SecureTrust
Certification Practice Statement

CPS

for S/MIME Certificates

Version 1.6.0

Effective Date: November 1, 2007

Policy OID: 2.16.840.1.114404.2.2.1

I. INTRODUCTION

A. Overview

This document is the SecureTrust Certification Practice Statement ("CPS") for SecureTrust S/MIME Certificates and is identified by the OID number 2.16.840.1.114404.2.2.1. Its purpose is to present the technical principles and practices that SecureTrust employs in managing the issuance and life cycle of SecureTrust S/MIME Certificates signed by SecureTrust Root Certificates as well as the terms and conditions under which the aforementioned SecureTrust Certificates are made available to Subscribers and Relying Parties in the SecureTrust Public Key Infrastructure ("PKI").

This CPS and any revisions to this CPS are incorporated by reference into S/MIME Certificates issued by SecureTrust. This CPS is published and any revisions will be published in the SecureTrust legal repository at https://www.SecureTrustsecurity.com/legal/.

B. SecureTrust

SecureTrust is a Certification Authority (CA) that issues highly-trusted, high-quality digital certificates to private and public companies and individuals in accordance with this CPS. Subscribers include all parties who contract with the CA for digital certificate services. All parties who may rely upon the certificates issued by the CA are considered relying parties.

C. Definitions

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

D. Third Party Services

SecureTrust may outsource in part or whole certain aspects of the delivery of its services. Regardless of the partner or agent selected to manage certain parts of the certificate life cycle or operations, SecureTrust remains ultimately in charge of the whole process. SecureTrust limits its responsibility thereof according to the conditions in this CPS.

Some third party businesses (User Agents) may perform some of the functions relating to the issuance of Certificates on behalf of Subscribers (e.g., the gathering of Subscriber information, generating and forwarding of a Certificate Signing Request, or installation and use of a Certificate following issuance). In such event, the processes and procedures stated in this CPS will be applied to the User Agents as if they were the Subscribers as closely as practicable.

E. SecureTrust S/MIME Certificates

SecureTrust may update or extend its list of products, including the types of certificates it issues, as it sees fit. The publication or updating of the list of SecureTrust products creates no claims by any third party. Upon the inclusion of a new certificate product in the SecureTrust hierarchy, an

amended version of this CPS will be made public within two days on the official SecureTrust repository.

SecureTrust's S/MIME Certificates provide limited authentication of a Subscriber's email address for the purposes of authenticating the sender of an email and providing a method of sharing keys necessary for encryption of emails. SecureTrust's S/MIME Certificates are made available for Subscribers worldwide, except for localities restricted by the U.S. government, in accordance with this CPS.

SecureTrust's S/MIME Certificates are issued with a typical Validity Period of one to three years. Unless a Certificate is revoked prior to the expiration of the Certificate's Validity Period, a SecureTrust certificate has an Validity Period as stated in the Certificate itself.

II. GENERAL PROVISIONS

A. Obligations of Parties

1. SecureTrust

SecureTrust will issue Certificates in accordance with this CPS. SecureTrust will perform limited authentication of Subscribers as described in this CPS. SecureTrust will revoke Certificates as described in this CPS. SecureTrust will perform any other functions which are described within this CPS.

2. Subscriber

Subscriber shall submit truthful information about itself and its business entity, domain ownership and contacts, as applicable. Subscribers shall at all times abide by this CPS. The Subscriber is solely responsible for the protection of its Private Key and shall immediately request revocation of a Certificate if the related Private Key is compromised. The Subscriber shall only use the SecureTrust S/MIME Certificate for purposes of authenticating or encrypting email communications.

3. Relying Party

Relying Parties shall verify that the Certificate is valid by examining the Certificate Revocation List (CRL) before using such a Certificate. SecureTrust does not accept responsibility for reliance on a fraudulently obtained Certificate or a Certificate that is on the CRL. Relying Parties acknowledge the applicability of limitation of liability and warranties pertaining to the reliance on Certificates issued by SecureTrust. Relying Parties shall also read and agree to SecureTrust's relying party agreement. SecureTrust's relying party agreement is available at www.SecureTrust.com/legal.

B. Fees

SecureTrust may charge Subscriber fees for the use of SecureTrust products and services. SecureTrust retains the right to change fees without prior notice. For updated fee information you may refer to SecureTrust's public web site.

