ENTRUST

TREND MICRO SSL

CERTIFICATION PRACTICE STATEMENT

Version 2.3

Effective Date: 29 April 2016

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Overview

This Entrust Trend Micro SSL Certification Practice Statement (the "**CPS**"), Version 2.3, effective date: 29 April 2016, presents the principles and procedures Entrust employs in the issuance and life cycle management of the roots, sub-roots, and certificates listed on Appendix A. Entrust acquired the roots, sub-roots, and certificates listed on Appendix A from Trend Micro Inc. on 28 April 2016.

This CPS and any and all amendments thereto are incorporated by reference into all of the Certificates listed on Appendix A. The CPS is available on Entrust's website. In the event of any differences between the Japanese and English versions of this document, the English version will prevail.

Entrust is established to provide certificate services for a variety of external customers. The organization operates from the sub-CA roots listed on Appendix A, which issue certificates to various Entrust Trend Micro SSL customers. Subscribers include all parties who contract with Entrust for Entrust Trend Micro SSL digital certificate services. All parties who may rely upon the Entrust Trend Micro SSL certificates issued by Entrust Limited are considered relying parties. This certification practice statement (CPS) and other Entrust Trend Micro SSL business practices disclosures are applicable to all Entrust Trend Micro SSL certificates issued by Entrust.

This CPS follows the format of RFC 3647. For the purposes of this CPS, all capitalized terms used herein shall have the meaning given to them in Section 1.6, Definitions and Acronyms, or elsewhere in this CPS.

1.2 Document Name and Identification

This document is the Entrust Trend Micro SSL Certification Practices Statement and was approved for publication on 29 April 2016 by the Entrust Trend Micro SSL PKI Policy Authority. IANA has assigned the following OID to Entrust: 1.3.6.1.4.1.34697. The OID for this CPS is 1.3.6.1.4.1.34697.1.1, which is also the OID that Entrust Trend Micro SSL uses to indicate its adherence to and compliance with the Baseline Requirements of the CA/Browser Forum pursuant to BR 9.3.4.

1.3 PKI Participants

1.3.1 Certification Authorities

Entrust is a certification authority (CA) that issues SSL digital certificates, code signing certificates, and client (S/MIME) certificates in accordance with this CPS. As a CA, Entrust performs functions associated with Public Key operations, including receiving certificate requests, issuing, revoking and renewing a digital certificate, and maintaining, issuing, and publishing CRLs and OCSP responses.

Entrust's self-signed, offline Root CAs create online subordinate CAs in accordance with this CPS and applicable cross-certification policies and memoranda of agreement with other CAs. For ease of reference herein, all Entrust Root CAs and cross-signed or subordinate CAs that issue certificates are referred to as "CAs."

Entrust operations are managed by the Entrust Trend Micro SSL PKI Policy Authority (PKIPA) which is composed of members of Entrust management. The PKIPA is responsible for the approval of this CPS and overseeing the conformance of the Entrust Trend Micro SSL practices with applicable requirements.

Entrust Trend Micro SSL Server Certificates are X.509 Certificates with SSL Extensions issued from sub-roots that chain and may be cross-signed to the trusted roots listed on Appendix A, and which facilitate secure electronic commerce by providing limited authentication of a Subscriber's server and permitting SSL encrypted transactions between a Relying Party's browser and the Subscriber's server.

The Entrust Trend Micro SSL conforms to the current version of the CA-Browser Forum Baseline Requirements (“Baseline Requirements”) and Guidelines for Issuance and Management of Extended Validation Certificates ("EV Guidelines") and implements the Baseline Requirements and EV Guidelines through this CPS and Entrust’s other Entrust Trend Micro SSL policies. In the event of any inconsistency between Entrust’s other Entrust Trend Micro SSL policies and the Baseline Requirements or EV Guidelines, the Baseline Requirements and EV Guidelines take precedence.

1.3.2 Registration Authorities

Entrust Trend Micro SSL does not use external Registration Authorities.

1.3.3 Subscribers

Subscribers use Entrust’s SSL services and PKI to support transactions and communications. The Subject of a certificate is the party named in the certificate. A Subscriber, as used herein, refers to both the Subject of the certificate and the entity that contracted with Entrust for the certificate’s issuance. Prior to verification of identity and issuance of a certificate, a Subscriber is an Applicant.

1.3.4 Relying parties

Relying Parties are entities that act in reliance on a Entrust Trend Micro SSL certificate and/or digital signature issued by Entrust. Relying parties must check the appropriate CRL or OCSP response prior to relying on information featured in a certificate. The location of the CRL distribution point is detailed within the certificate.

Relying Parties are also obligated to: (a) Restrict reliance on certificates issued by the CA to the purposes for those certificates, in accordance with this CPS, (b) Agree to be bound by the provisions of limitations of liability as described in the CPS (or other CA business practices disclosure) upon reliance on a certificate issued by the CA, and (c) agree to be bound by the Relying Party Agreement as published at the Entrust Trend Micro SSL website. Entrust does not accept responsibility for reliance on a fraudulently obtained Certificate or a Certificate that is on the CRL or OCSP.

1.3.5 Other Participants

No provision.

1.4 Certificate Usage

A digital certificate (or certificate) is formatted data that cryptographically binds an identified subscriber with a Public Key. A digital certificate allows an entity taking part in an electronic transaction to prove its identity to other participants in such transaction. Digital certificates are used in commercial environments as a digital equivalent of an identification card.

1.4.1 Appropriate Certificate Uses

Certificates issued pursuant to this CPS may be used for all legal authentication, encryption, access control, and digital signature purposes, as designated by the key usage and extended key usage fields found within the certificate. However, the sensitivity of the information processed or protected by a certificate varies greatly, and each Relying Party must evaluate the application environment and associated risks before deciding on whether to use a certificate issued under this CPS.

1.4.2 Prohibited certificate uses

Certificates do not guarantee that the Subject is trustworthy, honest, reputable in its business dealings, compliant with any laws, or safe to do business with. A certificate only establishes that the information in the certificate was verified as reasonably correct when the certificate issued. Code signing certificates do not indicate that the signed code is safe to install or free from malware, bugs, or vulnerabilities.

Certificates issued under this CPS may not be used (i) for any application requiring fail-safe performance such as (a) the operation of nuclear power facilities, (b) air traffic control systems, (c) aircraft navigation systems, (d) weapons control systems, or (e) any other system whose failure could lead to injury, death or environmental damage; or (ii) where prohibited by law.

1.5 Policy Administration

1.5.1 Organization administering the document

The authority administering this CPS is the Entrust Trend Micro SSL PKI Policy Authority, which can be contacted at:

Entrust Trend Micro SSL PKI Policy Authority
Entrust Limited
1000 Innovation Drive
Ottawa K2K 3E7 ON Canada
[New Entrust email address]

1.5.2 Contact person

Legal Counsel
Entrust Limited
1000 Innovation Drive
Ottawa K2K 3E7 ON Canada
[New Entrust email address

1.5.3 Person Determining CPS Suitability for the Policy

Entrust does not support a Certificate Policy, but instead enforces its PKI policies through this CPS and other documents. The PKI Policy Authority determines the suitability and applicability of this CPS for its policies.

1.5.4 CPS Approval Procedures

The PKI Policy Authority approves the CPS and any amendments. Amendments may be made by either updating the entire CPS or by publishing an addendum. The PKI Policy Authority determines whether an amendment to this CPS requires notice or an OID change. See also Section 9.10 and Section 9.12 below.

1.6 Definitions and Acronyms

Applicant. All parties who apply for Entrust Trend Micro SSL digital certificate services with Entrust to be a Subscriber.

Baseline Requirements. The CA/Browser Forum Baseline Requirements published at http://www.cabforum.org, as such Baseline Requirements may be amended from time to time.

CA. Certification Authority.

Certificate. A record that, at a minimum: (a) identifies the CA issuing it; (b) names or otherwise identifies its Subscriber; (c) contains a Public Key that corresponds to a Private Key under the control of the Subscriber; (d) identifies its Operational Period; and (e) contains a Certificate serial number and is digitally signed by the CA. The term Certificate, as referred to in this CPS, means a Certificate issued by Entrust pursuant to this CPS.

Certificate Revocation List. A time-stamped list of revoked Certificates that has been digitally signed by the CA Certification Authority. An entity that issues Certificates and performs all of the functions associated with issuing such Certificates.
Compromise. Suspected or actual unauthorized disclosure, loss, loss of control over, or use of a Private Key associated with a Certificate.

CRL. See Certificate Revocation List.

DV (Domain Validated) Certificate. A certificate that contains the domain name of the Subscriber that has been validated according to the issuer's disclosed practices, but that does not contain any information about any organization or person associated with the Subscriber.

Entrust. Entrust Limited, 1000 Innovation Drive, Ottawa K2K 3E7 ON Canada

Entrust Trend Micro SSL: The roots, sub-roots, and certificates listed on Appendix A and related CA services provided by Entrust.

EV Certificate: A certificate that contains information specified in the EV Guidelines and that has been validated in accordance with those Guidelines.

EV Certificate Beneficiaries. (a) The Subscriber entering into the Subscriber Agreement for the EV Certificate; (b) the Subject named in the EV Certificate; (c) all application software suppliers with whom Entrust has entered into a contract for inclusion of its Root Certificate in software distributed by such application software suppliers; and (d) all Relying Parties that actually rely on such EV Certificate during the period when it is valid.

EV Guidelines. The CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Certificates published at http://www.cabforum.org, as such Guidelines may be amended from time to time.

EV Policies. Entrust Trend Micro SSL EV Certificate practices, policies, and procedures governing the issuance of EV Certificates, including this CPS.

Extension, means to place additional information about a Certificate within a Certificate. The X.509 standard defines a set of Extensions that may be used in Certificates.

Key Pair. Two mathematically related keys, having the following properties: (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 computationally impractical to discover the other key.

OCSP. Online Certificate Status Protocol as used by Entrust to report the revocation status of Certificates.

Operational Period. A Certificate's period of validity. It 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 is earlier revoked unless it is suspended.

Organization. The entity named or identified in a Certificate in the Organizational Name field that has purchased a Certificate.

OV (Organization Validated) Certificate. A certificate that contains information about the organization named in the certificate that has been validated according to the issuer's disclosed practices, but which has not been validated according to the EV Guidelines.

Private Key. The key of a Key Pair used to create a digital signature. This key must be kept a secret.

Public Key. The key of a Key Pair used to verify a digital signature. The Public Key is made freely available to anyone who will receive digitally signed messages from the holder of the Key Pair. The Public Key is usually provided via a Certificate issued by Entrust. A Public Key is used to verify the digital signature of a message purportedly sent by the holder of the corresponding Private Key.

Relying Party. A recipient of a digitally signed message who relies on a Certificate to verify the digital signature on the message. Also, a recipient of a Certificate who relies on the information contained in the Certificate.

Root Key(s). The Private Key used by Entrust to sign the Certificates.

SSL An industry standard protocol that uses public key cryptography for Internet security.

Subscriber. A person or entity who (a) is the subject named or identified in a Certificate issued to such person or entity, (b) holds a Private Key that corresponds to a Public Key listed in that Certificate, and (c) the person or entity to whom digitally signed messages verified by reference to such Certificate are to be attributed. For the purpose of this CPS, a person or entity who applies for a Certificate (an "Applicant") by the submission of an enrollment form is also referred to as a Subscriber.

Subscriber Agreement (also known as Terms of Service). The agreement between a Subscriber and Entrust.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

Entrust publishes its root certificates, revocation data for issued digital certificates, CPSs, Relying Party Agreements, and Subscriber Agreements (Terms of Service) in Entrust Limited's publicly-available online repositories.

Entrust operates its PKI infrastructure to ensure that its root certificates and CRLs are available through an online repository 24 hours a day, 7 days a week, with minimal interruption. Entrust does not provide a Repository or directory making end-entity Certificates available to Relying Parties.

2.2 Publication of Certification Information

Entrust Trend Micro SSL certificate services and the Entrust Trend Micro SSL repository are accessible through several means of communication:

1. By email using any email link listed at the Entrust Trend Micro SSL website, or such successor website as Entrust may use.
2. By mail addressed to: Legal Counsel, Entrust Trend Micro SSL PKI Policy Authority, 1000 Innovation Drive, Ottawa K2K 3E7 ON Canada

Entrust publishes its CPS, CA certificates, cross-certificates, Subscriber Agreements (Terms of Service), Relying Party Agreements, and CRLs for all revoked un-expired certificates in online repositories.

2.3 Time or Frequency of Publication

Entrust Trend Micro SSL CA certificates are published in a repository as soon as possible after issuance. CRLs for end-user certificates are issued at least as frequently as required by the Baseline Requirements. CRLs for CA certificates are issued at least every 12 months. Entrust may publish new CRLs prior to the expiration of the current CRL.

