Certificate Practice Statement

CPS

for Extended Validation Certificates

Version 1.1.1

Effective Date: June 18, 2007

Policy OID: 2.16.840.1.114404.1.1.2.4.1

I. INTRODUCTION

A. Overview

This document is the SecureTrust Corporation ("SecureTrust") Certificate Practice Statement ("CPS") for SecureTrust Extended Validation Certificates and is identified by the OID number 2.16.840.1.114404.1.1.2.4.1. It's purpose is to present the technical principles and practices that SecureTrust employs in managing the issuance and life cycle of SecureTrust Extended Validation Certificates as well as the terms and conditions under which the aforementioned SecureTrust EV 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 Extended Validation SSL Certificates issued by SecureTrust and any subsidiaries. This CPS is published and any revisions will be published in the SecureTrust legal repository at http://www.securetrust.com/legal/.

B. SecureTrust

SecureTrust is a Certification Authority (CA) that issues highly-trusted, high-quality EV 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 be authorized by the Subscriber to 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. Types of SecureTrust EV SSL Certificates

SecureTrust may update or extend its list of products, including the types of EV 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 EV hierarchy, an amended version of this CPS will be made public within two days in the official SecureTrust legal repository.

SecureTrust Extended Validation SSL Web Server Certificates provide significant authentication of a Subscriber's web server and permit SSL encrypted transactions between a Relying Party's browser and the Subscriber's web server. SecureTrust's Extended Validation Certificates are X.509 compliant Certificates and are made available for Subscribers in accordance with this CPS and the CA/Browser Forum Guidelines.

SecureTrust's Extended Validation SSL Web Server Certificates are issued with an Operational Period of a maximum of 27 months. No extensions to this Operational Period may be granted. Unless a Certificate is revoked prior to the expiration of the Certificate's Operational Period, a SecureTrust certificate has an Operational Period as stated in the Certificate itself.

II. GENERAL PROVISIONS

A. Obligations of Parties

1. SecureTrust

SecureTrust will issue EV Certificates in accordance with this CPS. SecureTrust will perform detailed validation of information provided by Subscribers as described in this CPS. SecureTrust will revoke Certificates as described in this CPS.

2. Subscriber

Subscriber will submit truthful information about itself and its business entity, domain ownership and contacts, as applicable. Subscribers will not install a SecureTrust Extended Validation SSL Web Server certificate on more than a single server at a time unless permission is otherwise expressly granted by SecureTrust and Subscriber can only install certificate on a server with the respective domain name. The Subscriber is solely responsible for the protection of its Private Key and will immediately request revocation of a Certificate if the related Private Key is compromised. Subscriber must review and verify received certificate before installation and usage. The Subscriber will only use the SecureTrust EV SSL Web Server Certificates for purposes of initiating SSL sessions. Subscriber will at all times abide by the requirements of this CPS.

3. Relying Party

Relying Parties must 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 liability caps and warranties pertaining to the reliance on Certificates issued by SecureTrust. Relying Parties must also read and agree to SecureTrust's relying party agreement. SecureTrust's relying party agreement is available for reference at www.securetrust.com/legal.

B. Fees

SecureTrust may charge Subscriber fees for the use of SecureTrust products and services. SecureTrust retains its right to effect changes to fees without prior notice. For updated fee information you may refer to SecureTrust's public web site at www.securetrust.com

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 CRLs, 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 offers no refunds for the fees charged for an EV SSL Certificate for any reason.

SecureTrust may revoke a Certificate previously issued following reissue request. A request for a reissue of a Certificate can be treated as a request by the Subscriber for revocation of a Certificate previously issued by SecureTrust. Reissues include re-verification of the certificate approver and will run at a fee stated on the SecureTrust website.

C. Compliance Audit

An annual audit is performed by an independent external auditor to assess SecureTrust's compliance with the standards set forth by the Extended Validation Certificate Standard 1.0. Topics covered by the annual audit include but are not limited to the following:

· CA business practices disclosure

· Detailed validation process

· Service integrity

· 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. SecureTrust undergoes yearly AICPA/CICA WebTrust audits and complies with all requirements of the program.

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 and CA/Browser Forum Guidelines for Extended Validation Certificates Version 1.0; (ii) the information contained within the Certificate accurately reflects the information provided to SecureTrust by the Applicant in all material respects; and (iii) SecureTrust 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 ARE LIABLE FOR ANY MISREPRESENTATIONS MADE TO SECURETRUST AND 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 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. SECURETRUST 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 III(H) OF THIS CPS.

