True BusinessID® and True BusinessID with Extended Validation Certificate Practice Statement

TABLE of CONTENTS

I. INTRODUCTION

A. Overview

This Certificate Practice Statement (the "CPS") presents the principles and procedures GeoTrust employs in the issuance and life cycle management of True BusinessID®, True BusinessID Wildcard, and True BusinessID with Extended Validation ("EV") Certificates. This CPS and any and all amendments thereto are incorporated by reference into all of the above-listed GeoTrust Certificates. Internet service providers, hosting companies, or other businesses ("Partners") may perform some 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 Partners as if they were the Subscribers as closely as practicable.

B. 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.

C. Description and Use of Certificates

1. True BusinessID Certificates

True BusinessID Certificates are X.509 Certificates with SSL Extensions that chain to one of GeoTrust's trusted roots and which facilitate secure electronic commerce by providing limited authentication of a Subscriber's server and permitting SSL encrypted transactions between a Relying Party's browser and the Subscriber's server. In addition, GeoTrust may also enable the Certificate for use as a client Certificate.

2. True BusinessID Wildcard Certificates

True BusinessID Wildcard Certificates are X.509 Certificates with SSL Extensions that chain to one of GeoTrust's trusted roots and that are vetted to a specified level domain and may be used in connection with all next level higher domains that contain the specified vetted level domain. These certificates facilitate secure electronic commerce by providing limited authentication of a Subscriber's server and permitting SSL encrypted transactions between a Relying Party's browser and the Subscriber's server.

3. True BusinessID with Extended Validation Certificates

Extended Validation Certificates are certificates issued by GeoTrust in conformance with the Guidelines for Extended Validation Certificates published by the forum consisting of major certification authorities and browser vendors. Detailed procedures for processing Extended Validation Certificates are described in Appendix A1 to this CPS.

4. Operational Period of Certificates

True BusinessID Certificates and True BusinessID Wildcard Certificates have an Operational Period from one to five years from the date of issuance (depending on whether the Subscriber has purchased a one year, two year, or three year Certificate), unless another time period or expiration date is specified on such Certificate, or unless the Certificate is revoked prior to the expiration of the Certificate's Operational Period. If a Subscriber renews a Certificate within a specified period prior to expiration of an existing Certificate, GeoTrust may extend the Operational Period for the new Certificate by a specified number of days intended to give the Subscriber the approximate benefit of the remaining Operational Period of the existing Certificate. In addition, from time to time GeoTrust may extend the Operational Period of the Certificates it issues in connection with promotions or other packages. The specific details of these extensions of the Operational Period will be provided to the Subscriber by information posted on the

GeoTrust web site, the enrollment form, and/or the Subscriber Agreement. The Operational Period for a Certificate will be stated in the Certificate.

The maximum validity period for EV Certificates is further described in Section 8 of Appendix A1 to this CPS.

5. Installation of Certificates
Certificates may not be installed on more than a single server at a time unless Subscriber has requested to do so during the enrollment process and has paid the corresponding fees for installation on multiple servers.

6. Technical Requirements of Certificates
In order to use a Certificate, the appropriate server software must support SSL.

II. GENERAL PROVISIONS

A. Obligations

1. GeoTrust Obligations
GeoTrust will: (i) issue Certificates in accordance with this CPS; (ii) perform limited authentication of Subscribers as described in this CPS; (iii) revoke Certificates as described in this CPS; and (iv) perform any other functions which are described within this CPS.

2. Subscriber Obligations
Subscriber will submit truthful information about itself and its business entity, domain ownership and contacts, as applicable. Subscribers will at all times abide by this CPS and a Subscriber will immediately request revocation of a Certificate if the related Private Key is Compromised. The Subscriber will only use the Certificate for purposes of negotiating SSL sessions. The Subscriber is solely responsible for the protection of its Private Key and for notifying GeoTrust immediately in the event that its Private Key has been Compromised.

3. Relying Party Obligations
Relying Parties must verify that the Certificate is valid by examining the Certificate Revocation List ("CRL") before initiating a transaction involving such Certificate. GeoTrust does not accept responsibility for reliance on a fraudulently obtained Certificate or a Certificate that is on the CRL.

B. Fees

1. Issuance, Management, and Renewal Fees
GeoTrust is entitled to charge Subscribers for the issuance, management, and renewal of Certificates. The fees charged will be as stated on GeoTrust'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
GeoTrust 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
GeoTrust does not charge a fee as a condition of making the CRL required by CPS Section II. I available in a repository or otherwise available to Relying Parties. GeoTrust may, however, charge a fee for providing customized CRLs, OCSP services, or other value-added revocation and status information services. GeoTrust 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 GeoTrust's prior express written consent.

4. Fees for Other Services Such as Policy Information
GeoTrust does not charge a fee for access to this CPS.

5. Refund and Reissue Policy
GeoTrust's refund policy is available for review on the GeoTrust web site at http://www.geotrust.com/resources. 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 ("CSR") to GeoTrust or request reissue of a Certificate based upon a prior CSR previously provided to GeoTrust by the Subscriber.

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

C. Compliance Audit

An annual WebTrust for Certification Authorities examination will be performed for the Certificates issued under this CPS. GeoTrust's CA compliance audits are performed by a public accounting firm that (1) demonstrates proficiency in public key infrastructure technology, information security tools and techniques, security auditing, and the third-party attestation function, and (2) is accredited by the American Institute of Certified Public Accountants (AICPA), which requires the possession of certain skill sets, quality assurance measures such as peer review, competency testing, standards with respect to proper assignment of staff to engagements, and requirements for continuing professional education. Compliance audits of GeoTrust's operations will be performed by a public accounting firm that is independent of GeoTrust. The scope of GeoTrust's annual WebTrust for Certification Authorities examination will include certificate life cycle management and CA business practices disclosure.

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

D. Limited Warranty/Disclaimer

GeoTrust 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 GeoTrust 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 GeoTrust 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, GEOTRUST 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 GEOTRUST 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, GEOTRUST 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 GEOTRUST, 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 GEOTRUST AND RELIED UPON BY A RELYING PARTY. GEOTRUST 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. GEOTRUST 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(I) OF THIS CPS. GeoTrust 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 GeoTrust is not responsible or liable for any misrepresentations or incomplete representations of Certificates or any information contained therein caused by another party's application software or graphical user interfaces. The cryptographic key-generation technology used by Applicants, Subscribers and Relying Parties in conjunction with the Certificates may or may not be subject to the intellectual property rights of third parties. It is the responsibility of Applicants, Subscribers and Relying Parties to ensure that they are using technology that is properly licensed or to otherwise obtain the right to use such technology

E. Limitation on Liability

EXCEPT TO THE EXTENT CAUSED BY GEOTRUST'S WILLFUL MISCONDUCT, IN NO

EVENT SHALL THE CUMULATIVE LIABILITY OF GEOTRUST 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 TEN THOUSAND U.S. DOLLARS ($10,000.00).

GEOTRUST SHALL NOT BE LIABLE IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, FOR BREACH OF A STATUTORY DUTY OR IN ANY OTHER WAY (EVEN IF GEOTRUST 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 GeoTrust 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 GeoTrust (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 GeoTrust 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.

GeoTrust's limitation of liability for EV certificates is further described in Section 37 of Appendix A1 to this CPS.

F. Force Majeure

GeoTrust 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 GeoTrust.

G. Financial Responsibility

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

2. Indemnification by Applicant and Subscriber
Applicant and Subscriber, as applicable, hereby agrees to indemnify and hold GeoTrust (including, but not limited to, its officers, directors, employees, agents, successors and assigns) harmless from any claims, actions, or demands that are caused by the use or publication of a Certificate and that arises from (a) any false or misleading statement of fact by the Applicant (or any person acting on the behalf of the Applicant); (b) any failure by the Applicant or the Subscriber to disclose a material fact, if such omission was made 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 GeoTrust, 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 GeoTrust shall be governed by the substantive laws of the Commonwealth of Massachusetts, 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.

2. Dispute Resolution Procedures
Any dispute, controversy or claim arising under, in connection with or relating to this CPS or any Certificate issued by GeoTrust 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 Boston, Massachusetts. 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 GeoTrust 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, if any) or Relying Party and GeoTrust 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 GeoTrust 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

GeoTrust shall operate a CRL that will be available to both Subscribers and Relying Parties. GeoTrust shall post the CRL online at least weekly in a DER format except as otherwise provided in GeoTrust's Business Continuity Plan. Each CRL is signed by the issuing GeoTrust CA. The procedures for revocation are as stated elsewhere in this CPS. GeoTrust retains copies of all Certificates for the life of the CA, but does not archive or retain expired or superceded CRLs. GeoTrust 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 on enrollment forms for Certificates will be kept confidential by GeoTrust (such as contact information for individuals and credit card information) and GeoTrust shall not release such information without the prior consent of the Subscriber. Notwithstanding the foregoing, GeoTrust 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 GeoTrust'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 GeoTrust, (c) to an acquirer of GeoTrust or substantially all of the assets related to any portion of its business, to the extent that such information pertains to the acquired assets or line(s) of business, and (d) to third party service providers and vendors performing functions related to the GeoTrust products and services or as otherwise necessary for GeoTrust to perform its responsibilities under this Agreement, subject to such third parties' agreement to maintain the confidentiality of personally-identifiable Subscriber information. 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 GeoTrust. Subscriber acknowledges that Subscriber information will be controlled and processed in the United States, and to the extent that Subscriber is located outside the United States, Subscriber expressly consents to the transfer of such information to the United States for such control and processing.

