TREND MICRO SSL

CERTIFICATION PRACTICE STATEMENT

Version 1.7

Effective Date: 11 November 2014

TREND MICRO SSL
CERTIFICATION PRACTICE STATEMENT

VERSION 1.7
EFFECTIVE DATE: 11 NOVEMBER 2014

TABLE of CONTENTS

1. INTRODUCTION

1.1 Overview

This Trend Micro SSL Certification Practice Statement (the "CPS"), Version 1.7, effective date: 11 November 2014, presents the principles and procedures Trend Micro SSL employs in the issuance and life cycle management of the Trend Micro SSL roots, sub-roots, and certificates listed on Appendix A.

This CPS and any and all amendments thereto are incorporated by reference into all of the Trend Micro SSL Certificates listed on Appendix A. Trend Micro SSL's CPS is available on Trend Micro's website at http://ssl.trendmicro.com/resources/.

Trend Micro SSL 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 Trend Micro SSL customers. Subscribers include all parties who contract with the Trend Micro SSL for digital certificate services. All parties who may rely upon the certificates issued by Trend Micro SSL are considered relying parties.

This certification practice statement (CPS) and other Trend Micro SSL business practices disclosures are applicable to all certificates issued by Trend Micro SSL.

IANA has assigned the following OID to Trend Micro SSL: 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 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.

1.2 Definitions

For the purposes of this CPS, all capitalized terms used herein shall have the meaning given to them in Section 8, Definitions, or elsewhere in this CPS.

1.3 Description and Use of Certificates

Trend Micro SSL certificates and their uses are described below. Trend Micro SSL currently issues only the types of certificates and specific products as listed on Appendix A.

1.3.1 Trend Micro SSL Server Certificates

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. 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") published at http://www.cabforum.org, and implements the Baseline Requirements and EV Guidelines through this CPS and Trend Micro SSL’s other policies. In the event of any inconsistency between Trend Micro SSL’s other policies and the Baseline Requirements or EV Guidelines, the Baseline Requirements and EV Guidelines take precedence.

Trend Micro SSL does not issue EV wildcard server certificates.

In order to use a server certificate, the appropriate server software must support SSL.

1.3.2 Trend Micro SSL Client (S/MIME) Certificates

Trend Micro SSL Client (S/MIME) Certificates are typically used for authentication purposes, signing, and encryption of electronic mail and digital documents. They may also be referred to as S/MIME certificates and may be used for all purposes mentioned above or only for individual usage depending on the key usage limitations found in the Certificate.

1.3.3 Trend Micro SSL Code Signing Certificates

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.

1.3.4 Operational Period of Certificates

Trend Micro SSL Certificates have an Operational Period as listed on Appendix A for each product from the date of issuance, unless the Certificate is revoked prior to the expiration of the Certificate's Operational Period.

2. GENERAL PROVISIONS

2.1 Obligations for All Certificates

2.1.1 Trend Micro SSL Obligations

Trend Micro SSL will: (a) issue Certificates in accordance with this CPS; (b) perform authentication of Subscribers as described in this CPS; (c) revoke Certificates as described in this CPS; and (d) perform any other functions which are described within this CPS.

2.1.2 Subscriber Obligations

Subscribers are required to(a) submit truthful information about itself and its business entity, domain ownership and contacts, as applicable, (b) at all times abide by this CPS and the terms and conditions of the Subscriber Agreement, (c) safeguard their private key from Compromise, (d) use Certificates only for legal purposes, and (e) immediately request revocation of a Certificate if the related Private Key is Compromised. The Subscriber is solely responsible for the protection of its Private Key and for notifying Trend Micro SSL immediately in the event that its Private Key has been Compromised.

2.1.3 Relying Party Obligations

Relying Parties are obligated to: (a) Restrict reliance on certificates issued by the CA to the purposes for those certificates, in accordance with this CPS, (b) Verify the status of certificates at the time of reliance by examining the CRL and OSCP before initiating a transaction involving such Certificate, (c) 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 (d) agree to be bound by Trend Micro SSL's Relying Party Agreement at http://ssl.trendmicro.com/resources/.Trend Micro SSL does not accept responsibility for reliance on a fraudulently obtained Certificate or a Certificate that is on the CRL or OCSP.

2.2 Fees

2.2.1 Issuance, Management, and Renewal Fees

Trend Micro SSL is entitled to charge Subscribers for the issuance, management, and renewal of Certificates. The fees charged will be as stated on Trend Micro SSL's Web site or in any applicable contract at the time the Certificate is issued or renewed, and may change from time to time without prior notice.

2.2.2 Certificate Access Fees

Trend Micro SSL does not charge a fee as a condition of making Certificates available to Relying Parties.

2.2.3 Revocation or Status Information Fees

Trend Micro SSL does not charge a fee as a condition of making the CRL or OSCP required by CPS Section 2.9 available in a repository or otherwise available to Relying Parties. Trend Micro SSL 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 Trend Micro SSL's prior express written consent.

2.2.4 Fees for Other Services Such as Policy Information

Trend Micro SSL does not charge a fee for access to this CPS.

2.2.5 Refund and Reissue Policy

A Subscriber may apply a refund toward the issuance of a substitute Certificate. To obtain a substitute Certificate, the Subscriber must provide a new Certificate Signing Request to Trend Micro SSL or request reissue of a Certificate based upon a prior Certificate Signing Request previously provided to Trend Micro SSL by the Subscriber.

Trend Micro SSL 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 Trend Micro SSL unless the Subscriber follows the procedures for requesting revocation as stated at Section 3.10 of this CPS.

2.3 Compliance Audit

An annual WebTrust for Certification Authorities examination and Extended Validation WebTrust for Certification Authorities examination will be performed for the Certificates issued under this CPS. In the case of Certificates issued by Trend Micro SSL from a sub-root cross-signed by the root certificate of another Certification Authority, Trend Micro SSL will also rely on the annual WebTrust for Certification Authorities examination and Extended Validation WebTrust for Certification Authorities examination performed by that Certification Authority.

Trend Micro SSL's WebTrust audits are performed by a public accounting firm that (1) is independent of Trend Micro SSL and demonstrates proficiency in public key infrastructure technology, information security tools and techniques, security auditing, and the third-party attestation function, and (2) is accredited by the American Institute of Certified Public Accountants (AICPA), which requires the possession of certain skill sets, quality assurance measures such as peer review, competency testing, standards with respect to proper assignment of staff to engagements, and requirements for continuing professional education. The scope of Trend Micro SSL's annual WebTrust for

Certification Authorities examination will include certificate life cycle management and CA business practices disclosure.

With respect to WebTrust audits of Trend Micro SSL's operations, significant exceptions or deficiencies identified during the WebTrust audit will result in a determination of actions to be taken. This determination is made by Trend Micro SSL's PKI Policy Authority with input from the auditor. Trend Micro SSL's PKI Policy Authority is responsible for developing and implementing a corrective action plan. If Trend Micro SSL determines that such exceptions or deficiencies pose an immediate threat to the security or integrity of the Certificates issued under this CPS, a corrective action plan will be developed within 30 days and implemented within a commercially reasonable period of time. For less serious exceptions or deficiencies, Trend Micro SSL's PKI Policy Authority will evaluate the significance of such issues and determine the appropriate course of action. Results of the WebTrust audit of Trend Micro SSL's operations may be released at the discretion of Trend Micro SSL's PKI Policy Authority.