SecureTrust 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 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 on Liability

EXCEPT TO THE EXTENT CAUSED BY SECURETRUST'S WILLFUL MISCONDUCT, IN NO EVENT SHALL THE CUMULATIVE 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 SOUNDING IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, FOR BREACH OF A STATUTORY DUTY OR IN ANY OTHER WAY EXCEED TWO THOUSAND U.S. DOLLARS ($2,000.00).

SECURETRUST SHALL NOT BE LIABLE IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, FOR BREACH OF A STATUTORY DUTY OR IN ANY OTHER WAY (EVEN IF 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) 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 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 (See Section I(c) for more detail); (iii) has been tampered with; (iv) with respect to which the Key Pair underlying such Certificate or the cryptography algorithm used to generate such Certificate's Key Pair, has been Compromised by the action of any party other than SecureTrust (including without limitation the Subscriber or Relying Party); or (v) is the subject of misrepresentations or other misleading acts or omissions of any other party, including but not limited to 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 in the United States, 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 and the relationship between SecureTrust and the Applicant is not that of an agent and a principal. SecureTrust makes no representation to the contrary, either explicitly, implicitly, by appearance or otherwise. The Applicant has no authority to bind SecureTrust by contract or otherwise, to any obligation.

2. Indemnification by Applicant and Subscriber

Unless otherwise set forth in this CPS and/or Subscriber Agreement, Applicant and Subscriber, as applicable, hereby agree to indemnify and hold SecureTrust (including, but not limited to, its officers, directors, employees, agents, partner, 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 certificate requester) (b) any failure by the Applicant or the Subscriber to disclose a material fact, if such omission was made negligibly 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 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.

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 Texas, 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 Texas and any and all actions against SecureTrust or its affiliated companies must be brought in the State of Texas.

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 San Antonio, Texas. 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 represents the entire agreement between any Subscriber (including the Subscriber Agreement) or Relying Party (including the Relying Party Agreement) and SecureTrust and supersedes 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 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.

J. Confidentiality Policy

1. Individual Subscriber Information

Except as provided herein, certain information regarding Subscribers that is submitted with Certificate Requests or discovered during the validation process for Certificates will be kept confidential by SecureTrust (such as contact information for individuals, tax records, banking or financial statements, and credit card information) and SecureTrust shall not release such information without the prior consent of the Subscriber. Notwithstanding the foregoing, SecureTrust 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 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, information that can be found in the public domain, or to information regarding Subscribers that is already in the possession of or separately acquired by SecureTrust.

<u>2. Aggregate Subscriber Information</u>

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 reasonable opinion 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 and is in compliance with the CA/Browser Forum Guidelines. All enrollment forms are subject to review, approval and acceptance by SecureTrust. 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 Certificate Applications

<u>1. Enrollment</u>

Subscribers submit an EV Certificate Request, a signed Subscriber Agreement, and a digital CSR and provide additional documentation as necessary for SecureTrust to perform the EV validation process for EV certificate procurement.

a.) **EV Certificate Request**

The EV Cert request is received from the applicant or certificate requester and SecureTrust verifies the information in the request is accurate. The following data must be verified in the EV Certificate Request:

     i.   **Organization Name –** Full, legal name of Applicant as listed by incorporating agency and found in reliable source, i.e. Secretary of State Records.

     ii.   **Assumed Name** – The applicants DBA name as shown by the incorporating agency (if applicable).

     iii.   **Domain Name** – The fully qualified domain name for which the certificate is to be created.

     iv.   **Jurisdiction Data** – Applicant's City, State, Country of operation

     v.   **Incorporating Agency** – The full name of the Applicant's Incorporating Agency, as listed in Secretary of State Records or other credible sources.

     vi.   **Registration Number** – The business number assigned to the Applicant when the incorporated their business.

     vii.   **Applicant Address** – Full mailing address including telephone number

     viii.   **Certificate Approver and Certificate Requester** - Certificate approver and Certificate requester must be provided, as applicable.

b.) **Subscriber Agreement** – The Applicant must sign the Subscriber agreement before the EV Certificate Validation process can complete. SecureTrust may at its discretion use one Subscriber Agreement for multiple requests so long as all the multiple requests are mentioned in the Subscriber Agreement. The following components which must be verified in the Subscriber Agreement by SecureTrust before Certificate issuance are as follows:

     i. The contract signer, and applicant must be listed and signatures must be included.

         a.) By signing the Subscriber agreement, the applicant agrees to:

             1.) Verify the accuracy of the information provided

             2.) Properly protect their private key

             3.) Verify certificate information prior to installation

             4.) Use the Certificate only for lawful purposes

             5.) Promptly notify Secure Trust if Applicant's server is compromised.