2. Aggregate Subscriber Information
Notwithstanding the previous Section, GeoTrust may disclose Subscriber information on an aggregate basis, and the Subscriber hereby grants to GeoTrust 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.

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. GeoTrust may refuse to issue or may revoke Certificates if in the reasonable opinion of GeoTrust 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 Certificate shall complete a GeoTrust enrollment form in a form prescribed by GeoTrust. All enrollment forms are subject to review, approval and acceptance by GeoTrust. All Applicants are required to include a Domain Name within the enrollment form and an Organizational Name that will also appear on the Certificate. A Certificate may contain additional information as well. GeoTrust does not verify the authority of the Subscriber to request a Certificate. GeoTrust 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. Certificate Information

1. Domain Name
GeoTrust will verify that the Subscriber had the right to use the Domain Name submitted by the Subscriber at the time it submitted its application. For instance, GeoTrust may perform this verification by confirming that the Subscriber is the same person or entity that holds the Domain Name registration from the relevant domain name registrar or that the Subscriber is otherwise authorized to use such Domain Name. Domain names do not have to be meaningful or unique, but must match a second level domain name as posted by InterNIC. GeoTrust is not involved in the recognition, authentication, or role of trademarks involved in domain names. Name disputes (including trademark disputes) are not resolved by GeoTrust, 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.

2. Organizational Name
GeoTrust will take reasonable steps to establish that a Certificate request made on behalf of that Organization is legitimate and properly authorized. GeoTrust will ensure the following: (a) the Organizational Name appears in conjunction with a country and possibly a state or province of other locality to sufficiently identify its place of registration or a place where it is currently doing business; and (b) in the case of an Organization that could reasonably be expected to be registered with a local, state or national authority, in certain circumstances GeoTrust will obtain, view and verify copies of the registration documents. For instance, GeoTrust may (w) verify the validity of the registration through the authority that issued it, or (x) verify the validity of the registration through a reputable third party database or other resource, or (y) verify the validity of the Organization through a trusted third party, or (z) confirm that the Organization exists if such Organization is not the type that is typically registered or is capable of being verified under clause (y).

In addition, to prove that a Certificate is duly authorized by the Organization, GeoTrust will typically request the name of a contact person who is employed by or is an officer of the Organization. GeoTrust will also typically require a form of authorization from the Organization confirming its intent to obtain a Certificate and will usually document the Organization's contact person. GeoTrust normally confirms the contents of this authorization with the listed contact person.

C. Procedure for Processing Certificate Applications

Subscribers submit their Public Key to GeoTrust 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: Common Name, Organization, and Country. The following additional information is required on the enrollment form: the names, e-mail addresses, and telephone numbers for the Administrative, Technical, Support, and Billing points of contact.

GeoTrust will process the Certificate enrollment forms to confirm the information on the Certificates as discussed above. However, GeoTrust reserves the right to waive such procedures and issue a Certificate utilizing different authentication procedures in certain circumstances; provided that (a) the general principles for verifying the application information is maintained, and (b) and such issuance is approved by a GeoTrust Director Level or above. In addition, GeoTrust may use subcontractors or other third parties to assist in the performance of its operational requirements or any other obligation under this CPS.

EV Certificate processing is performed in terms of the procedures described in Appendix A.

D. Application Issues

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

E. Certificate Delivery

If GeoTrust finds that the applicant's enrollment form was sufficiently verified, then the applicant's Certificate will be signed by GeoTrust. Upon signing the applicant's Certificate, GeoTrust will attach such Certificate to an e-mail and send such e-mail to the appropriate contacts or make the Certificate available via the Application Programming Interface (API). The e-mail will typically be sent to the administrative contact, technical contact and billing contact designated by the Subscriber. Notification will not be sent to others than the subject of the Certificate and the subject's designated contacts. In certain circumstances the e-mail may include a GeoTrust customer service representative telephone number and e-mail address for any technical or customer service problems. GeoTrust, in its sole discretion, may provide such technical or customer support to the applicants/Subscribers. GeoTrust does not distribute Certificates via Integrated Circuit Cards (ICC) to Subscribers.

F. Certificate Acceptance

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

G. Certificate Renewal and Rekey

Prior to the expiration of an existing Certificate, it is necessary for the Subscriber to obtain a new Certificate to maintain continuity of Certificate usage. Subscribers have the option of generating a new Key Pair to replace the expiring Key Pair (technically defined as "rekey") or of creating a new CSR 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 are subject to the same authentication steps outlined in this CPS as apply to initial issuance of a Certificate except that Subscriber will not be required to submit registration documents to GeoTrust if Subscriber's (a) Organization name has not changed, (b) fully qualified Domain Name has not changed, and (c) Subscriber has not indicated in the enrollment form that such information has changed during the time since it was originally submitted. Expiring Certificates are not revoked by GeoTrust 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 GeoTrust's web site. GeoTrust may provide discounted prices and extended Operational Periods (see I.C.3) for renewal Certificates.

H. Certificate Expiration

GeoTrust 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, GeoTrust likely will not send expiration notices to that party due to contractual limitations.

I. Certificate Revocation

1. Circumstances For Revocation
Certificate revocation is the process by which GeoTrust prematurely ends the Operational Period of a Certificate by posting the serial number of the Certificate to a CRL.

A Subscriber shall inform GeoTrust 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; or
• upon a change in the ownership of a Subscriber's web server.

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

GeoTrust shall revoke a Certificate:
• upon request of a Subscriber as described above;
• in the event of Compromise of GeoTrust's Private Key used to sign a Certificate;
• upon the Subscriber's breach of either this CPS or Subscriber Agreement;
• if GeoTrust determines that the Certificate was not properly issued; or
• in the event the Certificate is installed on more than a single server at a time without permission of GeoTrust.

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

A refund and/or reissue request by a Subscriber pursuant to Section II.B.5 will not be treated as a request for revocation of a Certificate under this subsection unless the Subscriber specifically requests revocation of the Certificate.

2. Who Can Request Revocation
The only persons permitted to request revocation of a Certificate issued by GeoTrust are the Subscriber (including designated representatives), and the administrative or technical contact.

3. Procedure For Revocation Request
To request revocation, a Subscriber must contact GeoTrust, 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, GeoTrust will seek confirmation of the request by e-mail message to the person requesting revocation (as defined in Section III.I.2 above). The message will state that, upon confirmation of the revocation request, GeoTrust 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. GeoTrust 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 GeoTrust). Upon receipt of the confirming e-mail message, GeoTrust 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 GeoTrust 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 GeoTrust's Private Key used to sign a Certificate; GeoTrust 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.

In addition, revocation of an EV Certificate may be requested by completing the appropriate form on GeoTrust's website at http://www.geotrust.com/ev.

J. Certificate Suspension

GeoTrust does not support Certificate suspension for the Certificates.

K. Key Management

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

L. Subscriber Key Pair Generation

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

M. Records Archival

GeoTrust shall maintain and archive records relating to the issuance of the Certificates for three (3) years following the issuance of the applicable Certificate.

N. CA Termination

In the event that it is necessary for GeoTrust or its CAs to cease operation, GeoTrust will make a commercially reasonable effort to notify Subscribers, Relying Parties, and other affected entities of such termination in advance of the CA termination. Where CA termination is required, GeoTrust will develop a termination plan to minimize disruption to Subscribers and Relying Parties. Such termination plans may address the following, as applicable:
- Provision of notice to parties affected by the termination, such as Subscribers and Relying Parties, informing them of the status of the CA,
- Handling the cost of such notice,
- The revocation of the Certificate issued to the CA by GeoTrust,

• The preservation of the CA's archives and records for the time periods required in this CPS,
• The continuation of Subscriber and customer support services,
• The continuation of revocation services, such as the issuance of CRLs,
• The revocation of unexpired unrevoked Certificates of Subscribers and subordinate CAs, if necessary,
• The payment of compensation (if necessary) to Subscribers whose unexpired, unrevoked Certificates are revoked under the termination plan or provision, or alternatively, the issuance of replacement Certificates by a successor CA,
• Disposition of the CA's Private Key and the hardware tokens containing such Private Key,
• Provisions needed for the transition of the CA's services to a successor CA, and
• The identity of the custodian of GeoTrust's CA and RA archival records. Unless a different custodian is indicated through notice to Subscribers and Relying Parties, the Registered Agent for GeoTrust, Inc., a Delaware corporation, shall be the custodian.

IV. PHYSICAL SECURITY CONTROLS

A. Site Location and Construction

GeoTrust's CA operations are conducted within GeoTrust facilities that meet WebTrust for CAs audit requirements. All GeoTrust CA
operations are conducted within a physically protected environment designed to deter, prevent, and detect covert or overt penetration.
GeoTrust's CAs are physically located in a highly secure facility that includes the following:
• Slab to slab barriers
• Electronic control access systems
• Alarmed doors and video monitoring
• Security logging and audits
• Proximity card access for specially approved employees with defined levels of management approval required

B. Physical Access Controls

Access to the GeoTrust CA facility requires the three authentication factors of "be and have" incorporating biometrics, keys, and proximity cards. Access to the facility requires a minimum of two authorized GeoTrust employees and is checked at three independent physical locations.

C. Power and Air Conditioning

GeoTrust's CA facility is equipped with primary and backup:
• Power systems to ensure continuous, uninterrupted access to electric power and
• Heating/ventilation/air conditioning systems to control temperature and relative humidity.

