

10 Definitions

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

Applicant: means an eligible organization applying for an EV Certificate, but which has not yet been issued an EV Certificate, or an organization that currently has an EV Certificate or EV Certificates and that is applying for renewal of such EV Certificate or EV Certificates or for an additional EV Certificate or EV 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, including but not limited to KDE, Microsoft, Mozilla Corporation, Nokia Corporation, Opera Software ASA, and Red Hat, Inc.

ASV: see Application Software Vendor.

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

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

CA: see Certification Authority

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

Certification Authority: means an entity or organization that (i) creates and digitally signs Certificates that contain among other things a Subject's Public Key and other information that is intended to identify the Subject, (ii) makes Certificates available to facilitate communication with the Subject identified in the Certificate, and (iii) creates and digitally signs Certificate Revocation Lists containing information about Certificates that have been revoked and which should no longer be used or relied upon.

Certification Practice Statement: means a statement of the practices that a 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 a RA operating under an EV CA the right to promote EV Certificates.

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

CPS: see Certification Practice Statement.

CRL: see Certificate Revocation List.

Cross Certificate(s): shall mean a Certificate(s) that (i) includes the Public Key of a Public-Private Key pair generated by an EV CA; and (ii) includes the digital signature of an Entrust Root CA.

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.

Entrust: means Entrust Datacard Limited.

Entrust Group: means collectively, Entrust, Affiliates, independent third-party Registration Authorities, Resellers, Co-Marketers, distributors, subcontractors, agents, suppliers and any employees and directors of the foregoing.

Entrust.net: means Entrust Datacard Limited.

Entrust Operational Authority: means those personnel who work for or on behalf of Entrust and who are responsible for the operation of the EV CAs.

Entrust 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 EV CAs.

Entrust Repository: means a collection of databases and web sites that contain information about EV Certificates and services provided by Entrust in respect to EV Certificates, including among other things, the types of EV Certificates issued by the EV CAs, the services provided by Entrust in respect to EV Certificates, the fees charged by Entrust for EV Certificates and for the services provided by Entrust in respect to EV Certificates, Certificate Revocation Lists, the CPS, and other information and agreements that are intended to govern the use of EV Certificates.

EV CA: see EV Certification Authority

EV Certificate: means a Certificate issued by an Entrust EV CA meeting the requirements of one of the EV Guideline documents.

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

EV Certification Authority: means a CA operated by or on behalf of Entrust for the purpose of issuing, managing, revoking, renewing, and providing access to EV Certificates.

EV Certification Practice Statement: means this document.

EV Code Signing Certificate: means a Code Signing Certificate issued by an Entrust EV Code Signing CA meeting the requirements of the EV Code Signing Guidelines.

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

EV Guidelines: Collective referral to both the EV SSL Guidelines and the EV Code Signing Guidelines.

EV SSL Guidelines: CA/Browser Forum Guidelines For The Issuance and Management of Extended Validation Certificates published at http://www.cabforum.org. The EV 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 Guidelines, the EV Guidelines take precedence over this CPS.

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

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.

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.

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.

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.

RA: see Registration Authority.

Random Value: as defined in the Baseline Requirements.

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

Relying Party: means a person, entity, or organization that relies on or uses an EV Certificate and/or any other information provided in a Repository under an EV 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 an EV CA in respect to the provision and use of certain information and services in respect to EV 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, 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 a RA operating under an EV CA the right to license the right to use EV Certificates.

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

Subject: means an organization whose Public Key is contained in an EV Certificate.

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

Subscriber: means an organization that has applied for and has been issued an EV Certificate.

Subscription 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 an EV CA in respect to the issuance, management, and provision of access to an EV Certificate and the provision of other services in respect to such EV Certificate.

Subsidiary Company: as defined in the Baseline Requirements.

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

Appendix A – Certificate Profiles

Entrust.net Certification Authority (2048) (Root Certificate)

Field		**Value**
Attributes		
Version		V3
Serial Number		38 63 de f8
Signature Algorithm		sha-1 WithRSAEncryption {1.2.840.113549.1.1.5}

Issuer DN		CN = Entrust.net Certification Authority (2048)
		OU = (c) 1999 Entrust.net Limited
		OU = www.entrust.net/CPS_2048 incorp. by ref. (limits liab.)
		O = Entrust.net

Validity Period		Valid from: December 24, 1999 Valid to: July 24, 2029

Subject DN		CN = Entrust.net Certification Authority (2048)
		OU = (c) 1999 Entrust.net Limited
		OU = www.entrust.net/CPS_2048 incorp. by ref. (limits liab.)
		O = Entrust.net