6.) Promptly notify SecureTrust if Applicant's certificate is misused.

7.) Discontinue all use of the certificate after it expires or is revoked.

ii. Signature verification for the subscriber agreement

The signature must be a legally valid and an enforceable seal, handwritten signature, or enforceable digital signature. SecureTrust shall verify the signatures using one of the following methodologies:

1.) Contact Contract Signer or Certificate Requester via the Applicant's telephone number and verify the signature of the documents.

2.) Use a secure login process or digital signature mechanism

3.) Send a letter to the Applicant care of the Contract Signer or Certificate Requester and ask them to call/mail the CA to verify that they signed the documents.

c.) **Digital CSR**

Additionally, Subscribers 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 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 certificates issued in accordance with this CPS: Common Name (Fully Qualified Domain Name, or "FQDN"), Organization, City/Locality, State/Province, and Country.

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. Renewal / Competitive Upgrade

Each certificate must undergo the entire validation process upon certificate expiration for revalidation in accordance to the CA/Browser Forum Guidelines.

3. EV Validation Process.

The following applies to all EV Digital Certificates issued in accordance with this CPS and is based upon the requirements set in place by the CA/Browser Forum Guidelines (as defined below). SecureTrust will verify applicant legal existence, physical existence, operational existence, and domain control as shown below. In the event that there is a discrepancy between the following procedures and the CA/Browser Forum Guidelines, the CA/Browser Forum Guidelines will superceed the procedures detailed below.

A.) **Legal Existence**

Legal existence validation can be satifised with one or more of the following checks:

PRIVATE ORGANIZATIONS:

a.) Verification that the Applicant is listed with its incoporating agency and is not designated as "inactive", "invalid", "not current", or equivalent.

b.) Verification that the Applicant's real legal business name matches the information the incorporating agency has on file.

c.) Applicant's registration number must be accurate. In jurisdictions that do not assign a registration number, the date of incorporation will be used.

d.) Verification of Address and identity of Applicant's registered agent/office (if applicable).

e.) If applicant wishes for an assumed name or DBA to be included in the Certificate, SecureTrust will verify the DBA is registered with the incorporating agency in the proper jurisdiction, the name matches exactly to the name the incorporating agency has on file, and that the DBA is valid and current. Alternatively, a QIIS, a verified accountant letter, or a legal opinion letter may be used to verify a DBA in accordance with the CA/Browser Forum Guidelines.

GOVERNMENT ENTITIES:

a.) Verification that the Applicant is a legally recognized Government Entitiy in existence in the political subdivision in which such government operates.

b.) Verification that the Applicant's legal name matches Applicant's name in the EV Certificate Request.

c.) Verification of the Applicant's date of incorporation, registration, or formation, or a identifier for the legislative act that created the Government Entity. The information collected in this step will be used in the Registration Number field. In circumstances where this information is not available, appropriate language will be inserted into this field to indicate that the Subject is a Government Entity.

d.) If applicant wishes for an assumed name or DBA to be included in the Certificate, SecureTrust will verify the DBA is registered with the incorporating agency in the proper jurisdiction, the name matches exactly to the name the incorporating agency has on file, and that the DBA is valid and current. Alternatively, a QIIS, a verified accountant letter, or a legal opinion letter may be used to verify a DBA in accordance with the CA/Browser Forum Guidelines.

BUSINESS ENTITIES:

a.) Verify that the Applicant is engaged in business under the name submitted by the Applicant in the Application.

b.) Verify that the Applicant's formal legal name as recognized by the Registration Authority in Applican't Jurisdiction of Registration mathces Applicant's name in the EV Certificate Request.

c.) Applicant's registration number must be accurate. In jurisdictions that do not assign a registration number, the date of incorporation will be used.

d.) Verify the identitiy of the identified Principal Individual.

e.) If applicant wishes for an assumed name or DBA to be included in the Certificate, SecureTrust will verify the DBA is registered with the incorporating agency in the proper jurisdiction, the name matches exactly to the name the incorporating agency has on file, and that the DBA is valid and current. Alternatively, a QIIS, a verified accountant letter, or a legal opinion letter may be used to verify a DBA in accordance with the CA/Browser Forum Guidelines.