1. Issuance, Management, and Renewal Fees

SecureTrust is entitled to charge Subscribers for the issuance, management, and renewal of Certificates. The fees charged will be as stated on SecureTrust'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. Certificate Access Fees

SecureTrust does not charge a fee as a condition of making a Certificate available in a repository or otherwise making Certificates available to Relying Parties.

3. Revocation or Status Information Fees

SecureTrust does not charge a fee as a condition of making the CRL available in a repository or otherwise available to Relying Parties. SecureTrust may, however, charge a fee for providing customized CRL's, OCSP services, or other value-added revocation and status information services. SecureTrust 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 SecureTrust's prior express written consent.

4. Fees for Other Services Such as Policy Information

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

5. Refund and Reissue Policy

SecureTrust will refund the fees charged for a Certificate if the request for refund is made within 30 days of the date the Subscriber paid all applicable fees in full. If a Subscriber has paid the fees for the Certificate to another party such as a reseller, the Subscriber should request the refund from that party. 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 SecureTrust or request reissue of a Certificate based upon a prior Certificate Signing Request previously provided to SecureTrust by the Subscriber.

SecureTrust may revoke a Certificate previously issued following a refund or reissue request. A request for a refund or reissue of a Certificate can be treated as a request by the Subscriber for revocation of a Certificate previously issued by SecureTrust.

C. Compliance Audit

An annual audit is performed by an independent external auditor to assess SecureTrust's compliance with the AICPA/CICA WebTrust program for Certification Authorities. Topics covered by the annual audit include but are not limited to the following:

- CA business practices disclosure,
- Service integrity, and

- CA environmental controls

Material exceptions or deficiencies identified during an audit will result in a determination of actions to be taken. This determination is made by SecureTrust management with input from the independent auditor. SecureTrust management is responsible for developing and implementing a corrective action plan.

D. Limited Warranty/Disclaimer

SecureTrust provides the following limited warranty at the time of Certificate issuance: (i) it issued the Certificate substantially in compliance with this CPS; (ii) the information contained within the Certificate accurately reflects the information provided to SecureTrust 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 SecureTrust takes to verify the information contained in a Certificate is set forth in Section III of this CPS.

EXCEPT FOR THE LIMITED WARRANTY DESCRIBED ABOVE, SECURETRUST 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 SECURETRUST 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, SECURETRUST 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 SECURETRUST, 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 SECURETRUST OR RELIED UPON BY A RELYING PARTY. SECURETRUST DOES NOT WARRANT OR GUARANTEE UNDER ANY CIRCUMSTANCES THE "NON-REPUDIATION" BY A SUBSCRIBER AND/OR RELYING PARTY OF ANY TRANSACTION OR CONTRACT 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 APPLICANTS, SUBSCRIBERS AND RELYING PARTIES AGREE AND ACKNOWLEDGE THAT CERTIFICATES HAVE A LIMITED VALIDITY 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. SECURETRUST HEREBY DISCLAIMS ANY AND ALL LIABILITY TO SUBSCRIBERS AND RELYING PARTIES WHO DO NOT FOLLOW SUCH PROCEDURES OR THIS CPS. MORE INFORMATION ABOUT THE SITUATIONS IN WHICH A CERTIFICATE MAY BE REVOKED CAN BE FOUND IN SECTION III(H) OF THIS CPS.

SecureTrust provides no warranties with respect to another party's software, hardware, 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 SecureTrust 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 which is properly licensed or to otherwise obtain the right to use such technology

E. Limitation Of Liability

EXCEPT TO THE EXTENT CAUSED BY SECURETRUST'S WILLFUL MISCONDUCT, IN NO EVENT SHALL THE CUMULATIVE OR AGGREGATE LIABILITY OF SECURETRUST TO APPLICANTS, SUBSCRIBER AND/OR ANY RELYING PARTY FOR ALL CLAIMS RELATED TO THE INSTALLATION OF, USE OF OR RELIANCE UPON A CERTIFICATE OR FOR THE SERVICES PROVIDED HEREUNDER INCLUDING WITHOUT LIMITATION ANY CAUSE OF ACTION OR CLAIM IN CONTRACT, TORT (INCLUDING NEGLIGENCE AND TORTIOUS INTERFERENCE WITH CONTRACT), STRICT LIABILITY, FOR BREACH OF A STATUTORY DUTY OR FIDUCIARY DUTY OR IN ANY OTHER WAY EXCEED FIVE THOUSAND U.S. DOLLARS ($5,000.00).