Subject Public Key Info		2048-bit RSA key modulus rsaEncryption {1.2.840.113549.1.1.1}
Extension	**Critical**	
Authority Key Identifier		Not present
Subject Key Identifier	No	55 e4 81 d1 11 80 be d8 89 b9 08 a3 31 f9 a1 24 09 16 b9 70
Key Usage	Yes	Certificate Signing, CRL Signing
Certificate Policies		Not present
Basic Constraints		Subject Type=CA Path Length Constraint=None
CRL Distribution Points		Not present
Thumbprint (SHA1)		50 30 06 09 1d 97 d4 f5 ae 39 f7 cb e7 92 7d 7d 65 2d 34 31

Entrust Root Certification Authority (Root Certificate)

Field		**Value**
Attributes		
Version		V3
Serial Number		45 6b 50 54
Signature Algorithm		sha-1 WithRSAEncryption {1.2.840.113549.1.1.5}

Issuer DN		CN = Entrust Root Certification Authority
		OU = (c) 2006 Entrust, Inc.
		OU = www.entrust.net/CPS incorporated by reference
		O = Entrust, Inc.
		C = US

Validity Period		Valid from: November 27, 2006 Valid to: November 27, 2026

Subject DN		CN = Entrust Root Certification Authority
		OU = (c) 2006 Entrust, Inc.
		OU = www.entrust.net/CPS incorporated by reference
		O = Entrust, Inc.
		C = US

Subject Public Key Info		2048-bit RSA key modulus rsaEncryption {1.2.840.113549.1.1.1}
Extension	**Critical**	
Authority Key Identifier	No	KeyID=68 90 e4 67 a4 a6 53 80 c7 86 66 a4 f1 f7 4b 43 fb 84 bd 6d
Subject Key Identifier	No	68 90 e4 67 a4 a6 53 80 c7 86 66 a4 f1 f7 4b 43 fb 84 bd 6d
Key Usage	Yes	Certificate Signing, CRL Signing
Basic Constraints	Yes	Subject Type = CA Path Length Constraint = none

Entrust Root Certification Authority – G2 (Root Certificate)

Field		**Value**
Attributes		
Version		V3
Serial Number		4a 53 8c 28
Signature Algorithm		sha-256 WithRSAEncryption

Issuer DN		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

Validity Period		Valid from: July 7, 2009 Valid to: December 7, 2030

Subject DN		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

Subject Public Key Info		2048-bit RSA key modulus rsaEncryption {1.2.840.113549.1.1.1}
Extension	**Critical**	
Subject Key Identifier	No	6a 72 26 7a d0 1e ef 7d e7 3b 69 51 d4 6c 8d 9f 90 12 66 ab
Key Usage	Yes	Certificate Signing, CRL Signing
Basic Constraints	Yes	Subject Type = CA Path Length Constraint = none

Entrust Root Certification Authority – EC1 (Root Certificate)

Field		**Value**
Attributes		
Version		V3
Serial Number		00 a6 8b 79 29 00 00 00 00 50 d0 91 f9
Signature Algorithm		ECDSA-SHA384

Issuer DN		CN = Entrust Root Certification Authority – EC1
		OU = (c) 2012 Entrust, Inc. - for authorized use only
		OU = See www.entrust.net/legal-terms
		O = Entrust, Inc.
		C = US

Validity Period		Valid from: December 18, 2012 Valid to: December 18, 2037
Subject DN		Same as Issuer DN
Subject Public Key Info		Elliptic Curve Public Key SECG elliptic curve secp384r1 (aka NIST P-384)
Extension	**Critical**	
Authority Key Identifier		Not present
Subject Key Identifier	No	b7 63 e7 1a dd 8d e9 08 a6 55 83 a4 e0 6a 50 41 65 11 42 49
Key Usage	Yes	Certificate Signing, CRL Signing
Basic Constraints	Yes	Subject Type=CA Path Length Constraint=None
CRL Distribution Points		Not present

Subordinate CA Certificate

Field		**Value**
Attributes		
Version		V3
Serial Number		Unique number to PKI domain
Signature Algorithm		SHA-1, SHA-256 or SHA-384
Issuer DN		Unique X.500 CA DN
Validity Period		No later than 2030 notBefore and notAfter are specified
Subject DN		Unique X.500 CA DN
Subject Public Key Info		Minimum 2048-bit RSA key modulus rsaEncryption {1.2.840.113549.1.1.1} or ECC keys of NIST P-384, or P-521
Extension	**Critical**	
Authority Key Identifier	No	Hash of the Root CA Public Key
Subject Key Identifier	No	Hash of the subjectPublicKey in this certificate
Key Usage	Yes	Certificate Signing, CRL Signing
Extended Key Usage	No	As applicable from the following: None present Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2) Code Signing (1.3.6.1.5.5.7.3.3)
Certificate Policies	No	Policy Identifier = All Issuance Policies uri: set as applicable
Basic Constraints	Yes	Subject Type = CA Path Length Constraint = value set as required
Authority Information Access	No	Access Method = On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) accessLocation: http://ocsp.entrust.net
CRL Distribution Points	No	http://crl.entrust.net/2048ca.crl, http://crl.entrust.net/rootca1.crl http://crl/entrust.g2ca.crl, or http://crl.entrust.net/ec1root.crl