New or modified versions of this CPS, Subscriber Agreements (Terms of Service), or Relying Party Agreements are published within seven days after their approval.

2.4 Access Controls on Repositories

Information published on repositories is public information. Read only access is unrestricted. Entrust has implemented logical and physical controls to prevent unauthorized write access to its repositories.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

Certificates are issued with a non-null subject Distinguished Name (DN) that complies with ITU

X.500 standards.

Non-wildcard SSL Certificates and Unified Communications Certificates are issued using the Fully Qualified Domain Name (FQDN) name or IP address of the servers, services, or applications. Wildcard SSL Certificates have a wildcard asterisk character for the server name in the subject field. The FQDN or authenticated domain name is placed in the Common Name (CN) attribute of the Subject field and, when applicable, the Subject Alternative Name extension contains the FQDNs or authenticated domain names of the servers that are owned or under the control of the Subscriber. Subject Alternative Names are marked non-critical. When DNs are used, common names must respect name space uniqueness and must not be misleading.

3.1.2 Need for Names to Be Meaningful

Entrust uses distinguished names that identify both the subject and issuer of the certificate.

3.1.3 Anonymity or Pseudonymity of Subscribers

Generally, Entrust does not issue anonymous or pseudonymous certificates; however, for IDNs, Entrust may include the Punycode version of the IDN as the subject name.

3.1.4 Rules for Interpreting Various Name Forms

Distinguished Names in certificates are interpreted using X.500 standards and ASN.1 syntax. *See* RFC 2253 and RFC 2616 for further information on how X.500 distinguished names in certificates are interpreted as Uniform Resource Identifiers and HTTP references.

3.1.5 Uniqueness of Names

The uniqueness of each subject name in a certificate is enforced by entering the domain name in the Common Name attribute of the subject field or the Subject Alternative Name field. Domain name uniqueness is controlled by the Internet Corporation for Assigned Names and Numbers (ICANN).

3.1.6 Recognition, Authentication, and Role of Trademarks

Subscribers should not request certificates with any content that infringes on the intellectual property rights of another entity. Unless otherwise specifically stated in this CPS, Entrust does not verify an Applicant's right to use a trademark and does not resolve trademark disputes. Entrust may reject any application or require revocation of any certificate that is part of a trademark dispute.

3.2 Initial Identity Validation

Entrust may use any legal means of communication or investigation to ascertain the identity of an Applicant. Entrust may refuse to issue a certificate in its sole discretion.

3.2.1 Method to Prove Possession of Private Key

The Applicant must submit a CSR, generally in a PKCS#10 format, to establish that it holds the Private Key corresponding to the Public Key in the certificate request.

3.2.2 Authentication of Organization Identity

Entrust requires organizational applicants to include the organization name and address in the certificate application. Entrust verifies the organizational existence and identity of Applicants using reliable third party and government databases or through other direct means of communication with the entity or jurisdiction governing the organization's legal creation, existence, or recognition. If such efforts are insufficient to confirm the legal existence and identity of the subject, Entrust may require the Applicant to submit official company documentation, such as a business license, filed or certified articles of incorporation/organization, tax certificate, corporate charter, official letter, sales license, or other relevant documents. Entrust verifies the authority of the person requesting the certificate on behalf of an organization in accordance with Section 3.2.5.

Entrust also requires the following additional verification depending on the certificate type:

3.2.2.1 For Organization Validated (OV) Certificates

Entrust also validates the Applicant's right to use the domain name that will be listed in the certificate. Domain name ownership is validated by:

(a) Relying on publicly available records from the Domain Name Registrar. Entrust compares WhoIs Registrant information with the confirmed Organization identity information obtained for the Applicant under Section 3.2.2 using matching algorithms that include name, address, and other information. In the event of doubt, Entrust additionally requires use of the domain control confirmation methods stated in subsections (b) or (c). Entrust periodically correlates multiple sources to confirm the integrity of the WhoIs information used; or

(b) Communicating with one of the following email addresses: webmaster@domain.com, administrator@domain.com, admin@domain.com, hostmaster@domain.com, postmaster@domain.com, and any address listed in the technical, registrant, or administrative contact field of the domain's Domain Name Registrar record; or

(c) Requiring a practical demonstration of domain control (e.g., requiring the Applicant to make a specified change to a live page on the given domain).

If a third-party makes the certificate application on behalf of the company listed in the Domain Name Registrar record, the third party must submit a document that shows the Applicant's right to use the domain name that is signed by the Registrant (e.g. a domain owner's authorized representative) or the Administrative Contact on the Domain Name Registrar record.

3.2.2.2 For Extended Validation (EV) Certificates

EV Certificates are validated in accordance with the EV Guidelines of the CA/Browser Forum. For additional information on validation steps, see Section 11 of the EV Guidelines found at https://cabforum.org/documents/.

3.2.2.3 For Code Signing Certificates

(a) Application Procedure

Entrust Trend Micro SSL Code Signing Certificates are typically used to sign software objects, macros, device drivers, firmware images, virus updates, configuration files, or mobile applications.

An Applicant for a Code Signing Certificate shall complete an online Entrust Trend Micro SSL Code Signing Certificate enrollment form in a form prescribed by Entrust. All enrollment forms are subject to review, approval and acceptance by Entrust. All Applicants are required to include an Organization Name within the Code Signing Certificate enrollment form (or, if a Code Signing Certificate is requested in the name of an Individual, the Individual's name will be used for the Organizational Name within the enrollment form). Entrust performs the authentication steps listed below (and checks generally for errors and omissions relevant to the authentication steps taken), but does not otherwise verify the accuracy of the information contained in the Subscriber's Certificate request or otherwise check for errors and omissions.

(b) Authentication Process

(1) For Organizations

For Code Signing Certificates requested in the name of an Organization: Entrust will follow the procedures stated at Section 3.2.2.1 above for OV Server Certificates to confirm the identity of the Organization. In addition, the identity and authority of the individual requesting the certificate on behalf of the Organization will be verified by the methods stated in Section 3.2.5.1 below.

The CN and the O Subject Field of the code signing certificate issued to an organization shall contain the Subscriber's formal legal name that matches the name of the organization as per official government records in the Subscriber's jurisdiction of its place of business. If an assumed name is used, the assumed name shall be properly verified, and the legal name will also be included in [brackets].

(2) For Individuals

For Code Signing Certificates requested in the name of an Individual: Entrust will verify the identity of the Individual requesting the certificate by requiring the individual to provide sufficient personal data and copies of government-issued identification documents (e.g., passport, driver's license) to enable Entrust to confirm the Individual's identity through a reputable third party database or other resource. In addition, Entrust will require the Applicant to provide an e-mail contact address ("Contact Address") and telephone number ("Telephone Number") within the enrollment application and prove control over the Contact Address and Telephone Number. Entrust will verify that the Applicant controls the email account associated with the email address referenced in the certificate by sending an email to the address containing secret unpredictable information and giving the Applicant a limited time to use the information by sending a return email or using a web-based application to respond to the email. In addition, Entrust will confirm the Telephone Number either by calling the Applicant and asking for the secret unpredictable information contained in the email sent to the Applicant or by using an automated telephone application to perform a similar test.

The CN and the O Subject Field of the code signing certificate issued to an individual shall contain the name of the person in the form as displayed in the individual's confirmed identification documents, together with the words "Natural Person" in an OU field.

(c) Additional Requirements

Entrust may impose additional authentication requirements for Code Signing Certificates as required by certain browsers or applications. The additional requirements, if any, will be outlined to Applicant at the time of application.

3.2.2.4 For Client (S/MIME) Certificates

(a) Application Procedure

Entrust Trend Micro SSL Client (S/MIME) Certificates are typically used for authentication purposes, signing, and encryption of electronic mail and digital documents.

An Applicant for a client (S/MIME) Certificate shall complete an Entrust Trend Micro SSL Client Certificate enrollment application on behalf of Subscriber in a form prescribed by Entrust. All applications are subject to review, approval and acceptance by Entrust. All Applicants are required to include a name, e-mail contact address ("Contact Address") and telephone number ("Telephone Number") within the enrollment application and prove control over the Contact Address and Telephone Number. The Applicant may also ask for an Organization name to be included in the certificate, and provide related information for authentication. Entrust does not otherwise verify the accuracy of the information contained in the Applicant's enrollment form or otherwise check for errors and omissions.

(b) Authentication Process

Entrust will verify that the Applicant controls the email account associated with the email address referenced in the certificate or has been authorized by the email account holder to act on the account holder's behalf by sending an email to the address to be included in the certificate containing secret unpredictable information and giving the Applicant a limited time to use the information by sending a return email or using a web-based application to respond to the email and including the secret unpredictable information provided by Entrust. If the Applicant requests an Organization name be included in the certificate, Entrust will verify the Organization information and the Applicant's authority to request a certificate with the Organization information included according to the procedures outlined at Sections 3.2.2.1 and 3.2.5.1.

In addition, if Entrust determines in its discretion that additional verification is required to prove that a Certificate is duly authorized by the Applicant, Entrust may confirm the Telephone Number either by calling the Applicant and asking for the secret unpredictable information contained in the email sent to the Subscriber or by using an automated telephone application to perform a similar test.

3.2.3 Authentication of Individual Identity

Entrust does not issue SSL server certificates to individuals.

3.2.4 Non-Verified Subscriber Information

Provided that the right to use a domain name is verified in accordance with Section 3.2.2, Entrust may rely on the Subscriber's indication of the host or server name that forms the fully qualified domain name to be included in the SSL Certificate. Any other non-verified information included in a certificate is designated as such in the certificate.

3.2.5 Validation of Authority

3.2.5.1 For Organization Validated (OV) Certificates and Code Signing Certificates for Organizations

The authority of the individual requesting a certificate on behalf of an organization verified under section 3.2.2 is validated as follows:

Verifying the authority of the requester with an authorized contact listed with the Domain Name Registrar, through a person with control over the domain, or through an out-of-band confirmation with the organization.

Communication to persons with control over the domain consists of emailing one or more of the following email addresses: webmaster@domain.com, administrator@domain.com, admin@domain.com, hostmaster@domain.com, postmaster@domain.com, or any address listed as a contact field of the domain's Domain Name Registrar record.

3.2.5.2 For Extended Validation (EV) Certificates

Verifying authority of the Contract Signer and Certificate Approver in accordance with the EV Guidelines of the CA/Browser Forum. For additional information on validation steps, see Section 11 of the EV Guidelines, https://cabforum.org/documents/#Extended-Validation-Guidelines.

3.2.6 Criteria for Interoperation

No provision.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

Subscribers may request automatic re-key of a certificate prior to a certificate's expiration. After receiving a request for re-key, Entrust creates a new certificate with the same certificate contents except for a new Public Key and, optionally, an extended validity period. If the certificate has an extended validity period, Entrust may perform some revalidation of the Applicant but may also rely on information previously provided or obtained.

Subscribers re-establish their identity as follows:

OV Certificates:

Routine Re-Key Authentication:	Username and password
Re-Verification Required:	According to the Baseline Requirements

EV Certificates:

Routine Re-Key Authentication:	Username and password
Re-Verification Required:	According to the EV Guidelines

Code Signing Certificates:

Routine Re-Key Authentication:	Username and password
Re-Verification Required:	According to the Baseline Requirements

Client (S/MIME) Certificates:

Routine Re-Key Authentication:	Username and password
Re-Verification Required:	According to the Baseline Requirements

3.3.2 Identification and Authentication for Re-Key After Revocation

A subscriber requesting re-key after a certificate is revoked for a reason other than during a renewal or update action undergoes the initial registration process.

3.4 Identification and Authentication for Revocation Request

Revocation requests are authenticated by Subscribers after logging in to their accounts and requesting revocation of particular certificates and choosing a reason for revocation.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Either the Applicant or an individual authorized to request certificates on behalf of the Applicant may submit certificate requests. For certificates that include a domain name, the Domain Name Registrar record maintained by the domain registrar presumptively indicates who has authority over the domain. If a certificate request is submitted by an agent of the domain owner, the agent must send Entrust a document that authorizes Subscriber's use of the domain. Applicants are responsible for any data that the Applicant or an agent of the Applicant supplies to Entrust.

EV Certificate requests must be submitted by an authorized Certificate Requester and approved by a Certificate Approver. The certificate request must be accompanied by a signed (in writing or electronically) Subscriber Agreement from a Contract Signer.

Entrust does not issue certificates to any entity that is on a government denied list maintained by the United States or that is located in a country with which the laws of the United States prohibit doing business. For EV Certificates, Entrust verifies that the Applicant, the Applicant's Jurisdiction of Incorporation, Registration, and Place of Business are not included on such lists or subject to such prohibition.

4.1.2 Enrollment Process and Responsibilities

Entrust requires each Applicant to submit a certificate request and application information prior to issuing a Certificate. Entrust authenticates all communication from an Applicant and protects communication from modification.