SECURETRUST SHALL NOT BE LIABLE IN CONTRACT, TORT (INCLUDING NEGLIGENCE) AND TORTIOUS INTERFERENCE WITH CONTRACT), STRICT LIABILITY, FOR BREACH OF A STATUTORY OR FIDUCIARY DUTY OR IN ANY OTHER WAY (EVEN IF FORSEEABLE AND/OR SECURETRUST 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) NON-ECONOMIC LOSS OR ANY LOSS OF GOODWILL OR REPUTATION; OR (IV) ANY OTHER INDIRECT, CONSEQUENTIAL, INCIDENTAL, MULTIPLE, SPECIAL, PUNITIVE, EXEMPLARY DAMAGES.

THIS SECTION E "LIMITATION OF LIABILITY" SHALL APPLY WHETHER OR NOT SUCH LOSSES OR DAMAGES WERE WITHIN THE CONTEMPLATION OF THE PARTIES AT THE TIME OF THE APPLICATION FOR, INSTALLATION, USE, 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.

IN THE EVENT THAT SOME JURISDICTIONS DO NOT PERMIT 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 FULLEST 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 SecureTrust 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: (i) has expired or been revoked; (ii) has been used for any purpose other than as set forth in the CPS; (iii) has been tampered with; (iv) has been Compromised or if 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 SecureTrust (including without limitation the Applicant, Subscriber or Relying Party); or (v) is the subject of misrepresentations or other misleading acts or omissions of any other party, including but not limited to Applicants, Subscribers and Relying Parties. In no event shall SecureTrust 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.

F. Force Majeure

SecureTrust 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 SecureTrust.

G. Financial Responsibility

1. Fiduciary Relationships

SecureTrust is not an agent, fiduciary, trustee, or other representative of the Applicant, Subscriber , or Relying Party and the relationship between SecureTrust and the Applicant and the Subscriber is not that of an agent or a principal. SecureTrust makes no representation to the contrary, either explicitly, implicitly, by appearance or otherwise. An Applicant, Subscriber, or a Relying Party shall not have any authority to bind SecureTrust by contract or otherwise, to any obligation.

2. Indemnification by Applicant and Subscriber

Applicant, Subscriber and Relying Parties hereby agree to indemnify and hold SecureTrust and its affiliates (including, but not limited to, its parent company, officers, directors, employees, agents, partner, successors and assigns) harmless from any claims, actions, or demands that are caused by the use, publication or reliance on 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, regardless of whether 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; (d) any failure on the part of the Subscriber to promptly notify SecureTrust, 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; (e) the Subscriber's failure to the comply with the Subscriber Agreement; or (f) the Relying Party's failure to comply with this CPS and the Relying Party Agreement, including without limitation the Relying Party's failure to verify a Certificate in accordance with this CPS and the Relying Party Agreement.

H. Interpretation & Enforcement

1. Governing Law

The enforceability, construction, interpretation, and validity of this CPS and any Certificates issued by SecureTrust shall be governed by the substantive laws of the State of Delaware, United States of America, excluding (i) the conflicts of law provisions thereof and (ii) the United Nations Convention on Contracts for the International Sale of Goods. Applicants, Subscribers, and Relying Parties irrevocably consent to jurisdiction in the State of Illinois and any and all actions against SecureTrust or its affiliated companies must be brought in the State of Illinois.

2. Dispute Resolution Procedures

Any dispute, controversy or claim arising under, in connection with or relating to this CPS, SecureTrust's Websites, or any Certificate issued by SecureTrust shall be subject to and settled finally by binding arbitration in accordance with the Arbitration Rules of the American Arbitration Association (AAA). All arbitration proceedings shall be held in Chicago, Illinois. There shall be one arbitrator appointed by the AAA who shall exhibit a reasonable familiarity with the issues involved or presented in such dispute, controversy or claim. The award of the arbitrator shall be binding and final upon all parties, and judgment on the award may be entered by any court having proper

jurisdiction thereof. This CPS and the rights and obligations of the parties hereunder and under any Certificate issued by SecureTrust shall remain in full force and effect pending the outcome and award in any arbitration proceeding hereunder. In any arbitration arising hereunder, each party to the preceding shall be responsible for its own costs incurred in connection with the arbitration proceedings, unless the arbitrator determines that the prevailing party is entitled to an award of all or a portion of such costs, including reasonable attorneys fees actually incurred.