D. Water Exposures

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

E. Fire Prevention and Protection

The fire detection system in GeoTrust CA facility tests air health and looks for certain signatures of possible fire conditions in the air. In addition, the GeoTrust CA facility has a pre-action water suppression system. When temperatures above 300 degrees are detected, the effected sprinkler head will release water on the area where the temperature rise is detected.

F. Media Storage

All media containing production software and data, audit, archive, or backup information is stored within multiple GeoTrust facilities in TL-30 rated safes with appropriate physical and logical access controls designed to limit access to authorized personnel and protect such media from accidental damage.

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 GeoTrust's normal waste disposal requirements.

H. Off-Site Backup

GeoTrust 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 offsite
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 GeoTrust 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 GeoTrust management.

Certificates are issued off the Equifax Secure Certificate Authority CA, the Equifax Secure eBusiness CA-1, or the Equifax Secure Global eBusiness CA-1 (the "CA Certificates").

The EV CA certificate hierarchy contains an off-line CA that is located at a secure facility managed by VeriSign in accordance with its CPS at http://www.verisign.com/repository/index.html.

The cryptographic modules used for key generation and storage meet the requirements of FIPS 140-2 level 3. The CA Root Keys for each CA Certificate were generated and are stored in hardware and are backed up but not escrowed. The Root Keys for each CA Certificate are maintained under m out of n multiperson control.

The Root Keys for each CA Certificate may be used for Certificate signing (secure e-mail and server authentication), CRL signing, and off-line CRL signing.

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

GeoTrust generally provides the full certificate chain (including the issuing CA Certificate and any CA Certificates in the chain) to the Subscriber upon Certificate issuance. GeoTrust CA Certificates may also be downloaded from the GeoTrust web site at http://www.geotrust.com/resources.

There are no restrictions on the purposes for which the CA Key Pair may be used. The usage period or active lifetime for the Equifax Secure Certificate Authority CA Public and Private Keys is through August 22, 2018, and are generally available in the Root Key Store of the applicable browser or application software. The usage period or active lifetime for the Equifax Secure Certificate eBusiness CA-1 and Equifax Secure Certificate Global eBusiness CA-1 Public and Private Keys is through June 21, 2020, and are generally available in the Root Key Store of the applicable browser or application software.

GeoTrust 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 GeoTrust Root Key(s) (including the CA Certificates), GeoTrust shall promptly notify all Subscribers via email and notify Relying Parties and others via the CRL and additional notice posted at www.geotrust.com, and shall revoke all Certificates issued with such GeoTrust Root Key(s).

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

GeoTrust 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

GeoTrust recommends that Subscribers select the highest encryption strength option (e.g., 1024-bit) when generating their certificate requests. All GeoTrust certificates will accommodate the use of domestic and international 128-, 56-, and 40-bit strength browsers and web servers. Generation of Subscriber Key Pairs is generally performed by the Subscriber, and may be generated in either hardware or software. For server certificates, the Subscriber typically uses the key generation utility provided with the web server software. GeoTrust does not require any particular standard for the module used to generate the keys. Key pairs generated by the Subscriber for Certificates may be used for server authentication. There are no purposes for which GeoTrust restricts the use of the Subscriber Private Key.

For X.509 Version 3 Certificates, GeoTrust generally populates the KeyUsage extension of Certificates in accordance with RFC 3280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002.

C. Business Continuity Management Controls

GeoTrust has business continuity plans (BCP) to maintain or restore the GeoTrust 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 - 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, and monthly to GeoTrust's disaster recovery site, but may be performed less frequently in GeoTrust's discretion according to production schedule requirements. The recovery facilities are approximately 800 miles from the GeoTrust CA facility's main site.

D. Event Logging

GeoTrust CA event journal data is archived both daily and monthly. Daily event journals are reviewed several times each week. Monthly event journals are reviewed monthly.

VI. CERTIFICATE AND CRL PROFILE

A. Certificate Profile

GeoTrust Certificates conform to (a) ITU-T Recommendation X.509 Version 3 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997, and (b) RFC 3280: Internet X.509 Public Key Infrastructure Certificate and 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 GeoTrust'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. GeoTrust does not apply any specific Certificate Policy Object Identifier(s), but instead 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.

EV Certificate certificate content and profile requirements are discussed in Section 6 of Appendix A3 to this CPS.

B. CRL Profile

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

VII. CPS ADMINISTRATION

A. CPS Authority

The authority administering this CPS is the GeoTrust PKI Policy Authority. Inquiries to GeoTrust's PKI Policy Authority should be addressed as follows:
GeoTrust, Inc.
487 E Middlefield Road
Mountain View, CA 94043 USA
pkipolicy@geotrust.com
GeoTrust does not support a Certificate Policy (CP) for the Certificates.

B. Contact Person

Address inquiries about the CPS to pkipolicy@geotrust.com or to the following address:
PKI Policy Administrator
GeoTrust, Inc.
487 E Middlefield Road
Mountain View, CA 94043 USA

C. CPS Change Procedures

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

VIII. DEFINITIONS

CA. Certification Authority.

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

Compromise. Suspected or actual unauthorized disclosure, loss, loss of control over, or use of a Private Key associated with Certificate.

CRL. See Certificate Revocation List.

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.

GeoTrust. GeoTrust, 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 would typically begin on the date the Certificate is issued (or such later date as specified in the Certificate), and ends on the date and time it expires as noted in the Certificate or is earlier revoked unless it is suspended.

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

Principal Individual)s). Individuals of a Private Organization, Government Entity or Business Entity that are either owners, partners, managing members, directors or officers, as identified by their title of employment, or an employee, contractor or agent authorized by such entity or organization to conduct business related to the request, issuance and use of EV Certificates.

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 GeoTrust. A Public Key is used to verify the digital signature of a message purportedly sent by the holder of the corresponding Private Key.

Registration Agency. A Governmental Agency that registers business information in connection with an entity's business formation or authorization to conduct business under a license, charter or other certification. A Registration Agency MAY include, but is not limited (i) a State Department of Corporations or a Secretary of State; (ii) a licensing agency, such as a State Department of Insurance; or (iii) a chartering agency, such as a state office or department of financial regulation, banking or finance, or a federal agency such as the Comptroller of Currency (OCC) or Office of Thrift Supervision (OTC)

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 GeoTrust to sign the Certificates.

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

Subscriber. A person or entity who (1) is the subject named or identified in a Certificate issued to such person or entity, (2) holds a Private Key that corresponds to a Public Key listed in that Certificate, and (3) 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.

Subsidiary Company. A subsidiary company is defined, for EV, as a company that is wholly owned by Applicant as verified by referencing a QIIS or from financial statement supplied by a registered Chartered Professional Accountant (CPA) or equivalent outside of the USA.

[v. 2.7 07-01-07]

Appendix A1
Supplemental Validation Procedures for Extended Validation SSL Certificates

TABLE OF CONTENTS

A. INTRODUCTION

1. Introduction

This Appendix documents supplemental procedures to GeoTrust's currently published CPS procedures for issuing Extended Validation Certificates ("EV Certificates") in terms of the Guidelines for Extended Validation Certificates ("Guidelines"). The Guidelines describe certain of the minimum requirements that a Certificate Authority (CA) must meet in order to issue EV Certificates. Organization information from Valid EV Certificates may be displayed in a special manner by certain software applications (e.g., browser software) in order to provide users with trustworthy confirmation of the identity of the entity that controls the website they are accessing.

B. BASIC CONCEPT OF THE EV CERTIFICATE

2. Purpose of EV Certificates.

EV Certificates are intended for use in establishing web-based data communication conduits via TLS/SSL protocols.

(a) Primary Purposes

Per the guidelines, the primary purposes of an EV Certificate are to:

- Identify the legal entity that controls a website: Provide a reasonable assurance to the user of an Internet browser that the website the user is accessing is controlled by a specific legal entity identified in the EV Certificate by name, address of Place of Business, Jurisdiction of Incorporation or Registration, and Registration Number; and
- Enable/encrypted communications with a website: Facilitate the exchange of encryption keys in order to enable the encrypted communication of information over the Internet between the user of an Internet browser and a website.

(b) Secondary purposes

The secondary purpose of an EV Certificate is to help establish the legitimacy of a business claiming to operate a website by confirming its legal and physical existence, and to provide a vehicle that can be used to assist in addressing problems related to phishing and other forms of online identity fraud. By providing more reliable third-party verified identity and address information regarding the owner of a website, EV Certificates may help to:

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

(c) Excluded Purposes

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

- That the Subject named in the EV Certificate is actively engaged in doing business;
- That the Subject named in the EV Certificate complies with applicable laws;
- That the Subject named in the EV Certificate is trustworthy, honest, or reputable in its business dealings; or
- That it is "safe" to do business with the Subject named in the EV Certificate.

3. EV Certificate Warranties and Representations

(a) By GeoTrust

Beneficiaries of EV Certificates may be:

- The Subscriber entering into the Subscriber Agreement for the EV Certificate;
- The Subject named in the EV Certificate;
- All Application Software Vendors with whom the CA or its Root CA has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Vendors;
- All Relying Parties that actually rely on such EV Certificate during the period when it is Valid.