Trend Micro SSL also performs periodic internal audits performed by Trend Micro SSL personnel according to Trend Micro SSL's policies and procedures and the Baseline Requirements and EV Guidelines. Results of the periodic audits are presented to Trend Micro SSL's PKI Policy Authority with a description of any deficiencies noted and corrective actions taken.

2.4 Limited Warranty/Disclaimer

2.4.1 DV and OV Server Certificate, Email (S/MIME) Certificate, and Code Signing Certificate Limited Warranty

Trend Micro SSL provides the following limited warranty at the time of issuance of DV and OV server certificates, email (S/MIME) certificates, and code signing 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 Trend Micro SSL 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 Trend Micro SSL takes to verify the information contained in a Certificate is set forth in Section 3 of this CPS.

2.4.2 EV Server Certificate Limited Warranty

When Trend Micro SSL issues an EV Certificate, Trend Micro SSL represents and warrants to the EV Certificate Beneficiaries, during the period when the EV Certificate is valid, that Trend Micro SSL 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. Trend Micro SSL 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, Trend Micro SSL 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. Trend Micro SSL 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. Trend Micro SSL 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. Trend Micro SSL 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 Trend Micro SSL that satisfies the requirements of the EV Guidelines or the Applicant Representative has acknowledged and accepted the Terms of Use (if applicable);

(7) Status. Trend Micro SSL 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. Trend Micro SSL 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, Trend Micro SSL 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.

2.4.3 Disclaimer

EXCEPT FOR THE LIMITED WARRANTY DESCRIBEDIN SECTIONS 2.4.1 AND 2.4.2ABOVE, TREND MICRO SSL 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 TREND MICRO SSL 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, TREND MICRO SSL 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 TREND MICRO SSL, 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 TREND MICRO SSL AND RELIED UPON BY A RELYING PARTY. TREND MICRO SSL 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. TREND MICRO SSL 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 3.10 OF THIS CPS.

Trend Micro SSL 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 Trend Micro SSL 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

2.5 Limitation on Liability

2.5.1 Applicable to DV and OV Certificates, Email (S/MIME) Certificates, and Code Signing Certificates

EXCEPT TO THE EXTENT CAUSED BY TREND MICRO SSL'S WILLFUL MISCONDUCT, IN NO EVENT SHALL THE CUMULATIVE LIABILITY OF TREND MICRO SSL TO APPLICANTS, SUBSCRIBER AND/OR ANY RELYING PARTY FOR ALL CLAIMS RELATED TO THE INSTALLATION OF, USE OF OR RELIANCE UPON A DV OR AN OV CERTIFICATE, AN EMAIL (S/MIME) CERTIFICATE, OR A CODE SIGNING CERTIFICATE, OR FOR THE SERVICES PROVIDED HEREUNDER WHERE TREND MICRO SSL 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: (A) FOR DV CERTIFICATES, ONE HUNDRED U.S. DOLLARS ($100.00) IN THE AGGREGATE ALL CLAIMS AND ALL CLAIMANTS PER CERTIFICATE, (B) FOR OV CERTIFICATES, ONE THOUSAND U.S. DOLLARS ($1,000.00) IN THE AGGREGATE ALL CLAIMS AND ALL CLAIMANTS PER CERTIFICATE, AND (C) FOR CODE SIGNING CERTIFICATES, TEN THOUSAND U.S. DOLLARS ($10,000.00) IN THE AGGREGATE ALL CLAIMS AND ALL CLAIMANTS PER CERTIFICATE.

2.5.2 Applicable to EV Certificates

EXCEPT TO THE EXTENT CAUSED BY TREND MICRO SSL'S WILLFUL

MISCONDUCT, IN NO EVENT SHALL THE CUMULATIVE LIABILITY OF TREND MICRO SSL 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 TREND MICRO SSL 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, TWOTHOUSAND U.S. DOLLARS ($2,000.00) PER SUBSCRIBER OR RELYING PARTY 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.

2.5.3 Applicable to All Certificates

TREND MICRO SSL SHALL NOT BE LIABLE IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, FOR BREACH OF A STATUTORY DUTY OR IN ANY OTHER WAY (EVEN IF TREND MICRO SSL 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 Trend Micro SSL 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 (See Section 1.3 for more detail); (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 Trend Micro SSL (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 Trend Micro SSL 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.

2.6 Force Majeure

Trend Micro SSL 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, strikes, lockouts, or labor difficulties or any other similar cause beyond the reasonable control of Trend Micro SSL.

2.7 Financial Responsibility

2.7.1 Fiduciary Relationships

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

2.7.2 Indemnification by Applicant and Subscriber

Unless otherwise set forth in this CPS and/or Subscriber Agreement, Applicant and Subscriber, as applicable, hereby agrees to indemnify and hold Trend Micro SSL (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 Trend Micro SSL, 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.

2.7.3 Insurance for EV Certificates

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

2.8 Interpretation & Enforcement

2.8.1 Governing Law

North America: If you are located in the United States or Canada, the Trend Micro Entity is: Trend Micro Incorporated, 225 E. John Carpenter Freeway, Suite 1500, Irving, Texas 75062 U.S.A. Fax: (408) 257-2003 and the enforceability, construction, interpretation, and validity of this Agreement and any Certificates issued under this Agreement shall be governed by the substantive laws of the State of California, USA.

Latin America: If you are located in Spanish Latin America (other than in any countries embargoed by the U.S.), the Trend Micro Entity is: Trend Micro Latinoamérica, S. A. de C. V., Insurgentes Sur No. 813, Piso 11, Col. Nápoles, 03810 México, D. F. Tel: 3067-6000 and the enforceability, construction, interpretation, and validity of this Agreement and any Certificates issued under this Agreement shall be governed by the substantive laws of Mexico. If you are located in Brazil, the Trend Micro Entity is Trend Micro doBrasil, LTDA, RuaJoaquimFloriano, 1.120 – 2º andar, CEP 04534-004, São Paulo/Capital, Brazil and the enforceability, construction, interpretation, and validity of this Agreement and any Certificates issued under this Agreement shall be governed by the substantive laws of Brazil.

Europe, Middle East and Africa: If you are located in the United Kingdom, the enforceability, construction, interpretation, and validity of this Agreement and any Certificates issued under this Agreement shall be governed by the substantive laws of England and Wales. If you are located in Austria, Germany or Switzerland, the enforceability, construction, interpretation, and validity of this Agreement and any Certificates issued under this Agreement shall be governed by the substantive laws of the Federal Republic of Germany. If you are located in France, the enforceability, construction, interpretation, and validity of this Agreement and any Certificates issued under this Agreement shall be governed by the substantive laws of France. If you are located in Italy, the enforceability, construction, interpretation, and validity of this Agreement and any Certificates issued under this Agreement shall be governed by the substantive laws of Italy. If you are located in Europe, the Trend Micro Entity is: Trend Micro EMEA Limited, a company incorporated in Ireland under number 364963 and having its registered office at IDA Business and Technology Park, Model Farm Road, Cork, Ireland. Fax: +353-21 730 7 ext. 373.