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

The enrollment process includes:

1. Agreeing to the applicable Subscriber Agreement (Terms of Service),
2. Paying any applicable fees,
3. Submitting a complete certificate application,

4. Generating a key pair, and
5. Delivering the public key of the key pair to Entrust.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

After receiving an application, Entrust verifies the application information and other information in accordance with Section 3.2. All EV Certificates are validated in accordance with the EV Guidelines. After verification is complete, Entrust evaluates all the information and decides whether or not to issue the certificate.

At the present time, Entrust does not review or process CAA records, but Entrust does block issuance of certificates with certain names known to be top fraud targets, requiring additional authentication due diligence and manual approval and issuance. Any domain owner who wants to direct Entrust not to issue certificates for its Fully Qualified Domain Names and/or Second Level Domain Names should send a message to [new Entrust email address].

In the future, Entrust will begin reviewing and processing CAA records, and will amend this CPS with additional details at that time.

4.2.2 Approval or Rejection Of Certificate Applications

Entrust rejects any certificate application that Entrust cannot verify. Entrust may also reject a certificate application if Entrust believes that issuing the certificate could damage or diminish Entrust's reputation or business including the Entrust Trend Micro SSL business.

EV Certificate issuance approval requires authentication by two separate Entrust validation specialists. The second validation specialist cannot be the same individual who collected the authentication documentation and originally approved the EV Certificate. The second validation specialist reviews the collected information and documents for discrepancies or details that require further explanation. If the validation specialist has any concerns about the application, the second validation specialist may require additional explanations and documents. If satisfactory explanations and/or additional documents are not received within a reasonable time, Entrust will reject the EV Certificate request and notify the Applicant accordingly.

If some or all of the documentation used to support the application is in a language other than English, an Entrust employee or agent skilled in such language and having the appropriate training, experience, and judgment in confirming organizational identification and authorization performs the final cross-correlation and due diligence.

If the certificate application is not rejected and is successfully validated in accordance with this CPS, Entrust will approve the certificate application and issue the certificate. Additional certificates containing the same validated certificate information may be requested by the Subscriber via a confirmed communication and issued without further authentication during the period permitted before reauthentication of certificate information is required. Entrust is not liable for any rejected certificate and is not obligated to disclose the reasons for a rejection. Rejected Applicants may re-apply. Subscribers are required to check the data listed in the certificate for accuracy prior to using the certificate.

4.2.3 Time to Process Certificate Applications

Under normal circumstances, Entrust confirms certificate application information and issues a

digital certificate within a reasonable time frame. Issuance time frames are greatly dependent on when the Applicant provides the details and documentation necessary to complete validation. For non-EV SSL certificates, Entrust will usually confirm submitted application data, complete the validation process, and issue or reject a certificate application within two working days after Entrust receives all of the necessary details and documentation from the Applicant.

Occasionally, events outside of the control of Entrust delay the issuance process. However, Entrust makes reasonable effort to meet its issuance times and make Applicants aware of any factors that affect issuance times.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

Entrust verifies the source of the certificate request and the identity of the Applicant in a secure manner prior to issuing a certificate. Any database used to confirm Subscriber information is protected from unauthorized modification. After validation is complete, the certificate is issued and sent to the Subscriber.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

Entrust may deliver certificates in any secure manner within a reasonable time after issuance. Generally, Entrust delivers certificates via email to the email address designated by the Subscriber during the application process. The Subscriber is also provided a link to a user id/password-protected location on Entrust's web server where the Subscriber may log in and download each certificate or the zip file containing all certificates in the trust chain.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Subscribers are solely responsible for installing the issued certificate on the Subscriber's computer or hardware security module. Certificates are considered accepted on the earlier of (a) the Subscriber's use of the certificate or (b) 30 days after the certificate's issuance.

4.4.2 Publication of the Certificate by the CA

Entrust publishes all CA certificate in its repository. Entrust publishes end-entity certificates by delivering them to the Subscriber.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Entrust may publish Subscriber certificates to one or more CT (Certificate Transparency) logs which may be viewed by the public.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

Subscribers are contractually obligated to protect their Private Keys from unauthorized use or disclosure, discontinue using a Private Key after expiration or revocation of the associated certificate, and use Private Keys only as specified in the key usage extension.

4.5.2 Relying party public key and certificate usage

Relying Parties may only use software that is compliant with X.509 and other applicable standards. Entrust does not warrant that any third party's software will support or enforce the controls and requirements found herein.

A Relying Party should use discretion when relying on a certificate and should consider the totality of the circumstances and risk of loss prior to relying on a certificate. If the circumstances indicate that additional assurances are required, the Relying Party must obtain such assurances before using the certificate. Any warranties provided by Entrust are only valid if a Relying Party's reliance was reasonable and if the Relying Party adhered to the Relying Party Agreement set forth in the Entrust Trend Micro SSL repository.

A Relying Party should rely on a digital signature or SSL/TLS handshake only if:

1. The digital signature or SSL/TLS session was created during the operational period of a valid certificate and can be verified by referencing a valid certificate,
2. The certificate is not revoked and the Relying Party checked the revocation status of the certificate prior to the certificate's use by referring to the relevant CRLs or OCSP responses, and
3. The certificate is being used for its intended purpose and in accordance with this CPS.

4.6 Certificate Renewal

4.6.1 Circumstance for Certificate Renewal

Entrust may renew a certificate if:

1. The associated public key has not reached the end of its validity period,
2. The Subscriber name and attributes are unchanged,
3. The associated private key remains uncompromised, and
4. Re-verification of the Subscriber's identity is not required under Section 3.3.1.

Entrust makes reasonable efforts to notify Subscribers via email of the imminent expiration of a digital certificate and may begin providing notice of pending expiration 60 days prior to the expiration date (or such other period as may be chosen by the Subscriber). Certificate renewal may require payment of additional fees which are disclosed to Subscribers approaching their certificate or enterprise account expiration date. Renewal after revocation is not supported.

4.6.2 Who May Request Renewal

Only an authorized representative of a Subscriber may request renewal of the Subscriber's certificates. Entrust may renew a certificate without a corresponding request if the signing certificate is re-keyed.

4.6.3 Processing Certificate Renewal Requests

Renewal application requirements and procedures are generally the same as those used during the certificate's original issuance. Entrust validation personnel may reconfirm domain name ownership using current Domain Name Registrar information and may check state or other jurisdictional records to confirm geographic location, company control and good standing the jurisdiction of organization. If Entrust cannot verify any information it rechecks, the certificate is

not renewed.

Entrust will not reuse EV Certificate validation information if the age of the data exceeds the time specified in the EV Guidelines.

Some device platforms allow renewed use of the Private Key. If the Subscriber's other contact information and Private Key have not changed, the Subscriber may use the same CSR as was used for the previous certificate.

4.6.4 Notification of New Certificate Issuance to Subscriber

Entrust delivers renewed certificates to Subscribers in a secure fashion, typically via email to the address provided by the Subscriber during the renewal process. Entrust may deliver the certificate by providing the Subscriber a link to a user id/password-protected location on Entrust's web server where the subscriber may log in and download the certificate.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Renewed certificates are considered accepted on the earlier of (i) the Subscriber’s use of the certificate or (ii) 30 days after the certificate’s renewal.

4.6.6 Publication of the Renewal Certificate by the CA

Entrust publishes a renewed certificate by delivering it to the Subscriber. Renewed CA certificates are published in Entrust’s repository.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Entrust may publish Subscriber certificates to one or more CT (Certificate Transparency) logs which may be viewed by the public.

4.7. Certificate Re-Key

4.7.1. Circumstance for Certificate Rekey

Re-keying a certificate consists of creating a new certificate with a new public key and serial number while keeping the subject information the same. The new certificate may have a different validity period, key identifiers, CLR and OCSP distributions, and a different signing key. After re-keying a certificate, Entrust may revoke the old certificate but may not further re-key, renew, or modify the old certificate. Re-key after revocation is not supported.

4.7.2 Who May Request Certification of a New Public Key

Entrust may initiate certificate re-key certificates at the request of the certificate subject or authorized representative.

4.7.3 Processing Certificate Re-Keying Requests

If the Subscriber's other contact information and Private Key have not changed, Entrust can issue a replacement certificate using the previously provided CSR. Otherwise, the Subscriber must submit a new CSR. Entrust re-uses existing verification information unless re-verification is required under section 3.3.1 or Entrust believes that the information has become inaccurate.

4.7.4 Notification of New Certificate Issuance to Subscriber

Entrust notifies the Subscriber within a reasonable time after the certificate issues.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Issued certificates are considered accepted on the earlier of (a) the Subscriber's use of the certificate or (b) 30 days after the certificate is rekeyed.

4.7.6 Publication of the Re-Keyed Certificate by the CA

Entrust publishes rekeyed certificates by delivering them to Subscribers.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Entrust may publish Subscriber certificates to one or more CT (Certificate Transparency) logs which may be viewed by the public.

4.8 Certificate Modification

4.8.1 Circumstance for Certificate Modification

Modifying a certificate means creating a new certificate for the same subject with authenticated information that differs slightly from the old certificate (e.g., changes to non-essential parts of names or attributes) provided that the modification otherwise complies with this CPS. The new certificate may have the same or a different subject public key.

After modifying a certificate, Entrust can revoke the old certificate but will not further re-key, renew, or modify the old certificate.

4.8.2 Who May Request Certificate Modification

Entrust modifies certificates at the request of certain certificate subjects or in its own discretion. Entrust does not make certificate modification services available to all Subscribers.

4.8.3 Processing Certificate Modification Requests

After receiving a request for modification, Entrust verifies any information that will change in the modified certificate. Entrust will only issue the modified certificate after completing the verification process on all modified information. Entrust will not issue a modified certificate that has a validity period that exceeds the applicable time limits found in section 3.3.1 or 6.3.2.

4.8.4 Notification of New Certificate Issuance to Subscriber

Entrust notifies the Subscriber within a reasonable time after the certificate issues.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Issued certificates are considered accepted on the earlier of (a) the Subscriber's use of the certificate or (b) 30 days after the certificate is rekeyed.

4.8.6 Publication of the Modified Certificate by the CA

Entrust publishes modified certificates by delivering them to Subscribers.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Entrust may publish Subscriber certificates to one or more CT (Certificate Transparency) logs which may be viewed by the public.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

Revocation of a certificate permanently ends the operational period of the certificate prior to the certificate reaching the end of its stated validity period. Prior to revoking a certificate, Entrust verifies the identity and authority of the entity requesting revocation. Entrust may revoke any certificate in its sole discretion, including if Entrust believes that:

1. The Subscriber requested revocation of its certificate;
2. The Subscriber did not authorize the original certificate request and did not retroactively grant authorization;
3. Either the Private Key associated with the certificate or the Private Key used to sign the certificate was compromised;
4. The Subscriber or Entrust breached a material obligation under the CPS or the relevant Subscriber Agreement;
5. Either the Subscriber's or Entrust's obligations under the CPS are delayed or prevented by circumstances beyond the party's reasonable control, including computer or communication failure, and, as a result, another entity's information is materially threatened or compromised;
6. The certificate was not issued in accordance with the CPS or applicable industry standards;
7. Entrust received a lawful and binding order from a government or regulatory body to revoke the certificate;
8. Entrust ceased operations and did not arrange for another certificate authority to provide revocation support for the certificates;
9. Entrust's right to manage certificates under applicable industry standards was terminated (unless arrangements have been made to continue revocation services and maintain the CRL/OCSP Repository);
10. A court or arbitrator revoked the Subscriber's right to use a name or mark listed in the certificate, or the Subscriber failed to maintain a valid registration for such name or mark;
11. Any information appearing in the Certificate was or became inaccurate or misleading; or
12. The Subscriber was added as a denied party or prohibited person to a blacklist or is operating from a destination prohibited under the laws of the United States;

Entrust will always revoke an Entrust Trend Micro SSL certificate if it becomes aware that the binding between the subject and the subject's public key in the certificate is no longer valid or if an associated Private Key is compromised.

4.9.2 Who Can Request Revocation

The Subscriber or another appropriately authorized party (such as an administrative contact, a Contract Signer, Certificate Approver, or Certificate Requester) may request revocation of a certificate. Entrust may require that the revocation request be made by either the organizational

contact, billing contact or domain registrant.

Entrust will revoke a certificate if it receives sufficient evidence of compromise of loss of the private key and may revoke a certificate of its own volition without reason, even if no other entity has requested revocation. Other entities may request revocation of a certificate for problems related to fraud, misuse, or compromise by filing a "Certificate Problem Report". All certificate revocation requests must include the identity of the person or entity requesting revocation and the reason for revocation.