When GeoTrust issues an EV Certificate, it represents and warrants to the EV Certificate Beneficiaries, during the period when the EV Certificate is Valid, that it has followed the requirements of the Guidelines and its EV Policies in issuing the EV Certificate and in verifying the accuracy of the information contained in the EV Certificate ("EV Certificate Warranty"). This EV Certificate Warranty specifically includes, but is not limited to, the following warranties:

- Legal Existence: GeoTrust has confirmed with the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration that, as of the date the EV Certificate was issued, the Subject named in the EV Certificate legally exists as a valid organization or entity in the Jurisdiction of Incorporation or Registration;
- Identity: GeoTrust has confirmed that, as of the date the EV Certificate was issued, the legal name of the Subject named in the EV Certificate matches the name on the official government records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration, and if an assumed name is also included, that the assumed name is properly registered by the Subject in the jurisdiction of its Place of Business;
- Right to Use Domain Name: GeoTrust has taken all steps reasonably necessary in terms of the Guidelines to verify that, as of the date the EV Certificate was issued, the Subject named in the EV Certificate owns or has the exclusive right to use the domain name(s) listed in the EV Certificate;
- Authorization for EV Certificate: GeoTrust has taken all steps reasonably necessary in terms of the Guidelines to verify that the Subject named in the EV Certificate has authorized the issuance of the EV Certificate;
- Accuracy of Information: GeoTrust has taken all steps reasonably necessary to verify that all of the other information in the EV Certificate is accurate, as of the date the EV Certificate was issued;
- Subscriber Agreement: The Subject named in the EV Certificate has entered into a legally valid and enforceable Subscriber Agreement with GeoTrust that satisfies the requirements of the Guidelines;

o Status: GeoTrust will follow the requirements of these Guidelines and maintain a 24 x 7 online-accessible Repository with current information regarding the status of the EV Certificate as Valid or revoked; and

o Revocation: GeoTrust will follow the requirements of the Guidelines and promptly revoke the EV Certificate upon the occurrence of any revocation event as specified in the Guidelines and this Appendix.

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

o The Subject named in the EV Certificate is actively engaged in doing business;

o The Subject named in the EV Certificate complies with applicable laws;

o The Subject named in the EV Certificate is trustworthy, honest, or reputable in its business dealings; or

o It is "safe" to do business with the Subject named in the EV Certificate.

(b) By the Subscriber

GeoTrust will require, as part of the Subscriber Agreement, that the Subscriber make the commitments and warranties set forth in Subscriber Agreement Requirements section of these Guidelines, for the benefit of GeoTrust and the EV Certificate Beneficiaries.

C. COMMUNITY AND APPLICABILITY

4. Issuance of EV Certificates

When issuing EV Certificates, GeoTrust satisfies the following requirements as required by the Guidelines:

(a) Compliance

GeoTrust shall at all times:

(1) Comply with all laws applicable to its business and the certificates it issues in each jurisdiction where it operates;

(2) Comply with the requirements of the EV Guidelines;

(3) Comply with the requirements of (i) the then-current WebTrust Program for CAs, and (ii) the then-current WebTrust EV Program, or an equivalent for both (i) and (ii) as approved by the CA/Browser Forum; and

(4) Be licensed as a CA in each jurisdiction where it operates if licensing is required by the law of such jurisdiction for the issuance of EV Certificates.

(b) EV Policies

(1) **Implementation**
The GeoTrust CPS together with this Appendix A to the GeoTrust CPS:

(A) Implement the requirements of the Guidelines as they are revised from time-to-time;

(B) Implement the requirements of (i) the then current WebTrust Program for CAs, and (ii) the then-current WebTrust EV Program, or an equivalent for both (i) and (ii) as approved by the CA/Browser Forum;

(C) Specify the CA's and its Root CA's entire root certificate hierarchy including all roots that its EV Certificates depend on for proof of those EV Certificates' authenticity. GeoTrust's root hierarchy structure is available at http://www.geotrust.com/ev

(2) **Disclosure**
GeoTrust publicly discloses its EV policies through this CPS that is available on a 24x7 basis from the GeoTrust online repository..

(3) **Commitment to Comply with Guidelines**
GeoTrust conforms to the current version of the ***CA/Browser Forum Guidelines for Extended Validation Certificates*** ("Guidelines") published at http://www.cabforum.org. In the event of any inconsistency between this document and those Guidelines, those Guidelines take precedence over this document.

In addition, GeoTrust will include (directly or by reference) the applicable requirements of the Guidelines in all contracts with subordinate CAs, RAs, Enterprise RAs, and subcontractors, that involve or relate to the issuance or maintenance of EV Certificates. GeoTrust shall enforce compliance with such terms.

(c) Insurance

GeoTrust maintains the following insurance, with a company rated no less than A- as to Policy Holder's Rating in the current edition of Best's Insurance Guide, related to its performance and obligations under the EV Guidelines as follows:

- Commercial General Liability insurance (occurrence form) with policy limits of at least $2 million in coverage, and
- Professional Liability/Errors & Omissions insurance, with policy limits of at least $5 million in coverage, and including coverage for (i) claims for damages arising out of an act, error, or omission, unintentional breach of contract, or neglect in issuing or maintaining EV Certificates, and (ii) claims for damages arising out of infringement of the proprietary rights of any third party (excluding copyright, and trademark infringement), and invasion of privacy and advertising injury

5. Obtaining EV Certificates

In terms of the Guidelines, EV Certificates can only be issued to Private Organizations, Business Entities and Government Entities that satisfy the requirements specified below:

(a) Private Organization Subjects

GeoTrust may issue EV Certificates to Private Organizations that satisfy the following requirements:

(1) The organization MUST be a legally recognized entity whose existence was created by a filing with (or an act of) the Incorporating or Registration Agency, or Governing Body in its Jurisdiction of Incorporation or Registration (e.g., by issuance of a certificate of incorporation), or is an entity that is chartered by a state or federal regulatory agency;

(2) The organization MUST have designated with the Incorporating or Registration Agency, or Governing Body a Registered Agent, Registered Office (as required under the laws of the Jurisdiction of Incorporation or Registration) or an equivalent facility;

(3) The organization MUST not be designated on the records of the Incorporating or Registration Agency, or Governing Body by labels such as" inactive," "invalid," "not current," or the equivalent;

(4) The Private organization MUST have a verifiable physical existence and business presence

(5) The organization's Jurisdiction of Incorporation or Registration and/or its Place of Business MUST NOT be in any country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and

(6) The organization MUST NOT be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.

(b) Government Entity Subjects

GeoTrust may issue EV Certificates to Government Entities that satisfy the following requirements:

(1) The legal existence of the Government Entity is established by the political subdivision in which such Government Entity operates; I;

(2) The Government Entity MUST NOT be in any country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and

(3) The Government Entity MUST NOT be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.

(c) Business Entities

GeoTrust MAY issue EV Certificates to Business Entities that satisfy the following requirements:

(1) The Business Entity MUST be a legally recognized entity whose formation included the filing of certain forms with the Registration Agency in its Jurisdiction ,the issuance or approval by such Registration Agency of a charter, certificate, or license, and whose existence can be verified with that Registration Agency;

(2) The Business Entity MUST have a verifiable physical existence and business presence;

(3) At least one Principal Individual associated with the Business Entity MUST be identified and validated. ;

(4) The identified Principal Individual MUST attest to the representations made in the Subscriber Agreement;

Where the Business Entity represents itself under an assumed name, GeoTrust verifies the Business Entity's use of the assumed name pursuant to the requirements of Section 15 herein;

D. EV CERTIFICATE CONTENT AND PROFILE

6. EV Certificate Content Requirements

This section sets forth minimum requirements for the content of the EV Certificate as they relate to the identity of the CA and the Subject of the EV Certificate.

(a) Subject Organization Information

Subject to the requirements of the Guidelines, the EV Certificate shall include the following information about the Subject organization in the fields listed ("Subject Organization Information"):

(1) Organization name

The validated organization name is included in the organizationName field OID 2.5.4.10)

This field contains the Subject's full legal organization name as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration, or as otherwise verified as provided herein. GeoTrust MAY abbreviate the organization prefixes or suffixes in the Organization name, e.g., if the QGIS shows "*Company Name* Incorporated" GeoTrust MAY include *Company Name*, inc. GeoTrust uses common abbreviations that are generally accepted in the Jurisdiction of Incorporation or Registration.

In addition, an assumed name or d/b/a name used by the Subject MAY be included at the beginning of this field, provided that it is followed by the full legal organization name in parenthesis. If the combination of the full legal organization name and the assumed or d/b/a name exceeds 64 characters as defined by RFC 3280, GeoTrust will use only the full legal organization name in the certificate.

If the Organization name by itself exceeds 64 characters, GeoTrust MAY abbreviate parts of organization name, and/or omit non-material words in the organization name in such a way that the name in the certificate does not exceed the 64 character limit, and a Relying Party will not be misled into thinking they are dealing with a different Organization.

(2) Domain name

The validated domain name is included in the subject: commonName field (OID 2.5.4.3) and/or SubjectAlternativeName as a DNS Name

This field contains one or more host domain name(s) owned or controlled by the Subject and to be associated with Subject's server. Such server may be owned and operated by the Subject or another entity (e.g., a hosting service). Wildcard certificates are not allowed for EV certificates.

(3) Business Category:

The Business Category is included in the subject:businessCategory (OID 2.5.4.15)

This field contains one of the following strings: 'V1.0, Clause 5.(b)', 'V1.0, Clause 5.(c)' or 'V1.0, Clause 5.(d)', depending whether the Subject qualifies under the terms of Section 5b, 5c, or 5d of the Guidelines for Extended Validation Certificates, respectively.