If you are located in Africa or the Middle East (other than in those countries embargoed by the U.S.), or Europe (other than Austria, France, Germany, Italy, Switzerland or the U.K.), the Trend Micro Entity is: Trend Micro EMEA Limited, a company incorporated in Ireland under number 364963 and having its registered office at IDA Business and Technology Park, Model Farm Road, Cork, Ireland. Fax: +353-21 730 7 ext. 373 and the enforceability, construction, interpretation, and validity of this Agreement and any Certificates issued under this Agreement shall be governed by the substantive laws of the Republic of Ireland.

Asia Pacific (other than Japan or any countries embargoed by the U.S.): If you are located in Australia or New Zealand, the Trend Micro Entity is: Trend Micro Australia Pty Limited, Suite 302, Level 3, 2-4 Lyon Park Road, North Ryde, New South Wales, 2113, Australia, Fax: +612 9887 2511 or Tel: +612 9870 4888 and the enforceability, construction, interpretation, and validity of this Agreement and any Certificates issued under this Agreement shall be governed by the substantive laws of New South Wales, Australia.

If you are located in the People's Republic of China, the Trend Micro Entity is Trend Micro (China) Inc., 8th Floor, Century Ba-shi Building, No. 398 Huai Hai Zhong Road, Shanghai, China 20020, and the enforceability, construction, interpretation, and validity of this Agreement and any Certificates issued under this Agreement shall be governed by the substantive laws of People's Republic of China laws, and you agree that any dispute related to this Agreement must be submitted to the Beijing Arbitration Commission, Tel: 86-21-63848899, If you are located in Hong Kong, India, Indonesia, Malaysia, the Philippines, Singapore, Taiwan or Thailand, the Trend Micro Entity is: Trend Taiwan Incorporated, 8F, No.198, Tun-Hwa S. Road, Sec. 2, Taipei 106, Taiwan, Republic of China. If you are located in Hong Kong, the enforceability, construction, interpretation, and validity of this Agreement and any Certificates issued under this Agreement shall be governed by the substantive laws of Hong Kong. If you are located in India, the enforceability, construction, interpretation, and validity of this Agreement and any Certificates issued under this Agreement shall be governed by the substantive laws of India. If you are located in Indonesia, Malaysia, the Philippines, Singapore, or Thailand, the enforceability, construction, interpretation, and validity of this Agreement and any Certificates issued under this Agreement shall be governed by the substantive laws of Singapore. If you are located in Taiwan, the enforceability, construction, interpretation, and validity of this Agreement and any Certificates issued under this Agreement shall be governed by the substantive laws of Taiwan.

Japan: If you are located in Japan, the Trend Micro Entity is Trend Micro Incorporated, Shinjuku MAYNDS Tower, 1-1 Yoyogi 2-Chome, Shibuya-ku, Tokyo 151-0053, Japan and this agreement is governed by laws of Japan.

The United Nations Convention on Contracts for the International Sale of Goods and the conflict of laws' provisions of your state or country of residence do not apply to this Agreement under the laws of any country.

2.8.2 Dispute Resolution Procedures

Prior to commencing any litigation, Trend Micro and you 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 the governing law.

2.8.3 Conflict of Provisions

This CPS and the Subscriber Agreement (Terms of Service) represents the entire agreement between any Subscriber and Trend Micro SSL and supersedes 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 has with Trend Micro SSL with respect to a Certificate, including but not limited to a Subscriber Agreement, such other agreement shall take precedence.

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

2.8.4 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.

2.9 Repository, CRL, and OCSP

With regard to Trend Micro SSL Certificates, Trend Micro SSL shall operate one or more CRLs and OCSP that will be available to both Subscribers and Relying Parties. End-entity certificate CRLs will be updated and reissued at least every seven days, and the next Update field value will not be more than ten days, except as otherwise provided in Trend Micro SSL's Business Continuity Plan. Each CRL is signed by the issuing Trend Micro SSL sub-CA root listed on Appendix A. The procedures for revocation are as stated elsewhere in this CPS. Trend Micro SSL shall provide revocation information for end-entity EV Certificates via an OCSP service that is updated at least every four days, and OCSP responses from this service will have a maximum expiration time of ten days. Revoked Certificates will not be removed from the CRL and OCSP until after the expiration date of the revoked Certificate.

With regard to Trend Micro SSL's sub-CA roots listed on Appendix A, Trend Micro SSL will post a CRL at least every 12 months that will be available to both Subscribers and Relying Parties.

Trend Micro SSL retains copies of all Certificates for the life of the CA, but does not archive or retain expired or superseded CRLs. Trend Micro SSL does not provide a Repository or directory making end-entity Certificates available to Relying Parties.

2.10 Confidentiality Policy

2.10.1 Individual Subscriber Information

Except as provided herein, information regarding Applicants or Subscribers that is submitted on enrollment forms for Certificates will be kept confidential by Trend Micro SSL (such as contact information for individuals and credit card information) and Trend Micro SSL shall not release such information without the prior consent of the Applicant or Subscriber. Notwithstanding the foregoing, Trend Micro SSL may make such information available (a) to courts, law enforcement agencies or other third parties (including release in response to civil discovery) upon receipt of a court order or subpoena or upon the advice of Trend Micro SSL's legal counsel, (b) to law enforcement officials and others for the purpose of investigating suspected fraud, misrepresentation, unauthorized access, or potential illegal activity by the Subscriber in the opinion of Trend Micro SSL and (c) to third parties as may be necessary for Trend Micro SSL to perform its responsibilities under this Agreement. The foregoing confidentiality obligation shall not apply, however, to information appearing on Certificates, information relating to Certificate revocation, or to information regarding Subscribers that is already in the possession of or separately acquired by Trend Micro SSL.

2.10.2 Aggregate Subscriber Information

Notwithstanding the previous Section, Trend Micro SSL may disclose Subscriber information on an aggregate basis, and the Subscriber hereby grants to Trend Micro SSL a license to do so, including the right to modify the aggregated Subscriber information and to permit third parties to perform such functions on its behalf. Trend Micro SSL shall not disclose to any third party any personally identifiable information about any Subscriber that Trend Micro SSL obtains in its performance of services hereunder.

2.11 Waiver

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.

2.12 Survival

The following sections shall survive Certificate expiration or revocation, along with all definitions required thereby: Sections 1, 2, and 8.

2.13 Export

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. Trend Micro SSL may refuse to issue or may revoke Certificates if in the reasonable opinion of Trend Micro SSL such issuance or the continued use of such Certificates would violate applicable laws and regulations.

2.14 Intellectual Property Rights

Trend Micro SSL's Public Key Certificates, this CPS, CRLs, and OCSP issued by Trend Micro SSL are the property of Trend Micro, Inc.

3. OPERATIONAL REQUIREMENTS

3.1. Server Certificates

3.1.1 Domain Validated (DV) Server Certificates

(a) Application Procedure

An Applicant for a Domain Validated (DV) Server Certificate shall complete a Trend Micro SSL enrollment form or online application in a form prescribed by Trend Micro SSL. All enrollment forms are subject to review, approval and acceptance by Trend Micro SSL. All Applicants are required to include a Domain Name within the DV Certificate enrollment form. Trend Micro SSL does not verify the authority of the Subscriber to request a Certificate. Trend Micro SSL 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

Trend Micro SSL will verify that the Subscriber has control over such Domain Name at the time it submitted its application. To do this, Trend Micro SSL will perform one of the following three verification processes:

(1) Send an e-mail message to a limited list of the most commonly used generic e-mail addresses for authorized persons at domain names (e.g., "*admin@domain.com*," or "*hostmaster@domain.com*" for the domain name domain.com)requesting confirmation of the Certificate order and authorization to issue the Certificate in the Domain Name. The list in the preceding sentence is case-insensitive. However, when the email verification message is sent, it will be sent to the address with the same capitalization as specified by the Subscriber. For example, if a Subscriber requests that validation be sent to PostMaster@domain.com, the verification message will be sent to PostMaster@domain.com, with the capitalization that was specified by the certificate subscriber; or

(2) An e-mail address listed for the Domain Name in an official Inter NIC domain name registry.