4.9.3 Procedure for Revocation Request

Entities submitting certificate revocation requests must list their identity and explain the reason for requesting revocation. Entrust employs the following procedure after receiving a revocation request:

1. Entrust personnel log the identity of person or entity making the request or problem report and the reason for requesting revocation. Entrust may also include its own reasons for revocation in the log.
2. Entrust requests confirmation of the revocation from a known administrator via out-of-band communication (e.g., telephone, fax, etc.).
3. If the request is authenticated as originating from the Subscriber, Entrust will always revoke a certificate.
4. For requests from third parties, Entrust personnel begin investigating all Certificate Problem Reports within 24 hours after receipt and decide whether revocation is appropriate based on the following criteria:
    a. The nature of the alleged problem,
    b. The number of Certificate Problem Reports received about a particular certificate or website,
    c. The identity of the complainants (for example, complaints from a law enforcement official that a web site is engaged in illegal activities have more weight than a complaint from a consumer alleging they never received the goods they ordered), and
    d. Relevant legislation.
5. If revocation is appropriate, Entrust personnel revoke the certificate and cause the CRL to be updated.

Subscribers may revoke any of their certificates 24 x 7 by use of their online subscriber account, with no approval or other action required by Entrust.

4.9.4 Revocation Request Grace Period

Entrust provides revocation grace periods to Subscribers on a case-by-case basis.

4.9.5 Time Within Which CA Must Process the Revocation Request

Entrust will revoke a CA certificate immediately once a Subscriber clicks the Revoke button on its online subscriber account, or within one hour after receiving instructions from the PKI Policy Authority. Other certificates are revoked as quickly as practical after validating the revocation request in accordance with the process stated in Section 4.9.3.

4.9.6 Revocation Checking Requirement for Relying Parties

Prior to relying on information listed in a certificate, a Relying Party must confirm the validity of each certificate in the certificate path in accordance with IETF PKIX standards, including checks for certificate validity, issuer-to-subject name chaining, policy and key use constraints, and revocation status through CRLs or OCSP responders identified in each certificate in the chain.

4.9.7 CRL Issuance Frequency

CRLs for end-user certificates are issued at least once per day. CRLs for CA certificates are issued at least every 12 months. Under special circumstances, Entrust may publish new CRLs prior to the expiration of the current CRL.

4.9.8 Maximum Latency for CRLs

CRLs are posted automatically to the online repository within a commercially reasonable time after generation, usually within minutes of generation. Irregular, interim, or emergency CRLs are posted no later than four hours after generation. Otherwise, Entrust always posts regularly scheduled CRLs prior to the nextUpdate field in the previously issued CRL of the same scope.

4.9.9 On-Line Revocation/Status Checking Availability

Entrust makes certificate status information available via OCSP. OCSP responses are provided within a commercially reasonable time after the request is received, subject to transmission latencies over the Internet.

4.9.10 On-Line Revocation Checking Requirements

A Relying Party must confirm the validity of a certificate in accordance with section 4.9.6 prior to relying on the certificate.

4.9.11 Other Forms of Revocation Advertisements Available

No provision.

4.9.12 Special Requirements re Key Compromise

Entrust uses commercially reasonable efforts to notify potential Relying Parties by revocation of the affected certificates if it discovers or suspects the compromise of a Private Key. Entrust will transition any revocation reason code in a CRL to “key compromise” upon discovery of such reason. If a certificate is revoked because of compromise, Entrust will issue a new CRL within 24 hours after receiving notice of the compromise.

4.9.13 Circumstances for Suspension

Entrust does not support certificate suspension.

4.9.14 Who Can Request Suspension

No provision.

4.9.15 Procedure for Suspension Request

No provision.

4.9.16 Limits on Suspension Period

No provision.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Certificate status information is available via CRL and OCSP responder.

4.10.2 Service Availability

Certificate status services are available 24x7 without interruption.

4.10.3 Optional Features

No provision.

4.11 End of Subscription

A Subscriber's subscription service ends if its certificate expires or is revoked or if the applicable Subscriber Agreement expires without renewal.

4.12 Key Escrow and Recovery

Entrust does not escrow CA Private Keys or Subscriber private keys, or provide key Subscriber recovery services.

4.12.1 Key Escrow and Recovery Policy and Practices

No provision.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No provision.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical Controls

5.1.1 Site Location and Construction

Entrust performs its CA operations from secure, geographically diverse, commercial data centers that are equipped with logical and physical controls that make Entrust's CA operations inaccessible to non-trusted personnel. Entrust operates under a security policy designed to detect, deter, and prevent unauthorized access to Entrust's operations.

5.1.2 Physical Access

Entrust protects its equipment from unauthorized access and implements physical controls to reduce the risk of equipment tampering. The secure parts of Entrust's CA hosting facilities are

protected using physical access controls making them accessible only to appropriately authorized individuals.

The buildings where Entrust's CA systems are housed are accessed through areas with security personnel on duty full time (24 hours per day, 365 days per year). Access to secure areas of the buildings requires the use of an "access" or "pass" cards or biometric controls. The exterior and internal passageways of the buildings are under constant video surveillance. Entrust stores all removable media and paper containing sensitive plain-text information related to its CA operations in secure, locked containers.

Access to the data centers housing the CA platforms requires two-factor authentication, under which the individual must have an authorized access card, and doors to access rooms where the equipment is housed are equipped with biometric access control authenticators. These card-based biometric authentication access systems are also programmed to log each use of the access card.

Entrust deactivates, removes, and securely stores its CA equipment when not in use. Activation data must either be memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module and is never stored with the cryptographic module or removable hardware associated with equipment used to administer Entrust's private keys.

5.1.3 Power and Air Conditioning

Data centers have primary and secondary power supplies that ensure continuous and uninterrupted access to electric power. Uninterrupted power supplies (UPS) and diesel generators provide redundant backup power.

Entrust's data center facilities use multiple load-balanced HVAC systems for heating, cooling, and air ventilation through perforated-tile raised flooring to prevent overheating and to maintain a suitable humidity level for sensitive computer systems.

5.1.4 Water Exposures

The cages and racks housing Entrust's CA systems are located on raised flooring, and the data centers are equipped with monitoring systems to detect excess moisture.

5.1.5 Fire Prevention and Protection

The data centers are equipped with fire suppression mechanisms.

5.1.6 Media Storage

Entrust protects its media from accidental damage and unauthorized physical access. Backup files are created on a daily basis and are stored in a backup location that is separate from Entrust's primary system.

5.1.7 Waste Disposal

All unneeded copies of printed sensitive information are shredded on-site before disposal. All electronic media are initialized before disposal.

5.1.8 Off-Site Backup

Entrust maintains at least one full backup and makes regular backup copies of any information necessary to recover from a system failure. Entrust moves media designated for storage to secure off-site locations. Backup copies of CA Private Keys and activation data are stored off-site in locations that are accessible only by trusted personnel.

5.2 Procedural Controls

5.2.1 Trusted Roles

Personnel acting in trusted roles include CA system administration personnel, and personnel involved with identity vetting and customer support. The functions and duties performed by persons in trusted roles are distributed so that one person alone cannot circumvent security measures or subvert the security and trustworthiness of the PKI operations. Trusted roles are appointed by senior management.

5.2.2 Number of Persons Required Per Task

Entrust requires that at least two people acting in a trusted role take action to activate Entrust's Private Keys, generate a CA key pair, or backup an Entrust private key. Entrust creates backup Private Key parts on an 3-of-5 key part split.

5.2.3 Identification and Authentication for Each Role

All personnel are required to authenticate themselves to CA systems before they are allowed access to systems necessary to perform their trusted roles.

5.2.4 Roles Requiring Separation of Duties

The following roles requiring a separation of duties:

1. Generate a CA key pair
2. Physical or logical access to the CA or certificate systems
3. EV certificate Subscriber authentication

Entrust's policies and systems identify and authenticate individuals acting in trusted roles, restrict an individual from assuming multiple roles, and prevent any individual from having more than one identity.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

The PKI Policy Authority is responsible and accountable for Entrust's PKI operations and ensures compliance with this CPS. Entrust's personnel and management practices provide reasonable assurance of the trustworthiness and competence of its employees and of the satisfactory performance of their duties. The PKI Policy Authority ensures that all individuals assigned to trusted roles have the experience, qualifications, and trustworthiness required to perform their duties under this CPS.

5.3.2 Background Check Procedures

Entrust verifies the identity of each person to be appointed to a trusted role and performs a background check prior to allowing such person to act in a trusted role. Entrust requires each individual to appear in-person before a human resources employee whose responsibility it is to verify identity. The human resources employee verifies the individual's identity using the required forms of government-issued photo identification. Background checks include employment history, education, character references, national identification number, and criminal background. Background investigations are performed by a competent independent authority that has the authority to perform background investigations.

5.3.3 Training Requirements

Entrust provides skills training to all personnel involved in Entrust's PKI operations. The training relates to the person's job functions and covers:

1. Basic Public Key Infrastructure (PKI) knowledge,
2. Authentication and verification policies and procedures,
3. Common threats to the validation process, including phishing and other social engineering tactics, and
4. Applicable industry and government guidelines.

Training is updated from time to time and is also provided via a mentoring process involving senior members of the team to which the employee belongs.

Entrust maintains records of who received training and what level of training was completed. Validation Specialists must have the minimum skills necessary to satisfactorily perform validation duties before being granted validation privileges. All Validation Specialists validating EV Certificates are required to pass practice tests on the EV Certificate validation criteria outlined in the EV Guidelines.

5.3.4 Retraining Frequency and Requirements

Personnel must maintain skill levels that are consistent with industry-relevant training and performance programs in order to continue acting in trusted roles. Entrust makes all individuals acting in trusted roles aware of any changes to Entrust's operations. If Entrust's operations change, Entrust will provide documented training, in accordance with an executed training plan, to all personnel acting in trusted roles.

5.3.5 Job Rotation Frequency and Sequence

No provision.

5.3.6 Sanctions for Unauthorized Actions

Entrust employees and agents failing to comply with this CPS, whether through negligence or malicious intent, are subject to administrative or disciplinary actions, including termination of employment or agency and criminal sanctions. If a person in a trusted role is cited by management for unauthorized or inappropriate actions, the person will be immediately removed from the trusted role pending management review. After management has reviewed and discussed the incident with the employee involved, management may reassign that employee to a non-trusted role or dismiss the individual from employment as appropriate.

5.3.7 Independent Contractor Requirements

Independent contractors who are assigned to perform trusted roles are subject to the duties and requirements specified for such roles in this Section 5.3 and are subject to sanctions stated above in Section 5.3.6.

5.3.8 Documentation Supplied to Personnel

Personnel in trusted roles are provided with the documentation necessary to perform their duties, including a copy of this CPS, Baseline Requirements, EV Guidelines, and other technical and operational documentation needed to maintain the integrity of Entrust's CA operations. Personnel are also given access to information on internal systems and security documentation, identity vetting policies and procedures, discipline-specific books, treatises and periodicals, and other information.

5.4 Audit Logging Procedures

Entrust's systems require identification and authentication at system logon with a unique user name and password and use of hard token with changing password numbers. Vetting systems also require the use of a hard token with certificate and accounts with username and password. Important system actions are logged to establish the accountability of the operators who initiate such actions.

5.4.1 Types of Events Recorded

Entrust enables all essential event auditing capabilities of its CA applications in order to record all significant system events including the following:

- CA key lifecycle management events, including:
  - Key generation, backup, storage, recovery, archival, and destruction; and
  - Cryptographic device lifecycle management events.
- CA and Subscriber Certificate lifecycle management events, including:
  - Certificate Requests, renewal and re-key requests, and revocation;
  - All verification activities required by this CPS;
  - Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
  - Acceptance and rejection of Certificate Requests;
  - Issuance of Certificates; and
  - Generation of Certificate Revocation Lists (CRLs).
- Security events, including:
  - Successful and unsuccessful PKI system access attempts;
  - PKI and security system actions performed;
  - Security profile changes;
  - System crashes, hardware failures, and other anomalies;
  - Firewall and router activities; and
  - Entries to and exits from the CA facility.

If Entrust's applications cannot automatically record an event, Entrust implements manual procedures to satisfy the requirements. For each event, Entrust records the relevant (a) date and time, (b) type of event, (c) success or failure, and (d) user or system that caused the event or initiated the action. All event records are available to auditors as proof of Entrust's practices.

5.4.2 Frequency of Processing Log

An Entrust administrator reviews the logs generated by Entrust's systems, makes system and file integrity checks, and conducts a vulnerability assessment with at least the frequency required by the Network and Certificate System Security Requirements of the CA/Browser Forum Baseline Requirements. The administrator may perform the checks using automated tools. During these checks, the administrator (a) checks whether anyone has tampered with the log, (b) scans for anomalies or specific conditions, including any evidence of malicious activity, and (c) notifies the PKI Policy Authority and other staff of the results. Any anomalies or irregularities found in the logs are investigated and are made available to Entrust's auditors upon request. Entrust documents any actions taken as a result of a review.