B.) **Physical Existence**

SecureTrust must verify Applicant's physical existence matches with their physical address. This will be done with the following checks:

a.) If Applicants place of business is in the same country as the location of their incorporation

>   i.) Securetrust may verify Applicant address and phone number by finding the information in one or more QIIS.
>
>   ii.) If Applicant has a different physical address than reflected in QIIS, or a Qulified Governmental Tax Information Source, SecureTrust or a qualified third party may perform a site visit.
>
>   iii.) A legal opinion letter or verified accountant letter can be used to satisfy the physical existence.
>
>   iv.) SecureTrust may verify the phone number by calling directory assistance.

b.) If Applicant's place of business is NOT in the same country as the location of incorporation

i.) A legal opinion letter or verified accountant letter can be used to verify address and phone number to satisfy physical existence.

ii.) Applicant's telephone number must also be verified as the main phone number for the Applicant's business through physically calling the number, verifying during a site visit, or obtaining a verified legal opinion.

c.) For Government Entity Applicants SecureTrust may rely on the address contained within QGIS databases in applicant's jurisdiction.

C.) **Operational Existence**

SecureTrust shall verify Applicant's business operations have been in effect longer than 3 years or Applicant is listed in a current version of a QIIS, or a Qualified Government Tax Information Source.

If neither of the above conditions is met, SecureTrust must:

a.) Receive authentic documentation (bank letter, proof of Demand Deposit Account, etc.) from a financial institution showing that the Applicant has a current Demand Deposit account.

Or

b.) A legal opinion letter or verified accountant letter will be used to satisfy operational existence.

D.) **Domain Name**

SecureTrust must verify the Applicant has exclusive control over the domain name that will appear on the EV certificate by:

a.) Checking if the domain is registered with ICANN-approved or IANA-approved registrar, and the WHOIS data is public and correct including name, physical address, and admin contact information.

b.) If above WHOIS information does not match,

i. SecureTrust may communicate with Applicant to have them change the information; or

ii. can verify the domain by receiving a verified legal opinion or verified accountant letter stating the Applicant's exclusive right to use the domain; or

iii. Can verify the domain by obtaining confirmation of the exclusive right from the contract signer and then the applicant making a visible change to a page on the second level of the domain for SecureTrust to view.

c.) If domain registration is private, SecureTrust may contact the Applicant through the domain registrar by e-mail or paper mail if the domain registrar offers services to forward such communication to the registered domain holder.

E.) **Verification of Contract Signer / Certificate Approver**

a. SecureTrust will verify the name, title and agency of the Contract Signer and Certificate Approver. This is typically done by contacting the Applicant's HR department for verification or through a verified legal opinion letter or verified accountant letter.

b. SecureTrust must verify that the Contract Signer has authorization by Applicant to enter into subscriber agreement.

c. SecureTrust must verify the Certificate Approver is expressly authorized by the Applicant to do the following:

   i. Submit, or authorize a Certificate Requester to submit an EV Certificate Request on behalf of Applicant

   ii. Provide and/or authorize a Certificate Requester to provide information about the Applicant as requested by SecureTrust for the issuance of the EV certificate.

   iii. Approve EV Certificate Requests submitted by a Certificate Requester.

b and c above can be satisfied by:

   i. A verified legal opinion or verified accountant letter which states that the Contract Signer has signing authority and the Certificate Approver has EV Certificate authority;

   ii. SecureTrust can obtain a corporate resolution from Applicant which states the Contract Signer has signing authority and additionally states the Certificate Approver has the EV authority. This resolution must be certified by appropriate company officer and SecureTrust must be able to reliably verify the company officer has signed the resolution and that he/she has the authority to sign the resolution;

   iii. SecureTrust can obtain confirmation from the Applicant which states the Contract Signer has the signing authority and the Certificate Approver has the EV authority;

   iv. SecureTrust and Applicant may mutually enter into a contract which states that the Contract Signer has the Signing Authority and also states that the certificate approver has the EV Authority; or

v. SecureTrust can obtain confirmation that the Contract Signer or Certificate Approver has proper authority of the Applicant by contacting an individual in a superior role within the company for verification of such. Additionally, the verifying individual in the superior role must be verified by contact Applicant's HR department.