Subject Type	Business Category string
Private Organization	V1.0, Clause 5.(b)
Government Entity	V1.0, Clause 5.(c)
Business Entity	V1.0, Clause 5.(d)

Table 1 Business category field content

(4) Jurisdiction of Incorporation or Registration

GeoTrust will include the Subject's validated Jurisdiction of Incorporation or Registration using the fields shown in Table 1 below.

Address Part	Required/Optional	Certificate Field
Locality	If required	jurisdictionOfIncorporationLocalityName (OID 1.3.6.1.4.1.311.60.2.1.1) ASN.1 - X520LocalityName as specified in RFC 3280
State or province (if any)	If required	jurisdictionOfIncorporationStateOrProvinceName (OID 1.3.6.1.4.1.311.60.2.1.2) ASN.1 - X520StateOrProvinceName as specified in RFC 3280
Country	Required	jurisdictionOfIncorporationCountryName (OID 1.3.6.1.4.1.311.60.2.1.3) ASN.1 - X520countryName as specified in RFC 3280

Table 2. Jurisdiction of Incorporation or Registration Certificate Fields

These fields contain information only at and abovethe level of the Incorporating or Registration Agency – e.g., the Jurisdiction of Incorporation for an Incorporating Agency or Jurisdiction of Registration for a Registration Agency at the country level would include country information but not state or province or locality information; the Jurisdiction of Incorporation for the applicable Incorporating or Registration Agency at the state or province level would include both country and state or province information, but not iLocality; and so forth. Country information MUST be specified using the applicable ISO country code. State or province information, and Locality information (where applicable) for the Subject's Jurisdiction of Incorporation or Registration MUST be specified using the full name of the applicable jurisdiction.

(5) Registration Number

GeoTrust EV Certificates include the unique Registration Number assigned to the Subject by the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration (for Private Organization Subjects only) in the serialNumber field (OID 2.5.4.5), unless the jurisdiction does not assign a unique registration number, in which case the field will include the date of incorporation.

For Government Entities that do not have a Registration Number or readily verifiable date of creation,VeriSign enters appropriate language to indicate that the Subject is a Government Entity.

(6) Physical Address of Place of Business

GeoTrust EV certificates will include an address of a verified physical location of the Subject's Place of Business, in terms of the table below.

Address Part	Required/Optional	Certificate Field
Number & street	Optional	streetAddress (OID 2.5.4.9)
City or Town	Required	localityName (OID 2.5.4.7)
State or province (if any)	Required	stateOrProvinceName (OID 2.5.4.8)
Country	Required	countryName (OID 2.5.4.6)
Postal code (optional)	Optional	postalCode (OID 2.5.4.17)

Table 3. Physical address of Place of Business Certificate Fields

7. EV Certificate Policy Identification Requirements

(a) EV Subscriber Certificates

Each EV Certificate issued by GeoTrust to a Subscriber will include GeoTrust's EV OID in the certificate's certificatePolicies extension. GeoTrust's EV OID used for this purpose is 1.3.6.1.4.1.14370.1.6. This is the only GeoTrust EV certificate that contains this special GeoTrust EV OID since GeoTrust owns all CAs in the hierarchy.

(b) EV On-line Subordinate CA Certificate

The GeoTrust Extended Validation SSL CA contains the special anyPolicy OID (2.5.29.32.0) in the certificatePolicies extension.

(c) EV Off-line Subordinate CA Certificate

The GeoTrust Extended Validation SSL CA contains the special anyPolicy OID (2.5.29.32.0) in the certificatePolicies extension.

(d) Root CA Certificates

There are two GeoTrust EV Root certificates.
1 – The off-line GeoTrust Extended Validation SSL CA will be signed by the Equifax Secure Certification Authority Root certificate. This Root CA does not contain the certificatePolicies or extendedKeyUsage fields.
2 – The On-line Extended Validation SSL CA certificate is signed by the EV off-line Subordinate CA, And it is also signed by the GeoTrust Primary Certificate Authority. The EV-Offline subordinate CA and the GeoTrust EV Root CA both have the same subject DN and use the same key which allows individuals validating the chain to chain to either of these CA certificates.

8. Maximum Validity Period

(a) For EV Certificate

The maximum validity period for an EV Certificate is twenty-seven (27) months.

(b) For Validated Data

The maximum validity period for validated data that can be used to support issuance of an EV Certificate (before revalidation is required) is as follows:

- Legal existence and identity – one (1) year;
- Assumed name – one (1) year;
- Address of Place of Business – one (1) year, but thereafter data may be refreshed by checking a Qualified Independent Information Source (QIIS), even where a site visit was originally required;
- Telephone number for Place of Business – one (1) year;
- Bank account verification – one (1) years;
- Domain name – one (1) year;
- Identity and authority of Certificate Approver – one (1) year, unless a contract is in place between GeoTrust and the Applicant that specifies a different term, in which case, the term specified in such contract will control. For example, the contract may use terms that allow the assignment of roles that are perpetual until revoked, or until agreement expires or terminated

9. Other Technical Requirements for EV Certificates

See Appendix A2 and Appendix A3 attached.

E. EV CERTIFICATE REQUEST REQUIREMENTS

10. General Requirements

(a) Documentation Requirements

Prior to the issuance of an EV Certificate, GeoTrust obtains from the Applicant the following documentation, in compliance with the requirements of these Guidelines:

- EV Certificate Request
- Subscriber Agreement
- Additional documentation required by GeoTrust to satisfy its verification obligations under the Guidelines

(b) Role Requirements

The following Applicant roles are required for the issuance of an EV Certificate

- **Certificate Requester** – A Certificate Requester is a natural person who is employed and authorized by the Applicant, or an authorized agent who has express authority to represent the Applicant or a third party (such as an ISP or hosting company) that completes and submits an EV Certificate Request on behalf of the Applicant.

- **Certificate Approver** – The EV Certificate Request MUST be approved by an authorized Certificate Approver. A Certificate Approver is a natural person who is employed by the Applicant, or an authorized agent who has express authority to represent the Applicant to (i) act as a Certificate Requester and to authorize other employees or third parties to act as a Certificate Requester, and (ii) to approve EV Certificate Requests submitted by other Certificate Requesters.

A Certificate Approver is the same individual as the Contract Signer for GeoTrust EV Certificates.

- **Contract Signer** – A Subscriber Agreement applicable to the requested EV Certificate MUST be signed by an authorized Contract Signer. A Contract Signer is a natural person who is employed by the Applicant, or an authorized agent who has express authority to represent the Applicant who has authority on behalf of the Applicant to sign Subscriber Agreements on behalf of the Applicant.

  A Contract Signer is the same individual as the Certificate Approver for GeoTrust EV Certificates.

  One person MAY be authorized by the Applicant to fill one, two, or all three of these roles, provided that in all cases the Certificate Approver and Contract Signer must be an employee of Applicant. An Applicant MAY also authorize more than one person to fill each of these roles.

11. EV Certificate Request Requirements

(a) General

Prior to the issuance of an EV Certificate, GeoTrust obtains from the Applicant (via a Certificate Requester authorized to act on Applicant's behalf) a properly completed and signed EV Certificate Request that complies with the Guidelines.

(b) Request and Certification

The EV Certificate Request contains a request from or on behalf of the Applicant for the issuance of an EV Certificate, and a certification by or on behalf of the Applicant that all of the information contained therein is true and correct**.**

(c) Information Requirements

The EV Certificate Request MAY include all factual information about the Applicant to be included in the EV Certificate, and such additional information as is necessary for GeoTrust to comply with the Guidelines and GeoTrust's own policies. In cases where the EV Certificate Request does not contain all necessary information about the Applicant, GeoTrust MUST obtain the remaining information from either the Certificate Approver or Contract Signer, or, having obtained it from a reliable source, confirm it with the Certificate Approver or Contract Signer before it can process the EV Certificate request.

Before issuing an EV Certificate, GeoTrust must obtain the following information:

- Organization Name: Applicant's formal legal organization name to be included in EV Certificate, as recorded with the Incorporating Agency in Applicant's Jurisdiction of Incorporation or Registration (for Private Organizations), or as specified in the law of the political subdivision in which the Government Entity operates (for Government Entities), or as registered with the government business Registration Agency (for Business Entities);

;

- Assumed Name (Optional): Applicant's assumed name (e.g., d/b/a name) to be included in the EV Certificate, as recorded in the jurisdiction of Applicant's Place of Business, if applicable;
- Domain Name: Applicant's fully qualified domain name to be included in the EV Certificate;

- Jurisdiction of Incorporation or Registration: Applicant's Jurisdiction of Incorporation or Registration to be included in EV Certificate, and consisting of:

    (a) City or town (if any),
    (b) State or province (if any), and
    (c) Country.

- Incorporating or Registration Agency: The name of the Applicant's Incorporating or Registration Agency;
- Registration Number: The unique registration number assigned to Applicant by the Incorporating or Registration Agency in Applicant's Jurisdiction of Incorporation or Registration and to be included in EV Certificate (for Private Organization Applicants only).
- Applicant Address: The address of Applicant's Place of Business, including –

    (a) Building number and street,
    (b) City or town,
    (c) State or province (if any),
    (d) Country,
    (e) Postal code (zip code), and
    (f) Main telephone number.

- Certificate Approver: Name and contact information of the Certificate Approver submitting and signing, or that has authorized the Certificate Requester to submit and sign, the EV Certificate Application on behalf of the Applicant; and
- Certificate Requester: Name and contact information of the Certificate Requester submitting the EV Certificate Request on behalf of the Applicant, if other than the Certificate Approver.