3. Conflict of Provisions

This CPS and the applicable Subscriber Agreement and Relying Party Agreement represent the entire agreement between any Subscriber or Relying Party and SecureTrust and supersede any and all prior understandings and representations pertaining to its subject matter. In the event, however, of a conflict between this CPS and any other express agreement a Subscriber has with SecureTrust or its affiliates with respect to a Certificate, including but not limited to a Subscriber Agreement, such other agreement shall take precedence.

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.

I. Repository and CRL

With regard to SecureTrust Certificates, SecureTrust shall operate a CRL that will be available to both Subscribers and Relying Parties. SecureTrust shall post the CRL online at least once every two weeks in a PEM format except as otherwise provided in SecureTrust's Business Continuity Plan. Each CRL is signed by the issuing SecureTrust CA. The procedures for revocation are as stated elsewhere in this CPS.

SecureTrust retains copies of all Certificates for the life of the CA, but does not archive or retain expired or superceded CRLs. SecureTrust does not provide other online status mechanisms (e.g., OCSP) for checking certificate status requests, but may do so at a later date.

J. Confidentiality Policy

1. Individual Subscriber Information

Except as provided herein, certain information regarding Subscribers that is submitted on enrollment forms for Certificates will be kept confidential by SecureTrust (such as contact information for individuals and credit card information) and SecureTrust shall not release such information without the prior consent of the Subscriber. Notwithstanding the foregoing, SecureTrust may disclose 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 SecureTrust'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 SecureTrust and (c) to third parties as may be necessary for SecureTrust 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 SecureTrust.

2. Aggregate Subscriber Information

Notwithstanding the previous Section, SecureTrust may disclose Subscriber information on an aggregate basis, and the Subscriber hereby grants to SecureTrust 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. SecureTrust shall not disclose to any third party any personally identifiable information about any Subscriber that SecureTrust obtains in its performance of services hereunder.

K. 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.

L. Survival

The following sections shall survive, along with all definitions required thereby: Sections I, II, and VIII.

M. Export

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

III. OPERATIONAL REQUIREMENTS

A. Application Requirements

An Applicant for a SecureTrust Certificate shall complete a SecureTrust Certificate application in a form prescribed by SecureTrust. All enrollment forms are subject to review, approval and acceptance by SecureTrust. All Applicants are required to include the information listed below in Section III.B. Other than as provided in Section III.B.2, SecureTrust does not verify the authority of the Subscriber to request a Certificate. SecureTrust 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. Procedure for Processing S/MIME Certificate Applications

1. Enrollment Form

Applicants submit their Public Key to SecureTrust for certification electronically through the use of a PKCS#10 Certificate Signing Request (CSR) or other package digitally signed by the Applicant's

Private Key in a session secured by Secure Sockets Layer (SSL). Applicants must also provide a signed Subscriber Agreement, and any additional documentation as necessary for SecureTrust to perform the validation process for S/MIME certificate procurement.

SecureTrust reserves the right to use subcontractors or other third parties to assist in the performance of its operational requirements or any other obligation under this CPS (See section I.D).

2. Validation Process

S/MIME certificates issued under this CPS are validated as to the email address only. Applicants may populate other fields of the certificate request such as name and company, but this information is not validated in any way by SecureTrust. SecureTrust will confirm that the applicant holds the private key corresponding to the public key to be included in the Certificate. SecureTrust performs a limited confirmation of the Certificate Applicant's e-mail address through the following request/response mechanism:

1. SecureTrust receives an online request for an S/MIME certificate
2. SecureTrust will send an email to the email address provided in the certificate request with a unique link that the applicant must click on in order to retrieve their S/MIME certificate.
3. The Applicant must click on the link which will take them to a webpage.
4. The Applicant then confirms their information and clicks a button asking for the Certificate to be issued.
5. The Certificate is then issued and provided to the Subscriber in the form of a download link.
6. The Subscriber clicks on the download link and then saves the certificate file and installs it according to the instructions for their operating platform.