If the Applicant expects to submit many EV Certificates, a contract can be established between the SecureTrust and the Applicant to make the process easier in the future. Under this process, SecureTrust must verify the name and title of Contract Signer, verify the employment of the Contract Signer, and also verified the Signing Authority of the Contract Signer via the steps above. The contract must include:

i. The Applicant is bound to the terms of the Subscriber Agreement.

ii. Established provisions for authenticating the Certificate Approver for each request.

iii. Provisions for re-confirmation of the EV Authority of the Certificate Approver.

iv. A secure procedure for the Applicant to revoke EV Authority authorization from certain Certificate Approvers.

4. Domain Names / Trademarks.

Domain names do not have to be meaningful or unique, but must match a second level domain name as posted by the InterNIC. SecureTrust is not involved in the recognition, authentication, or role of trademarks involved in domain names. Name disputes (including trademark disputes) are not resolved by SecureTrust, but are to be resolved between the Subscriber and other disputing parties by InterNIC at time of application according to applicable InterNIC rules and/or by courts of competent jurisdiction.

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 all of the information and material supplied by the applicant to be sufficiently verified, an EV Certificate will be issued to the Applicant by SecureTrust. Upon issuance of the Applicant's EV Certificate, SecureTrust will attach such EV Certificate to an e-mail and send such e-mail to the appropriate contacts. The e-mail will typically be sent only to the verified certificate

requester. In certain circumstances the e-mail may include a SecureTrust customer service representative telephone number and e-mail address for any technical or customer service problems. SecureTrust, in its sole discretion, may provide such technical or customer support to the Applicants/Subscribers.

SecureTrust may also deliver the Subscriber's signed Certificate via an online account download or through an Application Programming Interface (API).

E. Certificate Acceptance

The Applicant expressly indicates acceptance of a Certificate by using such Certificate or downloading and installing the Certificate. Additionally, all Applicant conditions listed in the Subscriber Agreement are enforced upon certificate acceptance.

F. Certificate Renewal and Rekey

Subscribers may renew certificates by either generating a new Key Pair to replace the expiring Key Pair (technically defined as "rekey") or by 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. Renewal Certificates will undergo an identical validation process as new certificates outlined in this CPS and in adhearance to the CA/Browser Forum Guidelines. 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. SecureTrust may provide discounted prices for renewal certificates.

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 / Certificate Requester contacts listed during enrollment submitted by the Certificate Requester, 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 Operational Period of an EV Certificate by posting the serial number of the Certificate to a Certificate Revocation List. SecureTrust will revoke and EV certificate when any of the following events occurs:

(1) The Subscriber requests revocation of its EV Certificate;

(2) The Subscriber indicates that the original EV Certificate Request was not authorized and does not retroactively grant authorization;

(3) SecureTrust obtains reasonable evidence that the Subscriber's Private Key (corresponding to the Public Key in the EV Certificate) has been compromised, or that the EV Certificate has otherwise been misused;

(4) SecureTrust receives notice or otherwise becomes aware that a Subscriber violates any of its material obligations under the Subscriber Agreement;

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

(6) SecureTrust receives notice or otherwise becomes aware of a material change in the information contained in the EV Certificate;

(7) A determination, in SecureTrust's sole discretion, that the EV Certificate was not issued in accordance with the terms and conditions of these Guidelines or the SecureTrust's EV Policies;

(8) If SecureTrust determines that any of the information appearing in the EV Certificate is not accurate.

(9) SecureTrust ceases operations for any reason and has not arranged for another EV CA to provide revocation support for the EV Certificate;

(10) SecureTrust's Private Key for that EV Certificate has been compromised;

(11) Such additional revocation events as SecureTrust publishes in its EV Policies; or

(12) SecureTrust receives notice or otherwise become aware that a Subscriber has been added as a denied party or prohibited person to a blacklist, or is operating from a prohibited destination under the laws of SecureTrust's jurisdiction of operation

2. Who Can Request Revocation

The only persons permitted to request revocation of a Certificate issued by SecureTrust is the Subscriber (including designated representatives; Certificate Approver, Contract Signer)

3. Procedure for Revocation Request

To request revocation, a Subscriber must 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. The message will state that, upon confirmation of the revocation request, SecureTrust will revoke the Certificate and that posting the revocation to the appropriate CRL will constitute notice to the Subscriber that the Certificate has been revoked. SecureTrust 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 SecureTrust). Upon receipt of the confirming e-mail message, SecureTrust will revoke the Certificate and the revocation will be posted to the appropriate CRL. Notification will 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 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.

I. Certificate Suspension

SecureTrust does not support Certificate suspension for EV Certificates.