5.4.3 Retention Period for Audit Log

Event logs will be retained for at least seven years and will be available to Entrust's auditors upon request.

5.4.4 Protection of Audit Log

Audit logs are protected from destruction prior to the end of the audit log retention period and are retained securely on-site until transferred to a backup site. Entrust's off-site storage location is a safe and secure location that is separate from the location where the data was generated.

5.4.5 Audit Log Backup Procedures

On a periodic basis, Entrust makes backup copies of audit logs and audit log summaries and sends a copy of the audit log off-site.

5.4.6 Audit Collection System (Internal vs. External)

Automatic audit processes begin on system startup and end at system shutdown. If an automated audit system fails and the integrity of the system or confidentiality of the information protected by the system is at risk, Entrust's administrators will consider suspending its operation until the problem is remedied.

5.4.7 Notification To Event-Causing Subject

No provision.

5.4.8 Vulnerability Assessments

Entrust performs routine risk assessments that identify and assess reasonably foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any certificate data or certificate issuance process. Entrust also routinely assess the sufficiency of the policies, procedures, information systems, technology, and other arrangements that Entrust has in place to control such risks. Entrust also performs vulnerability scans and penetration testing of CA systems with at least the frequency required by the Network and Certificate System Security Requirements of the CA/Browser Forum Baseline Requirements. All such assessments are available to Entrust's auditors upon request.

5.5 Records Archival

5.5.1 Types of Records Archived

Entrust retains the following information in its archives (as such information pertains to Entrust's

CA operations):

1. Identity authentication data,
2. Issued certificates,
3. Certificate and revocation requests,
4. CRLs,
5. Compliance auditor reports,
6. Audit logs,
7. Key generation,
8. Changes to trusted Public Keys, and
9. Destruction of a cryptographic module.

5.5.2 Retention Period for Archive

Entrust retains archived data for the longer of seven years, or seven years after the date the applicable Certificate ceases to be valid.

5.5.3 Protection of Archive

Archive records are stored at a secure off-site location and are maintained in a manner that prevents unauthorized modification, substitution, or destruction. Archives are not released except as allowed by the PKI Policy Authority or as required by law. Entrust maintains any software application required to process the archive data until the data is either destroyed or transferred to a newer medium.

If Entrust needs to transfer any media to a different archive site or equipment, Entrust shall main both archived locations and/or pieces of equipment until the transfer are complete. All transfers to new archives will occur in a secure manner.

5.5.4 Archive Backup Procedures

Backups are written on at least a daily basis to a server at a secure location. In general, the process for creating, packaging, and transmitting archived records and backup copies is automated.

5.5.5 Requirements for Time-Stamping of Records

Entrust automatically time-stamps archived records with system time (non-cryptographic method) as they are created. Entrust stamps and records information collected during the identity verification process, including IP addresses associated with applicant submissions and screen shots provided by verification information sources where applicable. Certificate issuance is time-stamped as a function of the "Valid From" field in accordance with the X.509 Certificate Profile. Certificate revocation is time-stamped as a function of the "Revocation Date" field in accordance with the X.509 Certificate Revocation List Profile.

5.5.6 Archive Collection System (Internal or External)

Archive information is collected internally by Entrust.

5.5.7 Procedures to Obtain and Verify Archive Information

Upon a proper request made for a proper purpose by a Customer, its agent, or a party involved in a dispute over a transaction involving the Entrust PKI, and payment of all associated

research, retrieval, verification, and redaction costs, Entrust will create, verify, package, and send that discrete portion of the archived information that is relevant to the dispute or question involving the Entrust PKI. The integrity of archived information is verified when it is restored by, among other things, reference to the time stamps associated with such records as described in Section 5.5.5. Access and use of archive data is restricted in accordance with Entrust's internal security policies and procedures which govern the creation, verification, packaging, transmission, and storage of archive information.

5.6 Key Changeover

Key changeover procedures enable the smooth transition from expiring CA certificates to new CA certificates. Towards the end of a CA Private Key's lifetime, Entrust ceases using the expiring CA Private Key to sign certificates (well in advance of expiration) and uses the old Private Key only to sign CRLs and OCSP responder certificates. A new CA signing key pair is commissioned and all subsequently issued certificates and CRLs are signed with the new private signing key. Both the old and the new key pairs may be concurrently active. This key changeover process helps minimize any adverse effects from CA certificate expiration. The corresponding new CA Public Key certificate is provided to subscribers and relying parties through the delivery methods detailed in Section 6.1.4.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

If a disaster causes Entrust's CA operations to become inoperative, Entrust will re-initiate its operations on replacement hardware using backup copies of its software, data, and Private Keys at a comparable, secured facility after ensuring the integrity and security of the CA systems. Entrust will give priority to reestablishing the generation of certificate status information. If the Private Keys are destroyed, Entrust will reestablish operations as quickly as possible, giving priority to generating new key pairs.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

Entrust makes daily system backups and regular Private Key backups. Private Key backups are stored in a secure off-site location. If a disaster causes Entrust's CA operations to become inoperative, Entrust shall, after ensuring the integrity and security of the CA systems, re-initiate its operations on replacement hardware using backup copies of its software, data, and Private Keys at a secure facility. Entrust shall give priority to reestablishing the generation of certificate status information. If the Private Keys are destroyed, Entrust shall reestablish operations as quickly as possible, giving priority to generating new key pairs.

5.7.3 Entity Private Key Compromise Procedures

If Entrust suspects that one of its Private Keys has been comprised or lost then Entrust's PKI Policy Authority will immediately convene an emergency incident response team to assess the situation, to determine the degree and scope of the incident, and take appropriate action, including implementing Entrust's incident response plan. Specifically, Entrust will:

1. Collect all information related to the incident (and if the event is ongoing, ensure that all data is captured and recorded);
2. Begin investigating the incident and determine the degree and scope of the compromise;
3. Have its incident response team determine and report on the course of action or

strategy that should be taken to correct the problem and prevent reoccurrence;
4. If appropriate, contact government agencies, law enforcement, and other interested parties and activate any other appropriate additional security measures;
5. Notify any cross-certified entities of the compromise so that they can revoke their cross-certificates;
6. Make information available that can be used to identify which certificates and time-stamp tokens are affected, unless doing so would breach the privacy of an Entrust user or the security of Entrust's services;
7. Monitor its system, continue its investigation, ensure that data is still being recorded as evidence, and make a forensic copy of data collected;
8. Isolate, contain, and stabilize its systems, applying any short-term fixes needed to return the system to a normal operating state;
9. Prepare and circulate an incident report that analyzes the cause of the incident and documents the lessons learned; and
10. Incorporate lessons learned into the implementation of long term solutions and the Incident Response Plan.

Following revocation of the corresponding certificate and implementation of the Incident Response Plan, Entrust may generate a new key pair and sign a new certificate. Entrust will distribute the new certificate in accordance with Section 6.1.4. Entrust will cease related operations until appropriate steps have been taken to recover from the compromise and restore security. If a disaster physically damages Entrust's equipment and destroys all copies of Entrust's signature keys then Entrust will provide notice to all interested parties at the earliest feasible time.

5.7.4 Business Continuity Capabilities After a Disaster

To maintain the integrity of its services, Entrust implements data backup and recovery procedures. Entrust has developed a Business Continuity Plan (BCP). Entrust reviews and updates the BCP and supporting procedures at least annually. Entrust's systems are redundantly configured at its primary facility and are mirrored with a tertiary system located at a separate, geographically diverse location for failover in the event of a disaster.

5.8 CA Termination

Before terminating its CA activities, Entrust will:

1. Provide notice and information about the termination by sending notice by email to its customers, Application Software Vendors, and cross-certifying entities and by posting such information on Entrust's web site; and
2. Transfer all responsibilities to a qualified successor entity.

If no qualified successor entity exists, Entrust will:

1. Transfer those functions capable of being transferred to a reliable third party and arrange to preserve all relevant records with a reliable third party or a government, regulatory, or legal body with appropriate authority;
2. Revoke all certificates that are still un-revoked or un-expired on a date as specified in the notice and publish final CRLs;
3. Destroy all Private Keys; and
4. Make other necessary arrangements that are in accordance with this CPS.

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

All keys must be generated using a FIPS-approved method or equivalent international standard.

Entrust's CA key pairs are generated by multiple trusted individuals using a cryptographic hardware device as part of scripted key generation ceremony. The cryptographic hardware is evaluated to FIPS 140-1 Level 3. Activation of the hardware requires the use two-factor authentication.

The key generation ceremony is performed by Entrust personnel acting in trusted roles. Entrust creates auditable evidence during the key generation process to prove that the CPS was followed and role separation was enforced during the key generation process.

An independent auditor validates that each root key is generated in accordance with this CPS by having the auditor witness the key generation ceremony. After the root key is generated, the auditor issues a report that Entrust:

1. Documented its root key generation and protection procedures,
2. Included appropriate detailed procedures and controls in its root key generation script, and
3. Performed all of the procedures required by the root key generation script.

Subscribers must generate their keys in a secure manner that is appropriate for the certificate type.

6.1.2 Private Key Delivery to Subscriber

Entrust does not generate or deliver private keys to Subscribers or provide other Subscriber key management services.

6.1.3 Public Key Delivery to Certificate Issuer

The Subscriber generates its key pair and submits the Public Key to Entrust in a CSR as part of the certificate request process. The Subscriber’s signature is authenticated prior to issuing the certificate.

6.1.4 CA Public Key Delivery to Relying Parties

Entrust's Public Keys are provided to Relying Parties as specified in a certificate validation or path discovery policy file, as trust anchors in commercial browsers and operating system root store, and/or as roots signed by other CAs. Entrust may also distribute Public Keys that are part of an updated signature key pair as a self-signed certificate, as a new CA certificate, or in a key roll-over certificate. Relying Parties may also obtain Entrust's self-signed CA certificates from Entrust's web site.

6.1.5 Key Sizes

Entrust follows the NIST timelines in using and retiring signature algorithms and key sizes. Currently, Entrust uses the keys, signature algorithms, and hash algorithms for signing

certificates, CRLs, and certificate status server responses shown on Appendix A.

6.1.6 Public Key Parameters Generation and Quality Checking

Entrust uses a cryptomodule that conforms to FIPS 186-2 and provides random number generation and on-board generation of up to 4096-bit RSA Public Keys and a wide range of ECC curves.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

Entrust's certificates include the following key usage extension fields that specify the intended use of the certificate and technically limit the certificate's functionality in X.509v3 compliant software.

digitalSignature
keyEncipherment
dataEncipherment
keyAgreement
keyCertSign
cRLSign

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

Entrust's cryptographic modules are validated to the FIPS 140 Level 3.

6.2.2 Private Key (N Out of M) Multi-Person Control

Entrust's authentication mechanisms are protected securely when not in use and may only be accessed by actions of multiple trusted persons.

Backups of CA Private Keys are securely stored off-site and require 3 out of 5 multi-person control. Re-activation of a backed-up CA Private Key (unwrapping) requires the same security and multi-person control as when performing other sensitive CA Private Key operations.

6.2.3 Private Key Escrow

Entrust does not escrow its signature keys. Entrust does not provide private key escrow services for Subscribers.

6.2.4 Private Key Backup

Entrust's Private Keys are generated and stored inside Entrust's cryptographic module, which has been evaluated to at least FIPS 140 Level 3. When keys are transferred to other media for backup and disaster recovery purposes, the keys are transferred and stored in an encrypted form. Entrust's CA key pairs are backed up by multiple trusted individuals using a cryptographic hardware device as part of scripted and videotaped key backup process.

6.2.5 Private Key Archival

Entrust does not archive Private Keys.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

All keys must be generated by and in a cryptographic module. Private Keys are exported from the cryptographic module only for backup purposes. The Private Keys are encrypted when transferred out of the module and never exist in plaintext form. When transported between cryptographic modules, Entrust encrypts the private key and protects the keys used for encryption from disclosure. Private Keys used to encrypt backups are securely stored and require two-person access.

6.2.7 Private Key Storage on Cryptographic Module

Entrust's Private Keys are generated and stored inside Entrust's cryptographic module, which has been evaluated to at least FIPS 140 Level 3.

6.2.8 Method of Activating Private Key

Entrust's Private Keys are activated according to the specifications of the cryptographic module manufacturer during a scripted, videotaped, and witnessed key generation or certificate signing ceremony. Activation data entry is protected from disclosure.

Subscribers are solely responsible for protection of their Private Keys. Subscribers should use a strong password or equivalent authentication method to prevent unauthorized access or use of the Subscriber's Private Key.

6.2.9 Method of Deactivating Private Key

Entrust's Private Keys are deactivated via logout procedures on the applicable HSM device when not in use and are maintained in an off-line state. Entrust never leaves its HSM devices in an active unlocked or unattended state.

Subscribers should deactivate their Private Keys via logout and removal procedures when not in use.