EV SSL End Entity Certificate

Field		**Value**
Attributes		
Version		V3
Serial Number		Unique number to PKI domain with 64 bits entropy
Issuer Signature Algorithm		SHA-256 or SHA-384
Issuer DN		Unique X.500 CA DN
Validity Period		No greater than 27 months notBefore and notAfter are specified
Subject DN		CN = <DNS name of secure server> + serialNumber=<registration number of subscriber> OU = <organization unit of subscriber> (optional) businessCatergory = <applicable clause per the EV Guidelines> O = <full legal name of subscriber> jurisdicationOfIncorporationLocalityName (if applicable) = <jurisdication of registration or incorporation locality of subscriber> jurisdicationOfIncorporationStateOrProvinceName (if applicable) = <jurisdication of registration or incorporation state or province of subscriber> jurisdicationOfIncorporationCountry = <jurisdication of registration or incorporation country of subscriber> L = <locality of subscriber> S = <state or province of subscriber> (if applicable) C = <country of subscriber>
Subject Public Key Info		Minimum 2048 RSA key modulus rsaEncryption {1.2.840.113549.1.1.1} or ECC keys of NIST P-256, P-384, or P-521
Extension	**Critical**	
Authority Key Identifier	No	Hash of the CA Public Key
Subject Key Identifier	No	Hash of the subjectPublicKey in this certificate
Subject Alternative Name	No	DNS name(s) of secure server.
Certificate Transparency	No	1.3.6.1.4.1.11129.2.4.2 MAY include two or more Certificate Transparency proofs from approved CT Logs.
Key Usage	No	RSA keys - Digital Signature, Key Encipherment ECC keys – Digital Signature
Extended Key Usage	No	Server Authentication (1.3.6.1.5.5.7.3.1) and/or Client Authentication (1.3.6.1.5.5.7.3.2)
Certificate Policies	No	[1]Certificate Policy: Policy Identifier=2.16.840.1.114028.10.1.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.entrust.net/rpa
Basic Constraints	No	Subject Type = End Entity Path Length Constraint = None

Field		**Value**
Authority Information Access	No	Access Method = On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) accessLocation: http://ocsp.entrust.net Access Method = Certification Authority Issuer (1.3.6.1.5.5.7.48.2) accessLocation: http://aia.entrust.net/l1e-chain.cer OR http://aia.entrust.net/l1e-chainsha2.cer OR http://aia.entrust.net/l1j-ec1.cer OR http://aia.entrust.net/l1m-chain256.cer
CRL Distribution Points	No	http://crl.entrust.net/level1e.crl OR https//crl.entrust.net/level1j.crl OR http://crl.entrust.net/level1m.crl

EV Code Signing End Entity Certificate

Field		**Value**
Attributes		
Version		V3
Serial Number		Unique number to PKI domain with 64 bits entropy
Issuer Signature Algorithm		sha-256

Issuer DN		CN = Entrust Extended Validation Code Signing CA – EVCS1
		OU = (c) 2015 Entrust, Inc. - for authorized use only
		OU = See www.entrust.net/legal-terms
		O = Entrust, Inc.
		C = US

Validity Period		No greater than 39 months notBefore and notAfter are specified
Subject DN		CN = <full legal name of subscriber> serialNumber=<registration number of subscriber> businessCatergory = <applicable clause per the EV Guidelines> OU = <organization unit of subscriber> (optional) O = <full legal name of subscriber> jurisdicationOfIncorporationLocalityName (if applicable) = <jurisdication of registration or incorporation locality of subscriber> (optional) jurisdicationOfIncorporationStateOrProvinceName (if applicable) = <jurisdication of registration or incorporation state or province of subscriber> (optional) jurisdicationOfIncorporationCountry = <jurisdication of registration or incorporation country of subscriber> L = <locality of subscriber> (optional) S = <state or province of subscriber> (if applicable) C = <country of subscriber>
Subject Public Key Info		Minimum 2048-bit RSA key modulus rsaEncryption {1.2.840.113549.1.1.1}
Extension	Critical	
Authority Key Identifier	No	Hash of the CA public key
Subject Key Identifier	No	Hash of the subjectPublicKey in this certificate
Key Usage	Yes	Digital Signature
Extended Key Usage	No	Code Signing (1.3.6.1.5.5.7.3.3)
Certificate Policies	No	[1]Certificate Policy: Policy Identifier= 2.16.840.1.114028.10.1.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.entrust.net/rpa [2]Certificate Policy: Policy Identifier=2.23.140.1.3
Basic Constraints	No	Subject Type = End Entity Path Length Constraint = None
Authority Information Access		1. Access Method = On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.entrust.net

		2. Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://aia.entrust.net/evcs1-chain256.cer
CRL Distribution Points	No	uri: http://crl.entrust.net/evcs1.crl