12. Subscriber Agreement Requirements

(a) General

Prior to the issuance of the EV Certificate, GeoTrust obtains the Applicant's agreement to a legally enforceable Subscriber Agreement for the express benefit of Relying Parties and Application Software Vendors. The Subscriber Agreement must be signed by an authorized Contract Signer acting on behalf of the Applicant, and must apply to the EV Certificate to be issued pursuant to the EV Certificate Request. A separate Subscriber Agreement may be used for each EV Certificate Request for retail certificates, or a single Subscriber Agreement may be used to cover multiple future EV Certificate Requests and resulting EV Certificates.

(b) Agreement Requirements

The Applicant's agreement to the Subscriber Agreement shall, at a minimum, specifically name both the Applicant and the individual Contract Signer signing the Agreement on the Applicant's behalf. The Subscriber Agreement shall contain, among other things, provisions imposing on the Applicant the following obligations and warranties:

- Accuracy of Information: An obligation and warranty to provide accurate and complete information at all times to GeoTrust, both in the EV Certificate Request and as otherwise requested by GeoTrust in connection with the issuance of the EV Certificate(s) to be supplied by GeoTrust;

- Protection of Private Key: An obligation and warranty by the subscriber or a subcontractor (e.g. hosting provider) to take all reasonable measures necessary to maintain sole control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested EV

Certificate(s) (and any associated access information or device – e.g., password or token);

- Acceptance of EV Certificate: An obligation and warranty that it will not install and use the EV Certificate(s) until it has reviewed and verified the accuracy of the data in each EV Certificate;

- Use of EV Certificate: An obligation and warranty to install the EV Certificate only on the server accessible at the domain name listed on the EV Certificate, and to use the EV Certificate solely in compliance with all applicable laws, solely for authorized company business, and solely in accordance with the Subscriber Agreement;

- Reporting and Revocation Upon Compromise: An obligation and warranty to promptly cease using an EV Certificate and its associated Private Key, and promptly request GeoTrust to revoke the EV Certificate, in the event that: (a) any information in the EV Certificate is or becomes incorrect or inaccurate, or (b) there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key listed in the EV Certificate;

- Termination of Use of EV Certificate. An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key listed in an EV Certificate upon expiration or revocation of that EV Certificate.

F. INFORMATION VERIFICATION REQUIREMENTS

13. General Overview

This part of GeoTrust's procedures for issuing EV Certificates sets forth the verification requirements required in the Guidelines and the procedures used by GeoTrust to satisfy the requirements.

Before issuing an EV Certificate, GeoTrust ensures that all Subject organization information in the EV Certificate conforms to the requirements of, and has been verified in accordance with, the Guidelines and matches the information confirmed and documented by GeoTrust pursuant to its verification processes.

14. Verification of Applicant's Legal Existence and Identity

To verify Applicant's legal existence and identity, GeoTrust verifies that the Applicant is a legally recognized entity, in existence and validly formed (e.g., incorporated) directly with the Incorporating or Registration Agency in Applicant's Jurisdiction of Incorporation or Registration, and designated on the records of the Incorporating or Registration Agency by labels such as "active," "valid," "current," or the equivalent. Where no such designation is available, GeoTrust will confirm the Applicant is active before approving the Applicant.

GeoTrust verifies that the Applicant's formal legal name as recorded with the Incorporating or Registration Agency in Applicant's Jurisdiction of Incorporation or Registration matches Applicant's name in the EV Certificate Request.

GeoTrust obtains and records the specific unique Registration Number assigned to Applicant by the Incorporating or Registration Agency in the Applicant's Jurisdiction of Incorporation or Registration.
GeoTrust will also obtain and record the identity and address of the Applicant's Registered Agent or Registered Office (as applicable) in the Applicant's Jurisdiction of Incorporation or Registration.

To verify a Business Entity's legal existence and identity GeoTrust verifies that the Entity is engaged in business under the name submitted by Applicant in the Application. GeoTrust verifies that the Applicant's formal legal name as recognized by the Registration Authority in Applicant's Jurisdiction of Registration matches Applicant's name in the EV Certificate Request. GeoTrust records the specific unique Registration Number assigned to Applicant by the Registration Agency in Applicant's Jurisdiction of Registration. Where the Registration Agency does not assign a Registration Number, the Applicant's date of Registration will be recorded. In addition, the identity of a Principal Individual associated with the Business Entity is verified in accordance with Section 14(b)(4) of the EV Guidelines.

15. Verification of Applicant's Legal Existence and Identity – Assumed Name

If, in addition to the Applicant's formal legal name as recorded with the Incorporating or Registration Agency in Applicant's Jurisdiction of Incorporation or Registration, Applicant's identity as asserted in the EV Certificate is to contain any assumed name or "d/b/a" name under which Applicant conducts business, GeoTrust will verify, through use of a Qualified Government Information Source (QGIS) operated by or on behalf of such government agency, or by direct contact with such government agency, that: (i) the Applicant has registered its use of the assumed name or "d/b/a" name with the appropriate state, or local government agency for such filings in the jurisdiction of its Place of Business (as verified in accordance with the Guidelines), and (ii) that such filing continues to be valid.

Alternatively, GeoTrust may verify the assumed name through use of a QIIS provided that the QIIS has verified the assumed name with the appropriate government agency, or by relying on a Verified Legal Opinion, or a Verified Accountant Letter that indicates the assumed name under which Applicant conducts business, the government agency such assumed name is registered with, and that such filing continues to be valid.

16. Verification of Applicant's Physical Existence

(a) Address of Applicant's Place of Business

To verify Applicant's physical existence and business presence, GeoTrust verifies that the physical address provided by Applicant is an address where Applicant conducts business operations (e.g., not a mail drop or P.O. Box), and is the address of Applicant's Place of Business.

For other entities, in the absence of a Verified Legal Opinion, GeoTrust may verify the address independently following the below procedure.

(A) For Applicants whose Place of Business is in the same country as the Applicant's Jurisdiction of Incorporation or Registration:

(1) For Applicants listed at the same Place of Business address in the current version of at least one (1) QIIS, or a Qualified Governmental Tax Information Source(QGTIS), GeoTrust confirms that the Applicant's address as listed in the EV Certificate Request is a valid business address for Applicant by reference to such QIIS or QGTIS, and may rely on Applicant's representation that such address is its Place of Business;

(2) For Applicants who are not listed at the same Place of Business address in the current version of at least one (1) QIIS, or QGTIS, GeoTrust may confirm that the address provided by the Applicant in the EV Certificate Request is in fact Applicant's

business address by obtaining documentation of a site visit to the business address. When used, the site visit will be performed by a reliable individual or firm. The documentation of the site visit will:

(a) Verify that the Applicant's business is located at the exact address stated in the EV Certificate Request (e.g., via permanent signage, employee confirmation, etc.);

(b) Identify the type of facility (e.g., office in a commercial building, private residence, storefront, etc.) and whether it appears to be a permanent business location;

(c) Indicate whether there is a permanent sign (that cannot be moved) that identifies the Applicant;

(d) Indicate whether there is evidence that Applicant is conducting ongoing business activities at the site (e.g., that it is not just a mail drop, P.O. box, etc.), and

(e) Include one or more photos of (i) the exterior of the site (showing signage indicating the Applicant's name, if present, and showing the street address if possible), and (ii) the interior reception area or workspace.

(B) For Applicants whose Place of Business is not in the same country as the Applicant's Jurisdiction of Incorporation or Registration, GeoTrust requires a Verified Legal Opinion that indicates the address of Applicant's Place of Business and that business operations are conducted there.

(b) Telephone Number for Applicant's Place of Business

To further verify Applicant's physical existence and business presence, as well as to assist in confirming other verification requirements, GeoTrust verifies a telephone number that is a main phone number for Applicant's Place of Business. A listing in a Parent/Subsidiary Company's name at that address is acceptable.

GeoTrust may require a Verified Legal Opinion, or a Verified Accountant Letter attesting to the telephone number.

In the absence of a Verified Legal Opinion, GeoTrust may verify Applicant's telephone number by:

(A) Confirming the telephone number is listed as the Applicant's telephone number for the verified address of its Place of Business in records provided by the applicable phone company or alternatively in at least one (1) QIIS, or QGTIS; *or*

(B) During a site visit, the person who is conducting the site visit MUST confirm the Applicant's ,or a Parent/Subsidiary Company's, main telephone number by calling it and obtaining an affirmative response sufficient to enable a reasonable person to conclude that the Applicant is reachable by telephone at the number dialed.

For Government Entity Applicants, VeriSign may rely on the telephone number contained in the records of the QGIS in Applicant's Jurisdiction.

During the telephone verification process detailed in Section 21 below GeoTrust shall call this number and obtain an affirmative response sufficient to enable a reasonable person to conclude that the Applicant is reachable by telephone at the number dialed.

17. Verification of Applicant's Operational Existence

If the records of the Incorporating or Registration Agency indicate that the Applicant has been in existence for less than three (3) years, and the Applicant is not listed in either the current version of one (1) Qualified Independent Information Source or a Qualified Governmental Tax Information Source, GeoTrust verifies that the Applicant has the ability to engage in business.

In the absence of a Verified Legal or Accountant Opinion confirming an active current Demand Deposit Account with a regulated financial institution, GeoTrust shall verify the Applicant's operational existence by verifying the Applicant has an active current Demand Deposit Account with a regulated financial institution, by receiving authenticated documentation directly from a regulated financial institution verifying that the Applicant has an active current Demand Deposit Account with the institution.