C. Application Issues

At certain times during the application process in which SecureTrust 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 or request for a Certificate.

D. Certificate Delivery

If SecureTrust finds that the Applicant's enrollment form was sufficiently verified, then the Applicant's Certificate will be signed by SecureTrust. Upon signing the Applicant's Certificate, SecureTrust will deliver such Certificate to the customer in a secure communication via an online account download.

E. Certificate Acceptance

The Subscriber expressly indicates acceptance of a Certificate by using such Certificate or downloading and installing the Certificate.

F. 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. This process is defined as Cerificate Renewal. Subscribers shall generate a new Key Pair to replace the expiring Key Pair (technically defined as "rekey"). For purposes of this CPS, a "rekey" and "renewal" as defined above will be treated as a Renewal Certificate. Renewal Certificates are subject to the same authentication steps outlined in this CPS as apply to initial issuance of a Certificate. Expiring Certificates are not revoked by SecureTrust upon issuance of the renewal Certificate. The Subscriber must pay the fees and comply with the other terms and conditions for renewal as presented on SecureTrust's Web site.

G. Certificate Expiration

SecureTrust 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, SecureTrust may not send expiration notices to that party. SecureTrust is not responsible for making sure that the customer is notifed prior to the expiration of their certificate.

H. Certificate Revocation

1. Circumstances for Revocation

Certificate revocation is the process by which SecureTrust prematurely ends the Validity Period of a Certificate by posting the serial number of the Certificate to a Certificate Revocation List. A Subscriber shall inform SecureTrust and promptly request revocation of a Certificate: whenever any of the information on the Certificate changes or becomes obsolete; or whenever the Private Key, or the media holding the Private Key, associated with the Certificate is Compromised, suspected or threatened of being Compromised. Subscriber shall state the reason(s) for requesting revocation upon submitting the request.

SecureTrust shall revoke a Certificate:

Upon written request of a Subscriber as described above; in the event of Compromise of SecureTrust's Private Key used to sign a Certificate; upon the Subscriber's breach of either this CPS or Subscriber Agreement; if SecureTrust determines that the Certificate was not properly issued; SecureTrust shall revoke the Certificate. If SecureTrust initiates revocation of a Certificate, SecureTrust shall notify the administrative and/or technical contact provided by Subscriber by e-mail message of the revocation and the reasons for such revocation. In the event that SecureTrust ceases operations, all Certificates issued by SecureTrust shall be revoked prior to the date that

SecureTrust ceases operations, and SecureTrust shall notify the administrative and/or technical contact provided by Subscriber by e-mail message of the revocation and the reasons for such revocation. A refund and/or reissue request by a Subscriber may be treated as a request for revocation of a Certificate under this subsection.

2. Who Can Request Revocation

The only persons permitted to request revocation of a Certificate issued by SecureTrust is the Subscriber (including designated representatives), the administrative or technical contact.

3. Procedure for Revocation Request

To request revocation, a Subscriber shall contact SecureTrust, either by e-mail message, a national/regional postal service, facsimile, or overnight courier, and specifically request "revocation" (using that term) of a particular Certificate identified by the Subscriber. Upon receipt of a revocation request, SecureTrust will seek confirmation of the request by e-mail message to the person requesting revocation (as defined in Section III.H.2 above). The message will state that, upon confirmation of the revocation request, SecureTrust shall revoke the Certificate and that posting the revocation to the appropriate CRL shall constitute notice to the Subscriber that the Certificate has been revoked. SecureTrust shall require a confirming e-mail message back from either the administrative or technical contact authorizing revocation (or by other means of confirmation acceptable to SecureTrust). Upon receipt of the confirming e-mail message, SecureTrust shall revoke the Certificate and the revocation shall be posted to the appropriate CRL. Notification shall 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 SecureTrust shall respond to the revocation request within the next business day and post the revocation to the next published CRL. In the event of Compromise of SecureTrust's Private Key used to sign a Certificate, SecureTrust shall send an e-mail message as soon as practicable to all Subscribers with Certificates issued off the Private Key stating that the Certificates shall be revoked by the next business day and that posting the revocation to the appropriate CRL shall constitute notice to the Subscriber that the Certificate has been revoked.

I. Certificate Suspension

SecureTrust does not support Certificate suspension for the Certificates.