J. Key Management

SecureTrust does not provide Subscriber Private Key protection or other Subscriber Private Key management services in connection with Certificates issued under this CPS.

K. Subscriber Key Pair Generation

SecureTrust does not provide Subscriber Key Pair generation or Subscriber Private Key protection for Certificates issued under this CPS.

L. Records Archival

SecureTrust shall maintain and archive records relating to the issuance of the Certificates for seven (7) years following the expiration of the applicable Certificate.

M. CA Termination

In the event that it is necessary for SecureTrust or its CAs to cease operation, SecureTrust makes 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 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 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) 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 incorporating biometrics, physical keys, and personal identification numbers. Additionally all secure server rooms require dual-person access controls.

C. Power and Air Conditioning

SecureTrust's CA facility is equipped with primary and backup power to assure continuous operation of its servers and its network connections. SecureTrust's facility is also equipted 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 and the CA/Browser Forum 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.

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 Key(s), SecureTrust shall promptly notify all Subscribers via e-mail and notify Relying Parties and others via the CRL and additional notice posted at www.securetrust.com/legal/, and shall revoke all Certificates issued with such SecureTrust 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 7 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-bit and 128-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 EV Certificates, the Subscriber typically uses the key generation utility provided with the web server software. SecureTrust does not require any particular standard for the module used to generate the keys.

For X.509 SSL Version 3 EV Certificates, SecureTrust generally populates the KeyUsage extension of Certificates in accordance with RFC 2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, January 1999.

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 define the following time periods for acceptable system outage and recovery time:

1. Vet a Subscriber – 10 days

2. Issue a Certificate – 10 days

3. Publish a CRL – 10 days

4. Audit Vetting Procedures – 30 days

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.

E. Internal Quality Review

SecureTrust will perform a quality review of a minimum of 3% of issued certificates. The review will ensure that all validation procedures were followed.

VI. CERTIFICATE AND CRL PROFILE

A. Certificate Profile

SecureTrust EV 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 2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, January 1999 ("RFC 2459"). Certificate extensions and their criticality, as well as cryptographic algorithm object identifiers, are populated according to the IETF RFC 2459 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 2459 standards.

B. CRL Profile

SecureTrust issued CRLs conform to all RFC 2459 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:

TrustWave Holdings, Inc,
120 N. LaSalle Street, Suite 1250
Chicago, IL 60602

Telephone - 312-873-7500
Facsimile – 443-782-0470

email: legal@atwcorp.com

B. Contact Person

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

TrustWave Holdings, Inc,
120 N. LaSalle Street, Suite 1250
Chicago, IL 60602

Telephone - 312-873-7500
Facsimile – 443-782-0470

email: legal@atwcorp.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 are 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. See Subscriber.

CA/Browser Forum Guidelines. CA/Browser Forum Guidelines for Extended Validation Certificates, Version 1.0, dated June 7, 2007 and found at http://www.cabforum.org/.

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 SecureTrust pursuant to this CPS.

Certificate Requester. Party who is employed by the Applicant, or an authorized agent who has expressed authority to represent the Applicant or a third party that fills out and submits an EV Certificate Request on behalf of the Applicant

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.

Contract Signer. Party who is employed by the Applicant, or an authorized agent who has expressed authority to represent the Applicant who has authority on behalf of the Applicant to sign Subscriber Agreements on behalf of the applicant.

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.

SecureTrust. SecureTrust Security Services, Inc.

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.

Operational 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.

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

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.

QGIS. Qualified Government Information Source. A regularly-updated and current online publicly available database designed for the purpose of accurately providing the information for which it is consulted, and which is generally recognized as a dependable source of such information provided they are maintained by a Government Entity, the reporting of data is required of data is required by law and false or misleading reporting is punishable with criminal or civil penalties.

QIIS. Qualified Independent Information Source. A regularly updated and current online publicly available database designed for the purpose of accurately providing the information for which it is consulted, and which is generally recognized as a dependable source of such information.

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.

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

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.

Verified Legal Opinion Letter. A verified legal opinion has to be authorized by an independent legal practitioner (lawyer or notary) and is based on this practitioner's stated familiarity with the relevant facts and practitioner's judgment/expertise.

Verified Legal Accountant Letter. Is authorized by an independent, professional accounting, obtained by and representing the Applicant. The letter is based on the practitioner's familiarity with the relevant facts and the exercise of the accounting practitioner's professional judgment and expertise.