18. Verification of Applicant's Domain Name

GeoTrust verifies the Applicant's registration of the domain name(s) to be listed in the EV Certificate satisfy the following requirements:

(1) The domain name is registered with an Internet Corporation for Assigned Names and Numbers (ICANN)-approved registrar or a registry listed by the Internet Assigned Numbers Authority (IANA);

(2) Domain registration information in the WHOIS database SHOULD be public and SHOULD show the name, physical address, and administrative contact information for the organization.

For Government Entity Applicants, GeoTrust MAY rely on the domain name listed for that entity in the records of the QGIS in Applicant's Jurisdiction to verify Domain Name.

(3) The Applicant is the registered holder of the domain name or has been granted the exclusive right to use the domain name by the registered holder of the domain name

(4) The Applicant is aware of its registration or exclusive control of the domain name;

GeoTrust performs a WHOIS inquiry on the Internet for the domain name supplied by the Applicant to verify that the Applicant is the entity to whom the domain name is registered. Where the WHOIS record indicates otherwise, GeoTrust will require the WHOIS record to be updated to reflect the Applicant as the registered holder of the domain. Confirmation that the registered owner of the domain name is a Parent/Subsidiary Company of Applicant, or a registered trading name of Applicant is sufficient to establish that Applicant is the registered owner of the domain name.

In cases where the Applicant is not the registered holder of the domain name, or domain registration information cannot be obtained from WHOIS, GeoTrust may obtain positive confirmation from the registered domain holder that the Applicant has been granted the exclusive right to use the requested Fully Qualified Domain Name (FQDN). In these circumstances, GeoTrust also verifies the Applicant's exclusive right to use the domain name using one of the following methods:

(A) Relying on a Verified Legal Opinion to the effect that the Applicant has the exclusive right to use the specified domain name in identifying itself on the Internet; or

(B) Relying on a representation from the Contract Signer, or the Certificate Approver if expressly authorized in a mutually agreed upon contract, that it controls the confirmed domain name..

In cases where the registered domain holder cannot be contacted, GeoTrust shall:

- Rely on a Verified Legal Opinion to the effect that the Applicant has the exclusive right to use the specified domain name in identifying itself on the Internet, ***and***
- Rely on a representation from the Contract Signer, or the Certificate Approver if expressly authorized in a mutually agreed upon contract, coupled with a practical demonstration by the Applicant establishing that it controls the confirmed domain name by making an agreed-upon change in information found online on a web page identified by a uniform resource identifier containing the Applicant's FQDN;

GeoTrust may verify the Applicant is aware that it has exclusive control and/or ownership of the domain name by obtaining a confirmation from Certificate Approver verifying that the Applicant is aware that it has exclusive control of the domain name.

19. Verification of Name, Title, and Authority of Contract Signer and Certificate Approver

For both the Contract Signer and the Certificate Approver, GeoTrust verifies the following:

(1) Name, Title and Agency. GeoTrust verifies the name and title of the Contract Signer and the Certificate Approver, as applicable, as well as the fact that they are agents representing the Applicant.

(2) Authorization of Contract Signer. GeoTrust verifies, through a source other than the Contract Signer, that the Contract Signer is expressly authorized by the Applicant to enter into the Subscriber Agreement (and any other relevant contractual obligations) on behalf of the Applicant, including a contract that designates one or more Certificate Approvers on behalf of Applicant ("Signing Authority").

(3) Authorization of Certificate Approver. GeoTrust verifies, through a source other than the Certificate Approver, that the Certificate Approver is expressly authorized by the Applicant to do the following, as of the date of the EV Certificate Request ("EV Authority"):

(a) Submit, and if applicable authorize a Certificate Requester to submit, the EV Certificate Request on behalf of the Applicant; and

(b) Provide, and if applicable, authorize a Certificate Requester to provide, the information requested from the Applicant by the CA for issuance of the EV Certificate; and

(c) Approve EV Certificate Requests submitted by a Certificate Requester

Where the Contract Signer and Certificate Approver are the same person then the authorization of the Contract Signer shall include authorization as Certificate Approver.

In cases where a Certificate Approver is a different person from the Contract Signer GeoTrust verifies the name, title, agency status (as appropriate) and authorization of the Certificate Approver with the authorized Contract Signer.

In the absence of a Verified Legal Opinion, GeoTrust may verify agency of the Certificate Approver and/or employment of the Contract Signer by:

(A) Contacting the Applicant's human resources department by phone or mail (at the phone number or address for Applicant's Place of Business, verified in accordance with the Guidelines) and obtaining confirmation that the Contract Signer and/or the Certificate Approver, as applicable, is an employee; or

(B) Obtaining an Independent Confirmation From Applicant verifying that the Contract Signer and/or the Certificate Approver, as applicable, is either an employee or has been otherwise been appointed as an agent of Applicant.

In the absence of a Verified Legal Opinion or a Verified Accountant Letter, GeoTrust may verify the Signing Authority of the Contract Signer by using one of the following methods:

(1) **Corporate Resolution:** The Signing Authority of the Contract Signer, and/or the EV Authority of the Certificate Approver, may be verified by reliance on a properly authenticated corporate resolution that confirms that the person has been granted such Signing Authority, provided that such resolution is (1) certified by the appropriate corporate officer (e.g., secretary), and (2) GeoTrust can reliably verify that the certification was validly signed by such person, and that such person does have the requisite authority to provide such certification.

(2) **Independent Confirmation from Applicant:** The Signing Authority of the Contract Signer, and/or the EV Authority of the Certificate Approver, may be verified by obtaining an Independent Confirmation from Applicant.

(3) **Contract between CA and Applicant:** The EV Authority of the Certificate Approver may be verified by reliance on a contract between GeoTrust and the Applicant that designates the Certificate Approver with such EV Authority, provided the contract is signed by the Contract Signer and provided that the agency and Signing Authority of the Contract Signer has been verified.

(4) **Pre-Authorized Certificate Approver.** Where GeoTrust and the Applicant contemplate the submission of multiple future EV Certificate Requests and GeoTrust has:
- Verified the name and title of the Contract Signer and that he/she is an employee or agent of the Applicant, and
- Verified the Signing Authority of such Contract Signer in accordance with one of the procedures in this Section 19;

The Applicant may agree in writing, signed by the Contract Signer on behalf of the Applicant, to expressly authorize one or more designated Certificate Approver(s) to exercise EV Authority with respect to each future EV Certificate Application submitted on behalf of the Applicant and properly authenticated as originating with, or otherwise being approved by, such Certificate Approver(s).

In these circumstances the Applicant shall be obligated under the Subscriber Agreement for all EV Certificates issued at the request of, or approved by, such Certificate Approver(s) until such EV Authority is revoked, and MUST include mutually agreed-upon provisions for (i) authenticating the Certificate Approver when EV Certificate Requests are approved, (ii) periodic re-confirmation of the EV Authority of the Certificate Approver, (iii) secure procedure by which the Applicant can notify GeoTrust that the EV Authority of any such Certificate Approver is revoked, and (iv) such other appropriate precautions as are reasonably necessary.

20. Verification of Signature on Subscriber Agreement and EV Certificate Requests

The Subscriber Agreement for each EV Certificate Request MUST be signed by an authorized Contract Signer on behalf of the Applicant. If the Certificate Requester is not also an authorized Certificate Approver, or an Authorized Contract Signer, an authorized Certificate Approver or Contract Signer MUST independently approve the EV Certificate Request. In all cases, the signature MUST be a legally valid and enforceable seal or handwritten signature (for a paper Subscriber Agreement and/or EV Certificate Request), or a legally valid and enforceable electronic signature (for an electronic Subscriber Agreement and/or EV Certificate Request), that binds the Applicant to the terms of each respective document.

(a) Verification Requirements

GeoTrust authenticates the signature of the Contract Signer on the Subscriber Agreement on each request by contacting the Contract Signer directly using a verified telephone number for the Applicant, and asking to speak to the Contract Signer, followed by a response from someone who identifies themselves as such person confirming that he/she did sign the applicable document on behalf of the Applicant or by using a manner that makes it reasonably certain that the person named as the signer in the applicable document is, in fact, the person who signed the document on behalf of the Applicant.

In the absence of a telephone call as described above, GeoTrust may use one of the alternative methods of authenticating the signature of the Contract Signer:

(1) A letter mailed to the Applicant's or Registered Agent's address as verified through independent means in accordance with the Guidelines, c/o of the Certificate Requester or Contract Signer, as applicable, followed by a phone or mail response from someone who identifies themselves as such person confirming that he/she did sign the applicable document on behalf of the Applicant.

(2) Use of a signature process that establishes the name and title of the signer in a secure manner, such as through use of an appropriately secure login process that identifies the signer before signing, or through use of a digital signature made with reference to an appropriately verified certificate.

(3) Notarization by a notary, provided that GeoTrust independently verifies that such notary is a legally qualified notary in the jurisdiction of the Certificate Requester or Contract Signer;

21. Verification of Approval of EV Certificate Request

Before GeoTrust may issue the requested EV Certificate, GeoTrust verifies that an authorized Certificate Approver reviewed and approved the EV Certificate Request. GeoTrust verifies this by contacting the Certificate Approver by phone or mail (at a verified phone number or address) and obtaining oral or written confirmation that the Certificate Approver has reviewed and approved the EV Certificate Request.