6.2.10 Method of Destroying Private Key

Entrust personnel acting in trusted roles destroy CA Private Keys when they are no longer needed. Subscribers shall destroy their Private Keys when the corresponding certificate is revoked or expired or if the Private Key is no longer needed.

Entrust also initializes the HSM device and associated backup tokens according to the specifications of the hardware manufacturer. If the initialization procedure fails, Entrust will crush, shred, and/or incinerate the device in a manner that destroys the ability to extract any Private Key.

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Entrust archives copies of Public Keys in accordance with Section 5.5.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

See Appendix A.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Entrust activates the cryptographic module containing its CA Private Keys according to the specifications of the hardware manufacturer. This method has been evaluated as meeting the requirements of FIPS 140-2 Level 3. The cryptographic hardware is held under two-person control as explained in Section 5.2.2 and elsewhere in this CPS. Entrust will only transmit activation data via an appropriately protected channel and at a time and place that is distinct from the associated cryptographic module.

All Entrust personnel and Subscribers are instructed to use strong passwords and to protect PINs and passwords. If Entrust uses passwords as activation data for a signing key, Entrust will change the activation data change upon rekey of the CA certificate.

6.4.2 Activation Data Protection

Entrust protects data used to unlock private keys from disclosure using a combination of cryptographic and physical or logical access control mechanisms. Protection mechanisms include keeping activation mechanisms secure using role-based physical control.

6.4.3 Other Aspects of Activation Data

No provision.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

Entrust secures its CA systems and authenticates and protects communications between its systems and trusted roles. Entrust's CA servers and support-and-vetting workstations run on trustworthy systems that are configured and hardened using industry best practices. All systems are scanned for malicious code and protected against spyware and viruses.

Entrust’s systems, including any remote workstations, are configured to:

1. Authenticate the identity of users before permitting access to the system or applications,
2. Manage privileges of users to limit users to their assigned roles, and
3. Generate and archive audit records for all transactions.

6.5.2 Computer Security Rating

No provision.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

Entrust has mechanisms in place to control and monitor the acquisition and development of its CA systems. Change requests require the approval multiple authorized persons via approved RFCs under multi-person control. This allows Entrust to verify that each change to the system was properly evaluated for risk mitigation and authorized by management. Entrust only installs software on CA systems that is necessary to the CA's operation and all CA hardware and software is dedicated only to performing operations of the CA.

Vendors are selected based on their reputation in the market, ability to deliver quality product, and likelihood of remaining viable in the future. Management is involved in the vendor selection and purchase decision process. Non-PKI hardware and software is purchased without identifying the purpose for which the component will be used. All hardware and software are shipped under standard conditions to ensure delivery of the component directly to a trusted employee who ensures that the equipment is installed without opportunity for tampering.

Some of the PKI software components used by Entrust are developed in-house using standard software development methodologies. All such software is designed and developed under a formal, documented, development methodology in a controlled environment. Other software is purchased commercial off-the-shelf (COTS). Quality assurance is maintained throughout the process through testing and documentation or by purchasing from trusted vendors as discussed above.

Updates of equipment and software are purchased or developed in the same manner as the original equipment or software and are installed and tested by trusted and trained personnel. All hardware and software essential to Entrust's operations is scanned for malicious code.

6.6.2 Security Management Controls

Entrust has mechanisms in place to control and monitor the security-related configurations of its CA systems, including change control data entries that are processed, logged and tracked for any security-related changes. Entrust verifies the integrity of software used with its CA processes at least once a week.

6.6.3 Life Cycle Security Controls

No provision.

6.7 Network Security Controls

Entrust documents and controls the configuration of its systems, including any upgrades or modifications made. Entrust's CA system is connected to an internal network and is protected by firewalls and Network Address Translation for all internal IP addresses (e.g., 192.168.x.x). Entrust's customer support and vetting workstations are also protected by firewall(s) and only use internal IP addresses. Root Keys are kept offline and brought online only when necessary to sign certificate-issuing subordinate CAs, OCSP Responder Certificates, or periodic CRLs. Firewalls and boundary control devices are configured to allow access only by the addresses, ports, protocols and commands required for the trustworthy provision of PKI services by such systems.

Entrust's security policy is to block all ports and protocols and open only necessary ports to enable CA functions. All CA equipment is configured with a minimum number of services and all unused network ports and services are disabled. Entrust's network configuration is available for review on-site by its auditors and consultants under an appropriate non-disclosure agreement.

6.8 Time-Stamping

The system time on Entrust's computers is updated using the Network Time Protocol (NTP) to synchronize all system clocks.

7. CERTIFICATE, CRL, AND OCSP PROFILES

Information for interpreting the following Certificate Profiles and CRL Profiles may be found in IETF's RFC 5280. Entrust uses the ITU X.509, version 3 standard to construct digital certificates for use within the Entrust PKI. Entrust adds certain certificate extensions to the basic certificate structure for the purposes intended by X.509v3 as per Amendment 1 to ISO/IEC 9594-8, 1995.

7.1 Certificate Profile

7.1.1 Version Number(s)

All certificates are X.509 version 3 certificates.

7.1.2 Certificate Extensions

Certificate Extension	Criticality
Subject Key ID	Non-Critical
Authority Key ID	Non-Critical
Basic Constraints	Critical
Certificate Policies	Non-Critical
CRL Distribution Points	Non-Critical
Authority Information Access	Non-Critical
Key Usage	Critical
Extended Key Usage	Non-Critical
SubjectAlternativeNames	Non-Critical

7.1.3 Algorithm Object Identifiers

sha-1WithRSAEncryption	[iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5]
sha256WithRSAEncryption	[iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11]
sha384WithRSAEncryption	[iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12]
ecdsa-with-sha384	[iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures (4) ecdsa-with-SHA2 (3) 3]

Also See Appendix A.

7.1.4 Name Forms

Each certificate includes a unique serial number that is never reused. Optional subfields in the subject of an EV Certificate must either contain information verified by Entrust or be left empty. EV Certificates cannot contain metadata such as '.', '-', and ' ' characters or any other indication that the field is not applicable.

The Distinguished Name in a Certificate may contain the following information:

(1) Organization Name – Required in SSL Certificates
(2) Domain Name - Required in SSL Certificates
(3) Business Category – Required for EV Certificates
(4) Organizational Unit – Not supported unless special request
(5) Jurisdiction of Incorporation or Registration – Required in EV Certificates (as applicable)
(6) Registration Number - Required in EV Certificates
(7) Physical Address of Place of Business Number – Optional for street and postal code

The contents of the fields in EV Certificates must meet the requirements in Section 9 of the EV Guidelines.

7.1.5 Name Constraints

No provision.

7.1.6 Certificate Policy Object Identifier

An object identifier (OID) is a unique number that identifies an object or policy. The OIDs used by Entrust are listed in Section 1.2.

7.1.7 Usage Of Policy Constraints Extension

No provision.

7.1.8 Policy Qualifiers Syntax and Semantics

Entrust may include brief statements in certificates about the applicability of this CPS or limitations of liability and other terms associated with the use of a certificate in the Policy Qualifier field of the Certificates policy extension.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No provision.

7.2 CRL Profile

7.2.1 Version Number(s)

Entrust issues version 2 CRLs that conform to RFC 3280. CRLs contain the following fields:

Field	Value
Issuer Signature Algorithm	sha-1WithRSAEncryption [1 2 840 113549 1 1 5] OR sha-256WithRSAEncryption [1 2 840 113549 1 1 11] OR ecdsa-with-sha284 [1 2 840 10045 4 3]

Issuer Distinguished Name	Trend Micro
thisUpdate	CRL issue date in UTC format
nextUpdate	Date when the next CRL will issue in UTC format. The field is set to thisUpdate plus 24 hours
Revoked Certificates List	List of revoked certificates, including the serial number and revocation date
Issuer's Signature	[Signature]

7.2.2 CRL and CRL Entry Extensions

CRLs have the following extensions:

Extension	Value
CRL Number	Never repeated monotonically increasing integer
Authority Key Identifier	Same as the Authority Key Identifier listed in the certificate
Invalidity Date	Optional date in UTC format
Reason Code	Optionally included reason for the revocation

7.3 OCSP Profile

7.3.1 Version Number(s)

Entrust's OCSP responders conform to version 1 of RFC 2560.

7.3.2 OCSP Extensions

No provision.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The practices in this CPS are designed to meet or exceed the requirements of generally accepted industry standards, including the latest version of the AICPA/CICA (1) Trust Service Principles and Criteria for Certification Authorities, (2) WebTrust For Certification Authorities – Extended Validation Audit Criteria, and (3) WebTrust Principles, and Criteria for Certification Authorities – SSL Baseline with Network Security audit WebTrust Program for Certification Authorities.

8.1 Frequency or Circumstances of Assessment

Entrust has an annual audit by an independent external auditor to assess Entrust's compliance with the AICPA/CICA (1) Trust Service Principles and Criteria for Certification Authorities, (2) WebTrust For Certification Authorities – Extended Validation Audit Criteria, and (3) WebTrust Principles, and Criteria for Certification Authorities – SSL Baseline with Network Security audit WebTrust Program for Certification Authorities.

8.2 Identity/Qualifications of Assessor

Auditors must meet the requirements of Section 17.6 of the EV Guidelines and Baseline Requirements.

8.3 Assessor's Relationship to Assessed Entity

Entrust uses an independent auditor that does not have a financial interest, business relationship, or course of dealing that could foreseeably create a significant bias for or against Entrust.

8.4 Topics Covered by Assessment

The audit conforms to the WebTrust audit programs listed in Section 8.1, and covers Entrust's business practices disclosure and the integrity of Entrust's PKI operations.

8.5 Actions Taken as a Result Of Deficiency

If an audit reports any material noncompliance with applicable law, this CPS, or any other contractual obligations related to Entrust's services, then (1) the auditor will document the discrepancy, (2) the auditor will promptly notify Entrust, and (3) Entrust will develop a plan to cure the noncompliance. Entrust will submit the plan to the PKI Policy Authority for approval and to any third party that Entrust is legally obligated to satisfy. The PKI Policy Authority may require additional action if necessary to rectify any significant issues created by the non-compliance, including requiring revocation of affected certificates.

8.6 Communication of Results

The results of each audit are reported to the PKI Policy Authority and to any third party entities which are entitled by law, regulation, or agreement to receive a copy of the audit results.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

Entrust is entitled to charge Subscribers for the issuance, management, and renewal of Certificates. The fees charged will be as stated on Entrust's Web site or in any applicable Subscriber Agreement (Terms of Service) at the time the Certificate is issued or renewed, and may change from time to time without prior notice.

9.1.2 Certificate Access Fees

Entrust does not charge a fee as a condition of making Certificates available to Relying Parties.

9.1.3 Revocation or Status Information Access Fees

Entrust does not charge a fee as a condition of making the CRL or OSCP available in a repository or otherwise available to Relying Parties. Entrust does not permit access to revocation information, certificate status information, or time stamping in its repository by third parties that provide products or services that utilize such certificate status information without Entrust's prior express written consent.

9.1.4 Fees for Other Services

Entrust does not charge a fee for access to this CPS.

9.1.5 Refund Policy

A Subscriber may apply a refund for the cost of an individual certificate toward the issuance of a substitute Certificate. To obtain a substitute Certificate, the Subscriber must provide a new Certificate Signing Request to Entrust or request reissue of a Certificate based upon a prior Certificate Signing Request previously provided to Entrust by the Subscriber. As to Entrust's refund policy for enterprise Subscribers, see the terms of the Subscriber Agreement.

Entrust will not revoke a Certificate previously issued following a refund or reissue request. A request for a refund or reissue of a Certificate will not be treated as a request by the Subscriber for revocation of a Certificate previously issued by Entrust unless the Subscriber follows the procedures for requesting revocation as stated at Section 4.9.3 of this CPS.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

Entrust will maintain the insurance coverages or self-insurance for issuance of EV Certificates as required by the EV Guidelines.

9.2.2 Other Assets

No provision.

9.2.3 Insurance or Warranty Coverage for End-Entities

Entrust's warranty coverage for end-entities is specified in Subscriber Agreements and Relying Party Agreements.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

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

1. Private Keys;
2. Activation data used to access Private Keys or to gain access to the CA system;
3. Business continuity, incident response, contingency, and disaster recovery plans;
4. Other security practices used to protect the confidentiality, integrity, or availability of information;
5. Information held by Entrust as private information in accordance with Section 9.4;
6. Audit logs and archive records, including certificate application records and documentation submitted in support of certificate applications whether successful or rejected; and
7. Transaction records, financial audit records, and external or internal audit trail records and any audit reports (with the exception of an auditor's letter

confirming the effectiveness of the controls set forth in this CPS)

9.3.2 Information Not Within the Scope of Confidential Information

All information published on the Entrust website plus published certificate and revocation data is public information.