Upon receipt of a confirming e-mail message authorizing issuance of the Certificate, Trend Micro SSL will issue the Certificate to the Subscriber.

(3) Send the Applicant a unique phrase, or image ("Test Phrase") by email and request that the Applicant add the Test Phrase to a specific page and location on the Applicant's website. Upon successful placement of the Test Phrase on the Applicant's website as requested by Trend Micro SSL, Trend Micro SSL will issue the Certificate to the Subscriber.

(c) Certificate Profile

DV Server Certificates will be issued from intermediate Sub-CA root certificate with the following name “[Root Name] Domain Validated CA” or similar name, and will generally contain the following Subscriber Certificate Profile:

Common Name (CN)	[Authenticated domain name]
Organization (O)	[Authenticated domain name]

3.1.2 Organization Validated (OV) Server Certificates

(a) Application Procedure

An Applicant for an Organization Validated (OV) Certificate shall complete a Trend Micro SSL enrollment form or online application in a form prescribed by Trend Micro SSL. All enrollment forms are subject to review, approval and acceptance by Trend Micro SSL. All Applicants are required to include a Domain Name or IP address within the enrollment form and an Organizational Name that will also appear on the Certificate. A Certificate may contain additional information as well. Trend Micro SSL does not verify the authority of the Subscriber to request a Certificate. Trend Micro SSL 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) Domain Name or IP Address. Trend Micro SSL will verify that the Subscriber had the right to use the Domain Name or IP Address submitted by the Subscriber at the time it submitted its application. For instance, Trend Micro SSL may perform this verification by confirming that the Subscriber is the same person or entity that holds the Domain Name registration from the relevant domain name registrar or that the Subscriber is otherwise authorized to use such Domain Name. For authentication of IP addresses, Trend Micro SSL will generally follow one of the procedures outlined at Section 11.1.2 of the CA-Browser Forum Baseline Requirements.

(2) Organizational Name. Trend Micro SSL will take reasonable steps to establish that a Certificate request made on behalf of that Organization is legitimate and properly authorized. Trend Micro SSL will ensure the following: (a) the Organizational Name appears in conjunction with a country and possibly a state or province or other locality to sufficiently identify its place of registration or a place where it is currently doing business; and (b) in the case of an Organization that could reasonably be expected to be registered with a local, state or national authority, in certain circumstances Trend Micro SSL will obtain, view and verify copies of the registration documents. For instance, Trend Micro SSL may (w) verify the validity of the registration through the authority that issued it, or (x) verify the validity of the registration through a reputable third party database or other

resource, or (y) verify the validity of the Organization through a trusted third party, or (z) confirm that the Organization exists if such Organization is not the type that is typically registered or is capable of being verified under sub-item(y).

In addition, if Trend Micro SSL determines in its discretion that additional verification is required to prove that a Certificate is duly authorized by the Organization, Trend Micro SSL may request the name of a Contact Person who is employed by or is an officer of the Organization. Trend Micro SSL may also require a form of authorization from the Organization confirming its intent to obtain a Certificate and document the Organization's Contact Person. Trend Micro SSL may also confirm the contents of this authorization with the listed Contact Person by telephone using the main telephone number of the Organization as found by Trend Micro SSL from a reputable third party data base.

Trend Micro SSL may also use other verification techniques in its discretion if it determines additional verification is required to prove that a Certificate is duly authorized by the Organization.

(c) Certificate Profile

OV Server Certificates will be issued from intermediate Sub-CA root certificate with the following name "[Root Name] Organization Validated CA" or similar name, and will generally contain the following Subscriber Certificate Profile:

Common Name (CN)	[Authenticated domain name]
Organizational Unit (OU)	[Subscriber-provided department or division name (optional)]
Organization (O)	[Authenticated organization name]
Locality (L)	[Subscriber's locality]
State or Province (ST)	[Subscriber's state or province]
Country (C)	[Subscriber's country]

3.1.3 Extended Validation (EV) Server Certificates

Authentication of Applicants or Subscribers for Extended Validation Server Certificates will follow the processes and requirements of the Extended Validation Guidelines as published by the CA-Browser Forum, as such Guidelines may be updated from time to time. For a copy of the Guidelines, see www.cabforum.org.

EV Server Certificates will be issued from intermediate Sub-CA root certificate with the following name "[Root Name] Extended Validation CA" or similar name, and will generally contain the following Subscriber Certificate Profile:

Common Name (CN)	[Authenticated domain name]
Organizational Unit (OU)	[Subscriber-provided department or division name (optional)]

Organization (O)	[Authenticated organization name]
Locality (L)	[Subscriber's locality]
State or Province (ST)	[Subscriber's state or province]
Country (C)	[Subscriber's country]
Type of Organization	["Private Organization", "Government Entity", "Business Entity", or "Non-Commercial Entity" – as per EV Guidelines Sec. 9.2.4]
Jurisdiction of Incorporation or Registration	[As per EV Guidelines Sec. 9.2.5]
Registration Number	[As per EV Guidelines Sec. 9.2.6]

3.2. Email (S/MIME) Certificates

3.2.1 Application Procedure

An Applicant for an Email (S/MIME) Certificate shall complete a Trend Micro SSL enrollment application or online application on behalf of Subscriber in a form prescribed by Trend Micro SSL. All applications are subject to review, approval and acceptance by Trend Micro SSL. 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. Trend Micro SSL does not otherwise verify the accuracy of the information contained in the Applicant's enrollment form or otherwise check for errors and omissions.

3.2.2 Authentication Process

Trend Micro SSL 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. In addition, if Trend Micro SSL determines in its discretion that additional verification is required to prove that a Certificate is duly authorized by the Applicant, Trend Micro SSL 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 Certificate Profile

Email Certificates will be issued from intermediate Sub-CA root certificate with the following name "[Root Name] Email Certificate CA" or similar name, and will generally contain the following Subscriber Certificate Profile:

Common Name (CN)	[Person's name]
Organizational Unit (OU)	[Person's organization affiliation (optional)]
Organization (O)	[Authenticated organization name (optional)]
Locality (L)	[Subscriber's locality]
State or Province (ST)	[Subscriber's state or province]
Country (C)	[Subscriber's country]
Email (E)	[Subscriber email address]

3.3 Code Signing Certificates

3.3.1 Application Procedure

An Applicant for a Code Signing Certificate shall complete a Trend Micro SSL enrollment form or online application in a form prescribed by Trend Micro SSL. All enrollment forms are subject to review, approval and acceptance by Trend Micro SSL. 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). Trend Micro SSL 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.

3.3.2 Authentication Process

(a) For Organizations

For Code Signing Certificates requested in the name of an Organization: Trend Micro SSL will follow the procedures stated at Section 3.1.2 (b) (2) above for OV Server Certificates. In addition, the identity of the individual requesting the certificate on behalf of the Organization will be verified by the methods stated in Section 3.3.2 (b) below. The authority of the Individual to request and receive the Code Signing Person will be confirmed with the Contact Person referred to in Section 3.1.2 (b) (2).