J. Key Management

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

K. Subscriber Key Pair Generation

SecureTrust does not provide Subscriber Key Pair generation or Subscriber Private Key protection for the Certificates.

L. Records Archival

SecureTrust shall maintain and archive records relating to the issuance of the Certificates for one (1) year following the expiration of the applicable Certificate.

M. CA Termination

In the event that it is necessary for SecureTrust or its CA's to cease operation, SecureTrust shall 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, SecureTrust shall 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 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 end-user Subscribers and subordinate CAs, if necessary, the payment of compensation (if necessary and allowable) 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 SecureTrust's CA and RA archival records.

IV. PHYSICAL SECURITY CONTROLS

A. Site Location and Construction

All SecureTrust CA operations are conducted within a physically protected environment designed to deter, prevent, and detect covert or overt unauthorized access.

SecureTrust's CA is physically located in a highly secure facility that includes the following:

- Alarms
- Biometric controls to access
- Real ceiling to real floor barriers to access

B. Physical Access Controls

Access to the SecureTrust CA facility requires the three authentication factors of "be, have, know," incorporating biometrics, keys, and personal identification numbers.

C. Power and Air Conditioning

SecureTrust's CA facility is equipped with primary and backup power for the operation of its servers and its network connections. SecureTrust's facility is also equipped with redundant air conditioning systems to control temperature and relative humidity.

D. Water Exposures

The SecureTrust CA facility is located above ground and is not susceptible to flooding or other forms of water damage. SecureTrust has taken reasonable precautions to minimize the impact of water exposure to SecureTrust systems.

E. Fire Prevention and Protection

Fire prevention for SecureTrust's CA facility is done by on-site fire suppression equipment.

F. Media Storage

All media containing production software and data, audit, archive, or backup information is stored in a physically secure manner at both on-site and off-site facilities.

G. Waste Disposal

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed or zeroized in accordance the manufacturers' guidance prior to disposal. Other waste is disposed of in accordance with SecureTrust's normal waste disposal requirements.

H. Off-Site Backup

SecureTrust performs routine backups of critical system data, audit log data, and other sensitive information. Critical CA facility backup media are stored in a physically secure manner at an off-site facility.

V. TECHNICAL SECURITY CONTROLS

A. CA Key Pair

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. All CA Key Pairs are generated in pre-planned key generation ceremonies in accordance with the requirements of SecureTrust security and audit requirements 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 SecureTrust management.

The cryptographic modules used for key generation and storage are certified FIPS 140-1 level 3. The SecureTrust CA private signature keys were generated and are stored in FIPS 140-1 level 3 certified hardware and are backed up but not escrowed.

The SecureTrust Root Key may be used for Certificate signing, CRL signing, and off-line CRL signing.

SecureTrust generally provides the full certificate chain (including the issuing CA Certificate and any CA Certificates in the chain) to the Subscriber upon Certificate issuance. SecureTrust and its chain Certificates may also be downloaded from the SecureTrust repository Web site at http://www.SecureTrust.com/legal.

SecureTrust CA Key Pairs are maintained in a trusted and highly secured environment with backup and key recovery procedures. In the event of the Compromise of one or more of the SecureTrust CA Key(s), SecureTrust shall promptly notify all Subscribers via e-mail and notify Relying Parties and others via the CRL and post additional notice at www.SecureTrust.com/legal/, and shall revoke all Certificates issued with such SecureTrust CA Root Key(s).

When SecureTrust CA Key Pairs reach the end of their validity period, such CA Key Pairs will be archived for a period of at least 3 years. Archived CA Key Pairs will be securely stored using off-line media. Procedural controls will prevent archived CA Key Pairs from being returned to production use. Upon the end of the archive period, archived CA Private Keys will be securely destroyed. SecureTrust 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. New CA 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.

B. Subscriber Key Pairs

SecureTrust recommends that end-user Subscribers select the highest encryption strength option (e.g., 2048-bit) when generating their certificate requests. All SecureTrust certificates will accommodate the use of domestic and international 256-, 128-, 56-, and 40-bit strength browsers and web servers.

Generation of end-user Subscriber Key Pairs is generally performed by the Subscriber, and may be generated in either hardware or software. For SecureTrust S/MIME Certificates, the Subscriber typically uses the key generation utility provided with their email software. SecureTrust does not require any particular standard for the module used to generate the keys. There are no purposes for which SecureTrust restricts the use of the Subscriber key.