9.3.3 Responsibility to Protect Confidential Information

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

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

Entrust follows the Privacy Statement posted on its website when handling personal information. Personal information is only disclosed when required by law or when requested by the subject of personal information.

9.4.2 Information Treated as Private

Entrust treats all personal information about an individual that is not publicly available in the contents of a certificate or CRL as private information. Entrust shall protect private information in its possession using a reasonable degree of care and appropriate safeguards.

9.4.3 Information Not Deemed Private

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

9.4.4 Responsibility to Protect Private Information

All personnel involved with the Entrust PKI are expected to handle personnel information in strict confidence and meet the requirements of applicable law concerning the protection of personal data. All sensitive information is stored securely and protected against accidental disclosure.

9.4.5 Notice and Consent to Use Private Information

Personal data provided during the application, registration, and identity verification process that is not contained in Certificates is considered private information. Entrust may only use private information as part of the account registration and certificate issuance process, with the subject's express written consent, or as required by applicable law or regulation. Notwithstanding the foregoing, personal information contained in Certificates may be published in online public repositories. All Subscribers consent to the global transfer of any personal data contained in Certificates.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Entrust may disclose private information, without notice, when required to do so by law

or regulation.

9.4.7 Other Information Disclosure Circumstances

No provision.

9.5 Intellectual Property Rights

Entrust, or its Entrust Trend Micro SSL affiliates, own all intellectual property rights in Entrust Trend Micro SSL's services, including the Entrust Trend Micro SSL certificates, trademarks used in providing the services, and this CPS. "Trend Micro" is a registered trademark of Trend Micro, Inc. which is licensed to Entrust on a limited, non-exclusive for the purpose of providing Entrust Trend Micro SSL products and services.

Certificates and revocation information are the exclusive property of Entrust. Entrust grants permission to reproduce and distribute certificates on a non-exclusive, royalty-free basis, provided that they are reproduced and distributed in full. Entrust does not allow derivative works of its certificates or products without prior written permission. Private and Public Keys will remain the property of the Subscribers who rightfully hold them.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

9.6.1.1 OV Server, Code Signing, and Client (S/MIME) Certificate Limited Warranty

Entrust provides the following limited warranty at the time of issuance of OV server certificates, code signing certificates, and client (S/MIME) certificates: (i) it issued the certificate substantially in compliance with this CPS; (ii) the information contained within the certificate accurately reflects the information provided to Entrust by the Applicant in all material respects; and (iii) it has taken reasonable steps to verify that the information within the certificate is accurate. The nature of the steps Entrust takes to verify the information contained in a Certificate is set forth in Section 3 of this CPS.

Entrust provides no warranties with respect to another party's software, hardware or telecommunications or networking equipment utilized in connection with the use, issuance, revocation or management of Certificates or providing other services (including, without limitation, any support services) with respect to this CPS. Applicants, Subscribers and Relying Parties agree and acknowledge that Entrust is not responsible or liable for any misrepresentations or incomplete representations of Certificates or any information contained therein caused by another party's application software or graphical user interfaces. The cryptographic key-generation technology used by Applicants, Subscribers and Relying Parties in conjunction with the Certificates may or may not be subject to the intellectual property rights of third parties. It is the responsibility of Applicants, Subscribers and Relying Parties to ensure that they are using technology that is properly licensed or to otherwise obtain the right to use such technology.

9.6.1.2 EV Server Certificate Limited Warranty

When Entrust issues an EV Certificate, Entrust represents and warrants to the EV Certificate Beneficiaries, during the period when the EV Certificate is valid, that Entrust has followed the requirements of the EV Guidelines and its EV Policies in issuing the EV Certificate and in verifying the accuracy of the information contained in the EV Certificate ("**EV Certificate Warranties**"). The EV Certificate Warranties specifically include, but are not limited to, the following:

(1) Legal Existence. Entrust has confirmed with the incorporating or registration agency in the Subject's jurisdiction of incorporation or registration that, as of the date the EV Certificate was issued, the Subject named in the EV Certificate legally exists as a valid organization or entity in the jurisdiction of incorporation or registration;

(2) Identity. In accordance with the procedures stated in the EV Guidelines, Entrust has confirmed that, as of the date the EV Certificate was issued, the legal name of the Subject named in the EV Certificate matches the name on the official government records of the incorporating or registration agency in the Subject's jurisdiction of incorporation or registration, and if an assumed name is also included, that the assumed name is properly registered by the Subject in the jurisdiction of its place of business;

(3) Right to Use Domain Name. Entrust has taken all steps reasonably necessary to verify that, as of the date the EV Certificate was issued, the Subject named in the EV Certificate has the exclusive right to use the domain name(s) listed in the EV Certificate;

(4) Authorization for EV Certificate. Entrust has taken all steps reasonably necessary to verify that the Subject named in the EV Certificate has authorized the issuance of the EV Certificate;

(5) Accuracy of Information. Entrust has taken all steps reasonably necessary to verify that all of the other information in the EV Certificate is accurate, as of the date the EV Certificate was issued;

(6) Subscriber Agreement. The Subject named in the EV Certificate has entered into a legally valid and enforceable Subscriber Agreement with Entrust that satisfies the requirements of the EV Guidelines or the Applicant Representative has acknowledged and accepted the Terms of Use (if applicable);

(7) Status. Entrust will follow the requirements of these Guidelines and maintain a 24 x 7 online-accessible repository with current information regarding the status of the EV Certificate as valid or revoked; and

(8) Revocation. Entrust will follow the requirements of the EV Guidelines and revoke the EV Certificate upon the occurrence of any revocation event as specified in the EV Guidelines.

See the EV Guidelines for definition of defined terms above.

EV Certificates focus only on the identity of the Subject named in the Certificate, and not on the behavior of the Subject. As such, when issuing an EV Certificate, Entrust does not provide any assurances, or otherwise represent or warrant:

- That the Subject named in the EV Certificate is actively engaged in doing business;
- That the Subject named in the EV Certificate complies with applicable laws;

- That the Subject named in the EV Certificate is trustworthy, honest, or reputable in its business dealings; or
- That it is “safe” to do business with the Subject named in the EV Certificate.

9.6.2 RA Representations and Warranties

No provision.

9.6.3 Subscriber Representations and Warranties

Subscribers are solely responsible for any misrepresentations they make to third parties and for all transactions that use Subscriber’s Private Key, regardless of whether such use was authorized.

Subscribers represent to Entrust, Application Software Vendors, and Relying Parties that, for each certificate, the Subscriber will:

1. Securely generate its Private Keys, and protect its Private Keys from compromise,
2. Provide accurate and complete information when communicating with Entrust,
3. Confirm the accuracy of the certificate data prior to using the certificate,
4. Promptly cease using a certificate and notify Entrust if (i) any information that was submitted to Entrust or is included in a certificate changes or becomes misleading or (ii) there is any actual or suspected misuse or compromise of the Private Key associated with the certificate,
5. Ensure that individuals using certificates on behalf of an organization have received security training appropriate to the certificate,
6. Use the certificate only for authorized and legal purposes, consistent with the certificate purpose, this CPS, any applicable CP, and the relevant Subscriber Agreement, including only installing SSL certificates on servers accessible at the domain listed in the certificate and not using code signing certificates to sign malicious code or any code that is downloaded without a user’s consent,
7. Abide by the Subscriber Agreement and this CPS when requesting or using a Certificate, and
8. Promptly cease using the certificate and related Private Key after the certificate’s expiration.

9.6.4 Relying Party Representations and Warranties

Each Relying Party represents that, prior to relying on an Entrust certificate, it:

1. Made reasonable efforts to acquire sufficient knowledge on using digital certificates and PKI,
2. Studied the limitations on the usage of certificates and is aware of Entrust’s limitations on liability with respect to reliance on issued certificates,
3. Has read, understands, and agrees to the Relying Party Agreement and this CPS,
4. Verified both the Entrust certificate and any certificates in the certificate chain using the relevant CRL or OCSP,
5. Will not use an Entrust certificate if the certificate has expired or been revoked, and
6. Will take all reasonable steps to minimize the risk of relying on a digital signature created by an invalid, revoked, or expired certificate, including only relying on an Entrust certificate if appropriate after considering:

a) Applicable law and the legal requirements for identification of a party, protection of the confidentiality or privacy of information, and enforceability of the transaction;
b) The intended use of the certificate as listed in the certificate or this CPS,
c) The data listed in the certificate,
d) The economic value of the transaction or communication,
e) The potential loss or damage that would be caused by an erroneous identification or a loss of confidentiality or privacy of information in the application, transaction, or communication,
f) The Relying Party's previous course of dealing with the Subscriber,
g) The Relying Party's understanding of trade, including experience with computer-based methods of trade, and
h) Any other indicia of reliability or unreliability pertaining to the Subscriber and/or the application, communication, or transaction.

Any reliance on a certificate by a Relying Party that does not meet these requirements is at the party's own risk.

9.6.5 Representations and Warranties of Other Participants

No provision.

9.7 Disclaimers of Warranties

EXCEPT FOR THE LIMITED WARRANTY DESCRIBED IN SECTION 9.6.1 ABOVE, ENTRUST EXPRESSLY DISCLAIMS AND MAKES NO REPRESENTATION, WARRANTY OR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, WITH RESPECT TO THIS CPS OR ANY CERTIFICATE ISSUED HEREUNDER, INCLUDING WITHOUT LIMITATION, ALL WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE OR USE OF A CERTIFICATE OR ANY SERVICE (INCLUDING, WITHOUT LIMITATION, ANY SUPPORT SERVICES) PROVIDED BY ENTRUST AS DESCRIBED HEREIN, AND ALL WARRANTIES, REPRESENTATIONS, CONDITIONS, UNDERTAKINGS, TERMS AND OBLIGATIONS IMPLIED BY STATUTE OR COMMON LAW, TRADE USAGE, COURSE OF DEALING OR OTHERWISE ARE HEREBY EXCLUDED TO THE FULLEST EXTENT PERMITTED BY LAW. EXCEPT FOR THE LIMITED WARRANTY DESCRIBED ABOVE, ENTRUST FURTHER DISCLAIMS AND MAKES NO REPRESENTATION, WARRANTY OR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, TO ANY APPLICANT, SUBSCRIBER OR ANY RELYING PARTY THAT (A) THE SUBSCRIBER TO WHICH IT HAS ISSUED A CERTIFICATE IS IN THE FACT THE PERSON, ENTITY OR ORGANIZATION IT CLAIMS TO HAVE BEEN (B) A SUBSCRIBER IS IN FACT THE PERSON, ENTITY OR ORGANIZATION LISTED IN THE CERTIFICATE, OR (C) THAT THE INFORMATION CONTAINED IN THE CERTIFICATES OR IN ANY CERTIFICATE STATUS MECHANISM COMPILED, PUBLISHED OR OTHERWISE DISSEMINATED BY ENTRUST, OR THE RESULTS OF ANY CRYPTOGRAPHIC METHOD IMPLEMENTED IN CONNECTION WITH THE CERTIFICATES IS ACCURATE, AUTHENTIC, COMPLETE OR RELIABLE.

IT IS AGREED AND ACKNOWLEDGED THAT APPLICANTS AND SUBSCRIBERS ARE LIABLE FOR ANY MISREPRESENTATIONS MADE TO ENTRUST AND RELIED UPON BY A RELYING PARTY. ENTRUST DOES NOT WARRANT OR GUARANTEE UNDER ANY CIRCUMSTANCES THE "NON-REPUDIATION" BY A SUBSCRIBER AND/OR RELYING

PARTY OF ANY TRANSACTION ENTERED INTO BY THE SUBSCRIBER AND/OR RELYING PARTY INVOLVING THE USE OF OR RELIANCE UPON A CERTIFICATE.

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

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

9.8 Limitations of Liability

9.8.1 Applicable to OV, Code Signing, and Client (S/MIME) Certificates

EXCEPT TO THE EXTENT CAUSED BY ENTRUST'S WILLFUL MISCONDUCT, IN NO EVENT SHALL THE CUMULATIVE LIABILITY OF ENTRUST TO APPLICANTS, SUBSCRIBER AND/OR ANY RELYING PARTY FOR ALL CLAIMS RELATED TO THE INSTALLATION OF, USE OF OR RELIANCE UPON A AN OV**,** CODE SIGNING, OR CLIENT (S/MIME**)** CERTIFICATE OR FOR THE SERVICES PROVIDED HEREUNDER WHERE ENTRUST HAS NOT ISSUED OR MANAGED THE CERTIFICATE IN COMPLIANCE WITH THIS CPS, INCLUDING WITHOUT LIMITATION ANY CAUSE OF ACTION SOUNDING IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, FOR BREACH OF A STATUTORY DUTY OR IN ANY OTHER WAY EXCEED FOR SUBSCRIBERS AND RELYING PARTIES: FOR OV**,** CODE SIGNING, OR CLIENT (S/MIME) CERTIFICATES, ONE THOUSAND U.S. DOLLARS ($1,000.00) IN THE AGGREGATE ALL CLAIMS AND ALL CLAIMANTS PER CERTIFICATE.