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].

(b) For Individuals

For Code Signing Certificates requested in the name of an Individual: Trend Micro SSL 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 Trend Micro SSL to confirm the Individual's identity through a reputable third party database or other resource. In addition, Trend Micro SSL 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. Trend Micro SSL 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, Trend Micro SSL 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.

Trend Micro SSL 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.

3.3.3 Certificate Profile

Code Signing Certificates will be issued from intermediate Sub-CA root certificate with the following name "[Root Name] Code Signing CA" or similar name, and will generally contain the following Subscriber Certificate Profile:

Common Name (CN)	[Authenticated organization or individual name]
Organizational Unit (OU)	[Subscriber-provided department or division name (optional)]
Organization (O)	[Authenticated organization or individual name]
Locality (L)	Subscriber's locality
State or Province (ST)	Subscriber's state or province
Country (C)	Subscriber's country

3.4 Procedure for Processing Certificate Applications

Subscribers submit their Public Key to Trend Micro SSL for certification electronically through the use of a PKCS#10 Certificate Signing Request (CSR) or other package digitally signed by the Subscriber's Private Key in a session secured by Secure Sockets Layer (SSL). At a minimum, the Subscriber must provide the following data in or with the CSR:

For DV Server Certificates:	Common Name
For OV Server Certificates:	Common Name, Organization, and Country
For EV Server Certificates:	Common Name, Organization, State or Province, and Country
For Email (S/MIME) Certificates:	Email
For Code Signing Certificates:	Common Name, Organization (or Individual Name, if no Organization), State or Province, and Country

The following additional information is required on the enrollment form: the names, e-mail addresses, and telephone numbers for the Administrative, Technical, Support, and Billing points of contact.

Trend Micro SSL will process the Certificate enrollment forms to confirm the information on the Certificates using the procedures described above. Trend Micro SSL reserves the right to modify such procedures and issue a Certificate utilizing different authentication procedures in certain circumstances; provided that (a) the general principles for verifying the application information is maintained, and (b) and such issuance is approved by a Trend Micro SSL Director Level or above as being equivalent to or stronger than the standard procedures.

3.5 Application Issues

At certain times during the application process in which Trend Micro SSL is not able to verify information in an enrollment form, a customer service representative may be assigned to the applicant to facilitate the completion of the application process. Otherwise, the applicant may be required to correct its associated information with third parties and re-submit its enrollment form for a Certificate.

Trend Micro SSL will check all Certificate requests against lists of high risk certificate requests and certificate requests previously denied, and may take additional precautions or deny a Certificate request as a result.

3.6 Certificate Delivery

If Trend Micro SSL finds that the applicant's enrollment form was sufficiently verified, then the applicant's Certificate will be signed by Trend Micro SSL. Upon signing the applicant's Certificate, Trend Micro SSL will attach such Certificate to an e-mail and send such e-mail to the appropriate contacts or make the Certificate available via the Application Programming Interface (API). The e-mail will typically be sent to the administrative contact, technical contact and billing contact designated by the Subscriber. Delivery of EV Server Certificates may be by different procedures as specified in the EV Guidelines.

Notification will not be sent to others than the subject of the Certificate and the subject's designated contacts. In certain circumstances the e-mail may include a Trend Micro SSL customer service representative telephone number and e-mail address for any technical

or customer service problems. Trend Micro SSL, in its sole discretion, may provide such technical or customer support to the applicants/Subscribers. Trend Micro SSL does not distribute Certificates via Integrated Circuit Cards (ICC) to Subscribers.

3.7 Certificate Acceptance

The applicant expressly indicates acceptance of a Certificate by using such Certificate.

3.8 Certificate Renewal and Rekey

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to obtain a new Certificate to maintain continuity of Certificate usage. Subscribers have the option of generating a new Key Pair to replace the expiring Key Pair (technically defined as "rekey") or of creating a new Certificate Signing Request for an existing Key Pair (technically defined as "renewal"), depending on their preferences and the capabilities and restrictions of the Subscriber's web server and web server key generation tools. For purposes of this CPS, both a "rekey" and "renewal" as defined above will be treated as a renewal Certificate. Rekey after revocation or expiration is not supported.

Renewal Certificates are subject to the same authentication steps outlined in this CPS as apply to initial issuance of a Certificate except that Subscriber will not be required to submit registration documents to Trend Micro SSL if Subscriber's (a) Organization name has not changed, (b) fully qualified Domain Name has not changed, and (c) Subscriber has not indicated in the enrollment form that such information has changed during the time since it was originally submitted. Expiring Certificates are not revoked by Trend Micro SSL upon issuance of the renewal Certificate. Renewal of EV Server Certificates may be by different procedures as specified in the EV Guidelines.

The Subscriber must pay the fees and comply with the other terms and conditions for renewal as presented on Trend Micro SSL's Web site.

3.9 Certificate Expiration

Trend Micro SSL will attempt to notify all Subscribers of the expiration date of their Certificate. Notifications will generally be by e-mail message to the administrative, technical, and/or billing contacts listed in the enrollment form submitted by Subscriber, and will likely occur periodically during the 90 day period prior to the expiration date and the 14 day period following the expiration date. If Subscriber's enrollment form was submitted by another party on Subscriber's behalf, Trend Micro SSL likely will not send expiration notices to that party due to contractual limitations.

3.10 Certificate Revocation and Suspension

3.10.1 Circumstances for Revocation

Certificate revocation is the process by which Trend Micro SSL prematurely ends the Operational Period of a Certificate by posting the serial number of the Certificate to a Certificate Revocation List and OCSP. Trend Micro SSL will maintain a continuous 24x7

ability to accept and respond to revocation requests and related inquiries.

A Subscriber shall cease using a Certificate and its associated Private Key and shall inform Trend Micro SSL and promptly request revocation of a Certificate in the event that:

- Any information in the Certificate is or becomes incorrect or inaccurate;
- There is any actual or suspected misuse or Compromise of the Subscriber's Private Key associated with the Public Key listed in the Certificate; or
- upon a change in the ownership of a Subscriber's web server.

The Subscriber shall state the reason(s) for requesting revocation upon submitting the request.

Trend Micro SSL shall revoke a Certificate if:

- The Subscriber requests in writing that Trend Micro revoke the Certificate;
- The Subscriber notifies Trend Micro that the original certificate request was not authorized and does not retroactively grant authorization;
- Trend Micro obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a key Compromise or no longer complies with the requirements of the CA/Browser Forum Baseline Requirements;
- Trend Micro obtains evidence that the Certificate was misused;
- Trend Micro is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Service Agreement;
- Trend Micro is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a domain name registrant's right to use the domain name, a relevant licensing or services agreement between the domain name registrant and the Subscriber has terminated, or the domain name registrant has failed to renew the domain name);
- Trend Micro is made aware that a wildcard certificate has been used to authenticate a fraudulently misleading subordinate fully-qualified domain name;
- Trend Micro is made aware of a material change in the information contained in the Certificate;
- Trend Micro is made aware that the Certificate was not issued in accordance with the CA/Browser Forum Baseline Requirements and Extended Validation

Guidelines (as applicable) or Trend Micro's Certification Practice Statement;

- Trend Micro determines that any of the information appearing in the Certificate is inaccurate or misleading;

- Trend Micro ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;

- Trend Micro's right to issue Certificates under the CA/Browser Forum Baseline Requirements and Extended Validation Guidelines (as applicable) expires or is revoked or terminated, unless Trend Micro has made arrangements to continue maintaining the CRL/OCSP Repository;

- Trend Micro is made aware of a possible compromise of the private key of the subordinate CA used for issuing the Certificate;

- Revocation is required by Trend Micro's Certificate Policy and/or Certification Practice Statement;

- The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time).