For X.509 SSL Version 3 Certificates, SecureTrust will populate the KeyUsage and ExtendedKeyUsage extensions of Certificates in accordance with RFC 3280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April, 2002.

C. Business Continuity Management Controls

SecureTrust has business continuity plans (BCP) to maintain or restore the SecureTrust CAs 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:

1. Vet a Subscriber - 1 week

2. Issue a Certificate - 2 weeks

3. Publish a CRL - 2 weeks

4. Audit Vetting Procedures - 2 months

Backup copies of essential business and CA information are made routinely. In general, back-ups are performed daily on-site, weekly to an off-site location, but may be performed less frequently in SecureTrust's discretion according to production schedule requirements.

D. Event Logging

SecureTrust CA event journal data is archived both daily and monthly. Daily and monthly event journals are reviewed periodically.

VI. CERTIFICATE AND CRL PROFILE

A. Certificate Profile

SecureTrust Certificates conform to (a) ITU-T Recommendation X.509 Version 3: Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997, and (b) RFC 3280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April, 2002 ("RFC 3280"). Certificate extensions and their criticality, as well as cryptographic algorithm object identifiers, are populated according to the IETF RFC 3280 standards and recommendations. The name forms for Subscribers are enforced through SecureTrust'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. SecureTrust applies specific Certificate Policy Object Identifier(s) that refers to the applicable CPS version and URL address. The policy constraints extensions and policy qualifiers syntax and semantics, when used, conform to the RFC 3280 standards.

B. CRL Profile

SecureTrust issued CRLs conform to all RFC 3280 standards and recommendations.

VII. CPS ADMINISTRATION

A. CPS Authority

The authority administering this CPS is the SecureTrust PKI Policy Authority. Inquiries to SecureTrust's PKI Policy Authority should be addressed as follows:

SecureTrust
c/o TrustWave Holdings, Inc.
70 West Madison Street, Suite 1050
Chicago, IL 60602

Telephone: +1 (312) 873-7500
Facsimile: +1 (443) 782-0470

email: legal@SecureTrust.com

B. Contact Person

Address inquiries about the CPS to legal@SecureTrust.com or to the following address:

SecureTrust
c/o TrustWave Holdings, Inc.
70 West Madison Street, Suite 1050
Chicago, IL 60602

Telephone: +1 (312) 873-7500
Facsimile: +1 (443) 782-0470

email: legal@SecureTrust.com

C. CPS Change Procedures

This CPS (and all amendments to this CPS) is subject to approval by the Management of SecureTrust. SecureTrust may change this CPS at any time without prior notice. The CPS and any amendments thereto is available through http://www.SecureTrust.com/legal/ . Amendments to this CPS will be evidenced by a new version number and date, except where the amendments are purely clerical.

VIII. DEFINITIONS

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

Applicant. An entity or indiviual who submits the required information and documentation to SecureTrust in an effort to obtain a Certificate pursuant to and as set forth in this CPS**.**.

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 Validity 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 SecureTrust pursuant to this CPS.

Certificate Revocation List or CRL. A time-stamped list of revoked Certificates that has been digitally signed by the CA.

Certification Authority or CA. An entity which 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 Certificate.

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. OCSP is a network protocol useful in determining the current status of a digital certificate without requiring CRLs.

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

PKCS #10. RSA Laboratories' Public-Key Cryptography Standard (PKCS) #10. PKCS #10 describes the syntax for certification requests. A certification request consists of a distinguished name, a public key, and optionally a set of attributes, collectively signed by the entity requesting certification.

Place of Business. An entity's principal place of business or a satellite or regional office.

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 SecureTrust. 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 SecureTrust to sign the Certificates.

SecureTrust. SecureTrust Corporation merged into XRamp Security which is now a wholly-owned subisidary of TrustWave Holdings, Inc., a Delaware corporation.

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

S/MIME. The industry standard method of authenticating and encrypting email communications.

Subscriber. A person or entity who is the subject named or identified in a Certificate issued to such person or entity, holds a Private Key that corresponds to a Public Key listed in that Certificate, and 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 by the submission of an enrollment form is also referred to as a Subscriber.

Validity Period. A Certificate's period of validity. It typically begins 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 unless the Certificate is revoked before its expiration.