9.8.2 Applicable to EV Certificates

EXCEPT TO THE EXTENT CAUSED BY ENTRUST'S WILLFUL MISCONDUCT, IN NO EVENT SHALL THE CUMULATIVE LIABILITY OF ENTRUST TO APPLICANTS, SUBSCRIBER AND/OR ANY RELYING PARTY FOR ALL CLAIMS RELATED TO THE INSTALLATION OF, USE OF OR RELIANCE UPON AN EV CERTIFICATE OR FOR THE SERVICES PROVIDED HEREUNDER WHERE ENTRUST HAS NOT ISSUED OR MANAGED AN EV CERTIFICATE IN COMPLIANCE WITH THIS CPS, INCLUDING WITHOUT LIMITATION ANY CAUSE OF ACTION SOUNDING IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, FOR BREACH OF A STATUTORY DUTY OR IN ANY OTHER WAY EXCEED (A) FOR SUBSCRIBERS AND RELYING PARTIES, TWO THOUSAND U.S. DOLLARS ($2,000.00) PER SUBSCRIBER OR RELYING PARTY PER EV CERTIFICATE, BUT NOT TO EXCEED $50,000 IN THE AGGREGATE FOR ALL CLAIMS FROM ALL PARTIES PER EV CERTIFICATE, OR (B) FOR ALL OTHERS, TEN THOUSAND U.S. DOLLARS ($10,000.00) IN THE AGGREGATE ALL CLAIMS AND ALL CLAIMANTS PER EV CERTIFICATE.

9.8.3 Applicable to All Certificates

ENTRUST SHALL NOT BE LIABLE IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, FOR BREACH OF A STATUTORY DUTY OR IN ANY OTHER WAY (EVEN IF ENTRUST HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) FOR:

(I) ANY ECONOMIC LOSS (INCLUDING, WITHOUT LIMITATION, LOSS OF REVENUES, PROFITS, CONTRACTS, BUSINESS OR ANTICIPATED SAVINGS);
(II) TO THE EXTENT ALLOWED BY APPLICABLE LAW, ANY LOSS OR DAMAGE RESULTING FROM DEATH OR INJURY OF SUBSCRIBER AND/OR ANY RELYING PARTY OR ANYONE ELSE;
(III) ANY LOSS OF GOODWILL OR REPUTATION; OR
(IV) ANY OTHER INDIRECT, CONSEQUENTIAL, INCIDENTAL, MULTIPLE, SPECIAL, PUNITIVE, EXEMPLARY DAMAGES;

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

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

THE FOREGOING LIMITATIONS OF LIABILITY SHALL APPLY ON A CERTIFICATE-BY-CERTIFICATE BASIS, REGARDLESS OF THE NUMBER OF TRANSACTIONS OR CLAIMS RELATED TO EACH CERTIFICATE, AND SHALL BE APPORTIONED FIRST TO THE EARLIER CLAIMS TO ACHIEVE FINAL RESOLUTION.

In no event will Entrust be liable for any damages to Applicants, Subscribers, Relying Parties or any other party arising out of or related to the use or misuse of, or reliance on any Certificate issued under this CPS that: (a) has expired or been revoked; (b) has been used for any purpose other than as set forth in the CPS; (c) has been tampered with; (d) with respect to which the Key Pair underlying such Certificate or the cryptography algorithm used to generate such Certificate's Key Pair, has been Compromised by the action of any party other than Entrust (including without limitation the Subscriber or Relying Party); or (e) is the subject of misrepresentations or other misleading acts or omissions of any other party, including but not limited to Applicants, Subscribers and Relying Parties.

In no event shall Entrust be liable to the Applicant, Subscriber, Relying Party or other party for damages arising out of any claim that a Certificate infringes any patent, trademark, copyright, trade secret or other intellectual property right of any party.

9.9 Indemnities

Unless otherwise set forth in this CPS and/or Subscriber Agreement, Applicant and Subscriber, as applicable, hereby agrees to indemnify and hold Entrust and its affiliates (including, but not limited to, its officers, directors, employees, agents, successors and assigns) harmless from any claims, actions, or demands that are caused by the use or publication of a Certificate and that

arises from (a) any false or misleading statement of fact by the Applicant (or any person acting on the behalf of the Applicant) (b) any failure by the Applicant or the Subscriber to disclose a material fact, if such omission was made negligently or with the intent to deceive; (c) any failure on the part of the Subscriber to protect its Private Key and Certificate or to take the precautions necessary to prevent the Compromise, disclosure, loss, modification or unauthorized use of the Private Key or Certificate; or (d) any failure on the part of the Subscriber to promptly notify Entrust, as the case may be, of the Compromise, disclosure, loss, modification or unauthorized use of the Private Key or Certificate once the Subscriber has constructive or actual notice of such event.

9.10 Term and Termination

9.10.1 Term

This CPS and any amendments are effective when published to Entrust's online repository and remain in effect until replaced with a newer version.

9.10.2 Termination

This CPS and any amendments remain in effect until replaced by a newer version.

9.10.3 Effect of Termination and Survival

Entrust will communicate the conditions and effect of this CPS's termination via the Entrust Repository. The communication will specify which provisions survive termination. At a minimum, responsibilities related to protecting confidential information will survive termination. Subscriber Agreements remain effective until the end of the certificate's validity, even if this CPS terminates.

9.11 Individual Notices and Communications with Participants

Entrust accepts notices related to this CPS that are addressed to the location specified in Section 2.2 of this CPS. Notices are deemed effective after the sender receives a valid acknowledgment of receipt from Entrust. If an acknowledgement of receipt is not received within five days, the sender must resend the notice in paper form to the street address specified in Section 2.2 using either a courier service that confirms delivery or via certified or registered mail with postage prepaid and return receipt requested. Entrust may allow other forms of notice in its Subscriber Agreements.

9.12 Amendments

9.12.1 Procedure for Amendment

The PKI Policy Authority determines what amendments should be made to this CPS. Amendments are made by posting an updated version of the CPS to the online repository. Controls are in place to reasonably ensure that this CPS is not amended and published without the prior authorization of the PKI Policy Authority. This CPS is reviewed at least annually.

9.12.2 Notification Mechanism and Period

Notification of amendments to this CPS are made by posting an updated version of the CPS to the online repository. Amendments may be made at any time without any prior notice period.

9.12.3 Circumstances Under Which OID Must Be Changed

If the PKI Policy Authority determines an amendment necessitates a change in an OID, then the revised version of this CPS will also contain a revised OID. Otherwise, amendments do not require an OID change.

9.13 Dispute Resolution Provisions

Prior to commencing any litigation, Entrust and all Subscribers and Relying Parties agree to seek an amicable settlement of any disputes or claims, provided that either party may commence litigation at any time to avoid prejudice to any rights under governing law.

9.14 Governing Law

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

9.15 Compliance with Applicable Law

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

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

This CPS and the Relying Party Agreement represents the entire agreement between any Relying Party and Entrust and supersedes any and all prior understandings and representations pertaining to their subject matters.

9.16.2 Assignment

Entrust may assign its rights and obligations under this CPS at any time without notice or consent. Subscribers and Relying Parties may not assign their rights or obligations under this CPS without the prior written consent of Entrust.

9.16.3 Severability

If any provision of this CPS shall be held to be invalid, illegal, or unenforceable, the validity, legality, or enforceability of the remainder of this CPS shall not in any way be affected or impaired hereby.

9.16.4 Enforcement (Attorneys' Fees and Waiver Of Rights)

A failure or delay in exercising any right or remedy hereunder shall not operate as a waiver of that right or remedy, nor shall any single or partial exercise of any right or remedy preclude any other or further exercise thereof or the exercise of any other right or remedy.

9.16.5 Force Majeure

Entrust shall not be liable for any default or delay in the performance of its obligations hereunder to the extent and while such default or delay is caused, directly or indirectly, by fire, flood, earthquake, elements of nature or acts of God, acts of war, terrorism, riots, civil disorders, rebellions or revolutions in the United States, strikes, lockouts, or labor difficulties or any other similar cause beyond the reasonable control of Entrust.

9.17 Other Provisions

9.17.1 Conflict of Provisions

This CPS and the Subscriber Agreement (Terms of Service), and the Relying Party Agreement represent the entire agreement between any Subscriber or Relying Party and Entrust and supersede any and all prior understandings and representations pertaining to their subject matters. In the event, however, of a conflict between this CPS and any other express agreement a Subscriber or Relying Party has with Entrust with respect to a Certificate, including but not limited to a Subscriber Agreement or Relying Party Agreement, such other agreement shall take precedence.

9.17.2 Fiduciary Relationships

Entrust is not an agent, fiduciary, trustee, or other representative of the Applicant or Subscriber and the relationship between Entrust and the Applicant and the Subscriber is not that of an agent and a principal. Entrust makes no representation to the contrary, either explicitly, implicitly, by appearance or otherwise. Neither the Applicant nor the Subscriber has any authority to bind Entrust by contract or otherwise, to any obligation.

APPENDIX A TO ENTRUST TREND MICRO SSL CPS

1. Entrust Trend Micro SSL Root Certificate Information:

CA Root Name	Algorithm	CA Root Size	Signature Hash	CA Root Expires	SHA Hash Thumbprint
AffirmTrust Commercial	RSA	2048	SHA 256	12/31/2030	f9 b5 b6 32 45 5f 9c be ec 57 5f 80 dc e9 6e 2c c7 b2 78 b7
AffirmTrust Networking	RSA	2048	SHA 1	12/31/ 2030	29 36 21 02 8b 20 ed 02 f5 66 c5 32 d1 d6 ed 90 9f 45 00 2f
AffirmTrust Premium	RSA	4096	SHA 384	12/31/2040	d8 a6 33 2c e0 03 6f b1 85 f6 63 4f 7d 6a 06 65 26 32 28 27
AffirmTrust Premium ECC	ECC	384	SHA 384 ECDSA	12/31/2040	b8 23 6b 00 2f 1d 16 86 53 01 55 6c 11 a4 37 ca eb ff c3 bb

Entrust will offer its certificate products from intermediate sub-CAs issued off of one or more of the above roots as indicated in the Product Offerings information described in Section 4 below.

2. Cross-Signed Intermediate sub-CAs

No provision.

3. Extended Validation (EV) OIDs:

Extended Validation (EV) Certificates will contain the following EV OIDs:

AffirmTrust Commercial Root: EV OID is 1.3.6.1.4.1.34697.2.1
AffirmTrust Networking Root: EV OID is 1.3.6.1.4.1.34697.2.2
AffirmTrust Premium Root: EV OID is 1.3.6.1.4.1.34697.2.3
AffirmTrust Premium ECC Root: EV OID is 1.3.6.1.4.1.34697.2.4

4. Entrust Trend Micro SSL Product Offerings:

Entrust's Trend Micro SSL product offerings and their specifications are as follows:

A. Server Certificate Offerings

(1) Product Name: "Entrust Trend Micro SSL" (SHA-256)

Root certificate:	AffirmTrust Commercial
Issuing sub-CA root:	Trend Micro S2 CA
Sub-CA Root key length:	2048
Certificate Types:	- Extended Validation (EV) server certificates - Organization Validated (OV) server certificates
Maximum operational period for certificate:	Up to 27 months for EV Up to 39 months for OV

(2) Product Name: "Trend Micro SSL" (SHA-1). This product has not been offered since December 31, 2015.

Root certificate:	AffirmTrust Networking
Issuing sub-CA root:	Trend Micro CA
Sub-CA Root key length:	2048
Certificate Types:	- Extended Validation (EV) server certificates - Organization Validated (OV) server certificates
Maximum operational period for certificate:	Up to 27 months for EV Up to 39 months for OV

(3) Product Name: "Trend Micro SSL Code Signing Certificates". This product is not currently being offered.

Root certificates:	AffirmTrust Commercial, AffirmTrust Networking, AffirmTrust Premium, AffirmTrust Premium ECC
Issuing sub-CA root:	Trend Micro S2 CA
Sub-CA Root key length:	2048
Certificate Types:	Code Signing certificates
Maximum operational period for certificate:	Two years

(4) Product Name: "Trend Micro SSL Client Certificates". This product is not currently being offered.

Root certificates:	AffirmTrust Commercial, AffirmTrust Networking, AffirmTrust Premium, AffirmTrust Premium ECC
Issuing sub-CA root:	Trend Micro S2 CA
Sub-CA Root key length:	2048
Certificate Types:	Client (S/MIME) certificates
Maximum operational period for certificate:	Two years

B. Test Certificates

Test certificates may be issued from any existing intermediate Sub-CA root certificate, but such test certificates will be restricted in their use solely to test or demonstration environments.