- Trend Micro SSL receives notice or otherwise becomes aware that a Subscriber has been added as a denied party or prohibited person on any denied list or other legal black list as specified in Section 11.11.2 of the CA/Browser Forum Extended Validation Guidelines, or is operating from a prohibited destination under the laws of Trend Micro SSL's jurisdiction of operation.

- In case Trend Micro SSL is informed, or finds out by other means that a Subscriber has fallen under any of the categories of an organized crime group, an organized crime group member, a person for whom five years have not elapsed since the day on which the person ceased to be an organized crime group member, an organized crime group associate member, an organized crime group affiliated company, a racketeer group and the like, a group engaging in criminal activities under the pretext of conducting social campaigns and others, a crime group specialized in intellectual crimes and the like, or their equivalents (the "Organized Crime Group, etc."), or that a Subscriber has fallen under any of the following categories:

    (a) To have a relationship in which it is deemed that the Organized Crime Group, etc. holds control over, or is substantially involved in the Subscriber's management;

(b) To have a relationship in which it is deemed that the Subscriber uses the Organized Crime Group, etc. unjustifiably, such as for the purpose of ensuring unjustified benefits to himself/herself or a third-party, or for the purpose of inflicting harm to a third-party;

(c) To have a relationship in which it is deemed that the Subscriber is engaged in providing funds and the like, or benefits to the Organized Crime Group, etc.; or

(d) To have a relationship in which an executive officer or a person substantially involved in the Subscriber's management has a socially condemnable relationship with the Organized Crime Group, etc.

In the event that Trend Micro SSL deems that a Subscriber has committed or is likely to commit any act that falls into any of the categories below by himself/herself or by using a third-party:

(a) Use of fraudulent means, violent acts, or threatening statements;
(b) Illegal acts, or undue claims;
(c) Act of obstructing Trend Micro SSL's business;
(d) Act of damaging Trend Micro SSL's reputation, credit and the like; or
(e) Other acts equivalent to those listed above.

If Trend Micro SSL initiates revocation of a Certificate, Trend Micro SSL will notify the administrative and technical contact provided by Subscriber by e-mail message of the revocation and the reasons why. In the event that Trend Micro SSL ceases operations, all Certificates issued by Trend Micro SSL shall be revoked prior to the date that Trend Micro SSL ceases operations, and Trend Micro SSL will notify the administrative and technical contact provided by Subscriber by e-mail message of the revocation and the reasons why.

A refund and/or reissue request by a Subscriber pursuant to Section 2.2.5 will not be treated as a request for revocation of a Certificate under this subsection unless the Subscriber specifically requests revocation of the Certificate.

3.10.2 Who Can Request Revocation

The only persons permitted to request revocation of a Certificate issued by Trend Micro SSL are the Subscriber (including designated representatives) and the administrative or technical contact for the Subscriber.

3.10.3 Procedure for Revocation Request

To request revocation, a Subscriber must contact Trend Micro SSL, either by e-mail message, postal service, facsimile, or overnight courier, and specifically request "revocation" (using that term) of a particular Certificate identified by the Subscriber. Revocation requests may be sent to ssl_support@trendmicro.com. Upon receipt of a revocation request, Trend Micro SSL will seek confirmation of the request by e-mail

message to the person requesting revocation (as defined in Section 3.10.2 above). The message will state that, upon confirmation of the revocation request, Trend Micro SSL will revoke the Certificate and that posting the revocation to the appropriate CRL and OCSP will constitute notice to the Subscriber that the Certificate has been revoked. Trend Micro SSL will require a confirming e-mail message back from either the administrative or technical contact authorizing revocation (or by other means of confirmation acceptable to Trend Micro SSL). Upon receipt of the confirming e-mail message, Trend Micro SSL will revoke the Certificate and the revocation will be posted to the appropriate CRL and OSCP. Notification may be sent to the subject of the Certificate and the subject's designated contacts. There is no grace period available to the Subscriber prior to revocation, and Trend Micro SSL shall respond to the revocation request within the next business day and post the revocation to the next published CRL and OCSP.

In the event of Compromise of Trend Micro SSL's Private Key used to sign a Certificate; Trend Micro SSL will send an e-mail message as soon as practicable to all Subscribers with Certificates issued off the Private Key stating that the Certificates will be revoked by the next business day and that posting the revocation to the appropriate CRL will constitute notice to the Subscriber that the Certificate has been revoked.

3.10.4 Certificate Suspension

Trend Micro SSL does not support Certificate suspension for the Certificates.

3.11 Problem Reporting and Response

Subscribers, Relying Parties, Application Software Suppliers, and other third parties may report complaints or suspected Private Key Compromise, Certificate misuse, or other types of fraud, Compromise, misuse, or inappropriate conduct related to Certificates ("Certificate Problem Reports") at any time.

Trend Micro SSL will post instructions for how to send Certificate Problem Reports on its website, and will maintain 24x7 capability to accept and acknowledge such Reports. In addition, Trend Micro SSL will begin investigation of all Certificate Problem Reports within twenty-four hours and decide whether revocation or other appropriate action is warranted based on at least the following criteria:

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

Trend Micro SSL will also maintain a continuous 24x7 ability to internally respond to any high-priority Certificate Problem Report, and where appropriate, forward such complaints to law enforcement and/or revoke a Certificate that is the subject of such a complaint.

3.12 Key Management

Trend Micro SSL does not provide Subscriber Private Key protection or other Subscriber key management services in connection with its Certificates.

3.13 Subscriber Key Pair Generation

Trend Micro SSL does not provide Subscriber Key Pair generation or Subscriber Private Key protection for the Certificates.

3.14 Records Archival

Trend Micro SSL shall maintain and archive records relating to the issuance of the Certificates for seven (7) years after the date the applicable Certificate ceases to be valid.

3.15 CA Termination

In the event that it is necessary for Trend Micro SSL or its CAs to cease operation, Trend Micro SSL will make a commercially reasonable effort to notify Subscribers, Relying Parties, and other affected entities of such termination in advance of the CA termination. Where CA termination is required, Trend Micro SSL will develop a termination plan to minimize disruption to Subscribers and Relying Parties. Such termination plans may address the following, as applicable:

- Provision of notice to parties affected by the termination, such as Subscribers and Relying Parties, informing them of the status of the CA,
- Handling the cost of such notice,
- The revocation of the Certificate issued to the CA by Trend Micro SSL,
- The preservation of the CA's archives and records for the time periods required in this CPS,
- The continuation of Subscriber and customer support services,
- The continuation of revocation services, such as the issuance of CRLs,
- The revocation of unexpired unrevoked Certificates of Subscribers and subordinate CAs, if necessary,
- The payment of compensation (if necessary) to Subscribers whose unexpired unrevoked Certificates are revoked under the termination plan or provision, or alternatively, the issuance of replacement Certificates by a successor CA,

- Disposition of the CA's Private Key and the hardware tokens containing such Private Key,

- Provisions needed for the transition of the CA's services to a successor CA, and

- The identity of the custodian of Trend Micro SSL's CA and RA archival records. Unless a different custodian is indicated through notice to Subscribers and Relying Parties, the Registered Agent for Trend Micro, Inc., a California corporation, shall be the custodian.

4. PHYSICAL SECURITY CONTROLS

The Trend Micro SSL operates a tightly controlled and restricted PKI infrastructure at its secure facility in the greater metropolitan area of a major US city which has been evaluated and approved by formal action of the PKI Policy Authority. The infrastructure is comprised of physical boundaries, computer hardware, software and procedures that provide an acceptable resilience against security risks and provide a reasonable level of availability, reliability and correct operation and the enforcing of a security policy.

The hardware is located in a dedicated, resistant server enclosure. Access to the facility by individuals (personnel and others) is strictly controlled and restricted to authorized and trusted personnel only. Maintenance and other services applied to the cryptographic devices and server systems are limited to authorized Trend Micro SSL representatives. Physical access to the server infrastructure and facilities is logged and signed by at least one other authorized witness on the four-eyes principal. Otherwise physical access to the systems shall be avoided.

Maintenance operations, changes, modifications or removal of devices or hardware components of the CA server systems are strictly restricted and must be authorized by a member of the Trend Micro SSL PKI Policy Authority. Any removed device which may contain data (like hard drives) must be wiped out of any data before disposal.

The facility is fully air conditioned and maintains electrical power as well as electrical power backup (UPS), and is supported by an external, independent electricity power source for cases of prolonged power outages.

The facility has taken reasonable precautions to minimize the impact of water exposure. Fire alarm and prevention equipment are installed and available at the premise.

The facility public areas are monitored by a closed-circuit camera and television monitoring system with recording capabilities and records are archived in a rolling and increasing mode. Data is backed up upon the occurrence of all certificate life cycle events.

All waste (paper, media, or any other waste) is disposed of in a secure manner in order to prevent the unauthorized use of, or access to, or disclosure of, waste containing confidential information.

5. TECHNICAL SECURITY CONTROLS

5.1 CA Key Pair, Sub-CAs

CA Key Pair generation is performed by multiple trained and trusted individuals using secure systems and processes that provide for the security and required cryptographic strength for the keys that are generated and using the RSA or ECC algorithm. All CA Key Pairs are generated in pre-planned key generation ceremonies witnessed by independent auditors in accordance with the requirements of the EV Guidelines. The activities performed in each key generation ceremony are recorded, dated and signed by all individuals involved. These records are kept for audit and tracking purposes for a length of time deemed appropriate by Trend Micro SSL's PKI Policy Authority, but not less than the Key Pair validity period plus the archive period.

The cryptographic modules used for key generation and storage meet the requirements of FIPS 140-2 level 3. The CA Root Keys for each CA Certificate were generated and are stored in hardware. The Root Keys for each CA Certificate are maintained under multi-person control. The CA private key is backed up (but not escrowed), stored, and recovered by authorized personnel using dual control in a physically secured environment. Backup copies of the CA private keys are subject to the same or greater level of security controls as keys currently in use. If required, recovery of the CA private key is conducted in the same secure schema used in the backup process, using dual control.

The Root Keys for each CA Certificate may be used for Certificate signing, CRL and OCSP signing, and off-line CRL signing.

Trend Micro SSL makes the CA Certificates available to Subscribers and Relying Parties through their inclusion in web browser software. For specific applications, Trend Micro SSL's Public Keys are provided by the application vendors through the applications root stores.

Trend Micro SSL has not authorized any external sub-CAs to be operated by third parties at the present time. In the event Trend Micro SSL decides to authorize any external sub-CAs to be operated by third parties in the future, Trend Micro SSL intends to amend this CPS to impose legal, technical, attestation and audit, and other requirements on the sub-CAs substantially equivalent to those followed by Trend Micro SSL for similar certificates. In the event an external sub-CA is authorized by Trend Micro SSL to issue EV Certificates, Trend Micro SSL intends to state in its CPS Trend Micro SSL's practices following all relevant rules as stated in the EV Guidelines concerning external sub-CAs operated by third parties (as such rules may be amended from time to time in the Guidelines).

End-entity certificates are not issued off Trend Micro SSL's root certificates, but are issued off the intermediate Sub-CA root certificates listed on Appendix A.

Trend Micro SSL generally provides the full certificate chain (including the issuing CA Certificate and any other Certificates in the chain) to the Subscriber upon Certificate

issuance. Trend Micro SSL CA Certificates may also be downloaded from the Resourcestab at ssl.trendmicro.com/en/resources.
.
There are no restrictions on the purposes for which the CA Key Pair may be used. The usage period or active lifetime for the Trend Micro SSL Public and Private Keys is as listed on Appendix A. The CA Certificate for each is generally available in the Root Key Store of the applicable browser or application software.

In the event of the Compromise of one or more of the Trend Micro SSL Root Key(s) (including the CA Certificates), Trend Micro SSL shall promptly notify all Subscribers via e-mail and notify Relying Parties and others via the CRL and OCSP and additional notice posted at ssl.trendmicro.com/en/resources, and shall revoke all Certificates issued with such Trend Micro SSL Root Key(s).

When Trend Micro SSL CA Key Pairs reach the end of their validity period, such CA Key Pairs will be archived for a period of at least 5 years. Archived CA Key Pairs will be securely stored using offline media. Procedural controls will prevent archived CA Key Pairs from being returned to production use. Upon the end of the archive period, all copies of the archived CA Private Keys will be securely destroyed.

Trend Micro SSL CA Key Pairs are retired from service at the end of their respective maximum lifetimes as defined above, and so there is no key changeover. Certificates may be renewed as long as the cumulative certified lifetime of the Certificate Key Pair does not exceed the maximum CA Key Pair lifetime. Trend Micro SSL Key Pairs will be generated as necessary, for example to replace CA Key Pairs that are being retired, to supplement existing, active Key Pairs and to support new services in accordance with this CPS. Trend Micro SSL will cease to use the CA Key Pair at the end of the cryptoperiod or when the Compromise of the CA Private Key is known or suspected.

5.2 Subscriber Key Pairs

Trend Micro SSL recommends that Subscribers select the highest encryption strength option when generating their certificate requests. All Trend Micro SSL certificates will accommodate the use of domestic and international 256-, 128-, 56-, and 40-bit strength browsers and web servers.

Generation of Subscriber Key Pairs is generally performed by the Subscriber, and may be generated in either hardware or software. For server Certificates, the Subscriber typically uses the key generation utility provided with the web server software. Trend Micro SSL does not require any particular standard for the module used to generate the Keys. Key pairs generated by the Subscriber for Certificates may be used for server authentication. There are no purposes for which Trend Micro SSL restricts the use of the Subscriber key or Certificate.

For X.509 Version 3 Certificates, Trend Micro SSL generally populates the KeyUsage extension of Certificates in accordance with RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008.

5.3 Business Continuity Management Controls

Trend Micro SSL has a business continuity plan (BCP) to maintain or restore the Trend Micro SSL CA's business operations in a reasonably timely manner following interruption to or failure of critical business processes. The BCP defines the following time periods for acceptable system outage and recovery time:

(a) Restore ability to receive and respond to Subscriber and Public communications – 3 business days

(b) Post an existing CRL – 3 business days

(c) Restore existing root keys – 7 days

(d) Publish a new CRL - 7 days

(e) Vet a Subscriber -2 weeks

(f) Issue a Certificate - 2 weeks

(g) Audit Security Policy – 1 month

(h) Audit Vetting Procedures - 2 months

(i) Create new root keys – 2 months

Backup copies of essential business and CA information are made routinely. Backup root keys are maintained several miles from the Trend Micro SSL facility's main site.

5.4 Event Logging, Documentation, and Audit Trail Requirements

Trend Micro SSL's event journal data is archived at least monthly (or more frequently depending on data changes). Event journals are reviewed at regular intervals by the PKI Policy Authority or its designee. Event logs will be retained for at least seven years and will be available to independent auditors upon request.

Trend Micro SSL will record in detail every action taken to process an EV Certificate Request and to issue an EV Certificate, including all information generated or received in connection with an EV Certificate Request, and every action taken to process the Request, including time, date, and personnel involved in the action. These records will be available as auditable proof of the CA's practices.

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

- 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.
- Log entries MUST include the following elements:
    - Date and time of entry;
    - Identity of the person making the journal entry; and
    - Description of entry.

Trend Micro SSL will retain all documentation relating to all Certificate Requests and verification thereof, and all Certificates and revocation thereof, for at least seven years after any Certificate based on that documentation ceases to be valid. In connection therewith, Trend Micro SSL will maintain an internal database of all previously revoked Certificates and previously rejected Certificate Requests due to suspected phishing or other fraudulent usage or concerns. Such information will be used to flag suspicious Certificate Requests.

6. CERTIFICATE, CRL, AND OCSP PROFILE

6.1 Certificate Profile

Trend Micro SSL Certificates conform to (a) ITU-T Recommendation X.509 Version 3 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997, and (b) RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008 ("RFC 5280"). Certificate extensions and their criticality, as well as cryptographic algorithm object identifiers, are populated according to the IETF RFC 5280 standards and recommendations.

The name forms for Subscribers are enforced through Trend Micro SSL's internal policies and the authentication steps described elsewhere in this CPS. Name constraint enforcement is not through the name constraint extension, but through the authentication steps followed and contractual limitations with each Subscriber. Domain names do not have to be meaningful or unique, but must match a second level domain name as posted by InterNIC. Subscribers are not permitted to use pseudonyms (names other than a Subscriber's true personal or organizational name).Any name claim disputes between a Subscriber and any other party (including disputes involving trademarks) must be resolved separately by the parties, and Trend Micro SSL will abide by any final and binding judicial or arbitration result between the parties. The policy constraints extensions and policy qualifiers syntax and semantics, when used, conform to the RFC 5280 standards.

Trend Micro SSL will generally use the Certificate profiles described in this CPS. See also Appendix A for additional details for specific Trend Micro SSL products.

6.2 CRL Profile

Trend Micro SSL-issued CRLs conform to all RFC 5280 standards and recommendations.

6.3 OCSP Profile

Trend Micro SSL-issued OCSPs conform to all RFC 2560 standards and recommendations.

7. CPS ADMINISTRATION

7.1 CPS Authority

The authority administering this CPS is the Trend Micro SSL PKI Policy Authority. The Authority shall be responsible for establishing and maintaining all Trend Micro SSL security, information, and other critical policies as well as change control procedures. The Authority shall also establish and maintain appropriate personnel security policies as well as physical, operational, system access, and environmental security policies and compliance with legal requirements in order to enhance and support the trustworthiness of Trend Micro SSL's operations and Certificates and help protect them from Compromise or interruption. Inquiries to Trend Micro SSL's PKI Policy Authority should be addressed as follows:

Trend Micro SSL PKI Policy Authority
Trend Micro, Inc.
10101 N. De Anza Boulevard
Cupertino, CA 95014 USA

Trend Micro SSL does not support a Certificate Policy (CP) for its certificates.

7.2 Contact Person

Address inquiries about the CPS to ssl_support@trendmicro.comor to the following address:

Trend Micro SSL PKI Policy Authority
Trend Micro, Inc.
10101 N. De Anza Boulevard
Cupertino, CA 95014 USA

7.3 CPS Change Procedures

This CPS (and all amendments to this CPS) is subject to approval by the PKI Policy Authority. Trend Micro SSL may change this CPS at any time without prior notice. The CPS and any amendments thereto are available on Trend Micro's website athttp://ssl.trendmicro.com/resources/. Amendments to this CPS will be evidenced by a new version number and date posted online(except where the amendments are purely clerical), and shall apply as of the stated effective date.

8. DEFINITIONS

Applicant. All parties who apply for digital certificate services with Trend Micro SSL 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 Trend Micro SSL 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.

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 the Trend Micro SSL 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. Trend Micro SSL's 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 Trend Micro SSL 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 Trend Micro SSL. 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 Trend Micro SSL 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.

Trend Micro. Trend Micro Incorporated, Shinjuku MAYNDS Tower, 1-1 Yoyogi 2-Chome, Shibuya-ku, Tokyo 151-0053, Japan and its subsidiary Trend Micro, Inc., a California, USA corporation, and its wholly-owned subsidiary AffirmTrust, LLC.

Trend Micro SSL. Trend Micro Incorporated, Shinjuku MAYNDS Tower, 1-1 Yoyogi 2-Chome, Shibuya-ku, Tokyo 151-0053, Japan and its subsidiary Trend Micro, Inc., a California, USA corporation, and its wholly-owned subsidiary AffirmTrust, LLC.

APPENDIX A TO TREND MICRO SSL CPS

1. 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 caebff c3 bb

Trend Micro SSLwill 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

Trend Micro SSL's intermediate sub-CAs may be cross-signed by one of the SwissSign root certificates listed below, as indicated more specifically in the Product Offerings information described in Section 4 below.

Cross-Signing CA Root Name	Algorithm	CA Root Size	Signature Hash	CA Root Expires	SHA Hash Thumbprint
SwissSign Gold CA – G2	RSA	4096	SHA 1	10/25/2036	5b 25 7b 96 a4 65 51 7e b8 39 f3 c0 78 66 5e e8 3a e7 f0 ee
SwissSign Silver CA – G2	RSA	4096	SHA 1	10/25/2036	17 a0 cd c1 e4 41 b6 3a 5b 3b cb 45 9d bd 1c c2 98 fa 86 58

3. Extended Validation (EV) OIDs:

Trend Micro SSL 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 is1.3.6.1.4.1.34697.2.2
AffirmTrust Premium Root: EV OID is1.3.6.1.4.1.34697.2.3
AffirmTrust Premium ECC Root: EV OID is 1.3.6.1.4.1.34697.2.4

4. Current Trend Micro SSL Product Offerings:

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

A. Server Certificate Current Offerings

(1) Product Name: "Trend Micro SSL"

Root certificate:	AffirmTrust Networking
Cross-signed by:	SwissSign Gold CA-G2 - *Root*
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

(2) Product Name: "Trend Micro SSL"

Root certificate:	SwissSign Gold CA-G2 - *Root*
Issuing sub-CA root:	Trend Micro Gold 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

B. Test Certificates

Test certificates for any of the certificate types listed at Sections 3.1 through 3.3 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.