22. Verification of Certain Information Sources

(a) Verified Legal Opinion

(1) Verification Requirements. Before relying on any legal opinion, GeoTrust verifies that such legal opinion meets the following requirements ("Verified Legal Opinion"):

(A) Status of Author. GeoTrust verifies that the legal opinion is authored by a legal practitioner retained by and representing the Applicant (or an in-house legal practitioner employed by the Applicant) ("Legal Practitioner") who is either:

(i) A lawyer (or solicitor, barrister, advocate, or equivalent) licensed to practice law in the Applicant's Jurisdiction of Incorporation or Registration or any jurisdiction where the Applicant maintains an office or physical facility. GeoTrust verifies the professional status of the author of the legal opinion by directly contacting the authority responsible for registering or licensing such Legal Practitioner(s) in the applicable jurisdiction; or

(ii) A notary that is a member of the International Union of Latin Notaries, and is licensed to practice in the country of Applicant's Jurisdiction of Incorporation or Registration or any jurisdiction where the Applicant maintains an office or physical facility (and that such jurisdiction recognizes the role of the Latin Notary).

(B) Basis of Opinion. GeoTrust verifies that the Legal Practitioner is acting on behalf of the Applicant and that the conclusions of the Verified Legal Opinion are based on the Legal Practitioner's stated familiarity with the relevant facts and the exercise of the Legal Practitioner's professional judgment and expertise.

(C) Authenticity. GeoTrust confirms the authenticity of the Verified Legal Opinion by calling or sending a copy of the legal opinion back to the Legal Practitioner at the address, phone number, facsimile, or (if available) e-mail address for the Legal Practitioner listed with the authority responsible for registering or licensing such Legal Practitioner and obtain confirmation from the Legal Practitioner or the Legal Practitioner's assistant that the legal opinion is authentic. In circumstances where the opinion is digitally signed, in a manner that confirms the authenticity of the document and the identity of the signer, as verified by GeoTrust in Section 22(b)(2)(A), no further verification of authenticity is required.

(b) Verified Accountant Opinion Letter

(1) Verification Requirements. Before relying on any accountant letter submitted GeoTrust verifies that such accountant letter meets the following requirements ("Verified Accountant Letter"):

(A) Status of Author. GeoTrust shall by directly contact the authority responsible for registering or licensing such Accounting Practitioner(s) in the applicable jurisdiction to establish that the accountant letter is authored by an independent professional accountant retained by and representing the Applicant (or an in-house professional accountant employed by the Applicant) ("Accounting Practitioner") who is a certified public accountant, chartered accountant, or equivalent licensed by a full member of the International Federation of Accountants (IFAC) to practice accounting in the country of the Applicant's Jurisdiction of Incorporation or Registration or any jurisdiction where the Applicant maintains an office or physical facility;

(B) Basis of Opinion. The Accounting Practitioner is acting on behalf of the Applicant and that the conclusions of the Verified Accountant Letter are based on the Accounting Practitioner's stated familiarity with the relevant facts and the exercise of the Accounting Practitioner's professional judgment and expertise.

(C) Authenticity. To confirm the authenticity of the accountant's opinion, GeoTrust will call or send a copy of the accountant letter back to the Accounting Practitioner at the address, phone number, facsimile, or (if available) e-mail address for the Accounting Practitioner listed with the authority responsible for registering or licensing such Accounting Practitioner and obtain confirmation from the Accounting Practitioner or the Accounting Practitioner's assistant that the

accountant letter is authentic. In circumstances where the opinion is digitally signed, in a manner that confirms the authenticity of the document and the identity of the signer, as verified by GeoTrust in Section 22(b)(2)(A), no further verification of authenticity is required.

(c) Face-to-face Validation of Principal Individual

Before relying on any face-to-face vetting documents GeoTrust verifies that the Third-Party Validator meets the following requirements:

(A) Qualification of Third-Party Validator. GeoTrust independently verifies that the Third-Party Validator is a legally-qualified Latin Notary or Notary (or legal equivalent in Applicant's jurisdiction), Lawyer, or Accountant in the jurisdiction of the individual's residency, by directly contacting the authority responsible for registering or licensing such Third-Party Validators in the applicable jurisdiction.

(B) Document chain of custody. GeoTrust verifies that that the Third-Party Validator viewed the Vetting Documents in a face-to-face meeting with the individual being validated. The Third party validator must attest that they obtained the Vetting Documents submitted to the CA for the individual during a face-to-face meeting with the individual.

(C) If the Third-Party Validator is not a Latin Notary, then GeoTrust confirms the authenticity of the attestation and vetting documents, by making a telephone call to the Third-Party Validator and obtaining confirmation from them or their assistant that they performed the face-to-face validation. GeoTrust may rely upon self-reported information obtained from the Third-Party Validator for the sole purpose of performing this verification process. In circumstances where the attestation is digitally signed, in a manner that confirms the authenticity of the documents,and the identity of the signer as verified by GeoTrust in Section 22(c)(2)(A), no further verification of authenticity is required.

(d) Independent Confirmation from Applicant

An "Independent Confirmation From Applicant" is a confirmation of a particular fact (e.g., knowledge of its exclusive control of a domain name, confirmation of the employee or agency status of a Contract Signer or Certificate Approver, confirmation of the EV Authority of a Certificate Approver, etc.) that is:

(i) Received by GeoTrust from a person employed by the Applicant (other than the person who is the subject of the inquiry) that has the appropriate authority to confirm such a fact ("Confirming Person"), and who represents that he/she has confirmed such fact;

(ii) Received by GeoTrust in a manner that authenticates and verifies the source of the confirmation; and

(iii) Binding on the Applicant.

An Independent Confirmation From Applicant may be obtained via the following procedure:

(1) Confirmation Request: GeoTrust will initiate an appropriate out-of-band communication requesting verification or confirmation of the particular fact in issue ("Confirmation Request") as follows:

(A) Addressee: The Confirmation Request MUST be directed to:

(i) A position within Applicant's organization that qualifies as a Confirming Person (e.g., Secretary, President, CEO, CFO, COO, CIO, CSO, Director,

etc.) and is identified by name and title in a current Qualified Government Information Source (e.g., an SEC filing) or a QIIS, a Verified Legal Opinion, or a Verified Accountant Letter; or

(ii) Applicant's Registered Agent or Registered Office in the Jurisdiction of Incorporation or Registration as listed in the official records of the Incorporating or Registration Agency, with instructions that it be forwarded to an appropriate Confirming Person.

(iii) A named individual verified to be in the direct line of management above the Contract Signer or Certificate Approver by contacting Applicant's Human Resources Department by phone or mail (at the verified phone number or address for Applicant's Place of Business)

(B) Means of Communication: The Confirmation Request MUST be directed to the Confirming Person in a manner reasonably likely to reach such person. The following options are acceptable:

(i) By paper mail, addressed to the Confirming Person at:

(a) The address of Applicant's Place of Business as verified by GeoTrust in accordance with these procedures; or

(b) The business address for such Confirming Person specified in a current government-operated Qualified Government Information Source (e.g., an SEC filing), a QIIS, a Qualified Government Tax Information Source, a Verified Legal Opinion, or a Verified Accountant Letter; or

(c) The address of Applicant's Registered Agent or Registered Office listed in the official records of the Jurisdiction of Incorporation or Registration; or

(ii) By e-mail addressed to the Confirming Person at the business e-mail address for such person listed in a current Qualified Government Information Source or a QIIS, a Verified Legal Opinion, or a Verified Accountant' Letter; or

(iii) By telephone call to the Confirming Person, where such person is contacted by calling the main phone number of Applicant's Place of Business (verified in accordance with the Guidelines) and asking to speak to such person, and a person taking the call identifies himself as such person; or

(iv) By facsimile to the Confirming Person at the Place of Business. The facsimile number must be listed in a current Qualified Government Information Source or a QIIS, a Verified Legal Opinion, or a Verified Accountant Letter. The cover page must be clearly addressed to the Confirming Person.

(2) Confirmation Response: GeoTrust must receive a response to the Confirmation Request from a Confirming Person that confirms the particular fact in issue. Such response may be provided by telephone, by e-mail, or by paper mail, so long as GeoTrust can reliably verify that it was provided by a Confirming Person in response to the Confirmation Request.

(e) Qualified Independent Information Sources (QIIS)

Commercial Information Sources used by GeoTrust for verifying EV certificate application information meet the databases requirements required by the Guidelines.

(f) Qualified Government Information Source (QGIS)

Government Information Sources used by GeoTrust for verifying EV certificate application information meet the databases requirements required by the Guidelines. GeoTrust may use

third-party vendors to obtain the information from the Government Entity provided that the third party obtains the information directly from the Government Entity.

(g) Qualified Government Tax Information Source (QGTIS). A Qualified Governmental Information Source that specifically contains tax information relating to Private Organizations, Business Entities or Individuals (e.g. the I.R.S. in the United States).

23. Other Verification Requirements

(a) High Risk Status

GeoTrust takes reasonable steps to identify Applicants that are likely to be at a high risk applications e.g., if they may possibly be targeted for fraudulent attacks ("High Risk Applicants"), and conduct such additional verification activity and take such additional precautions as are reasonably necessary to ensure that such Applicants are properly verified under the Guidelines.

GeoTrust maintains an internal database that includes previously revoked SSL certificates, including EV Certificates and previously rejected EV Certificate Requests, due to suspected phishing or other fraudulent usage. This information is used to flag suspicious new EV Certificate Requests. If an Applicant is flagged as a High Risk Applicant, GeoTrust performs reasonably appropriate additional authentication and verification to be certain beyond reasonable doubt that the Applicant and the target in question are the same entity.

(b) Denied Lists and Other Legal Black Lists

GeoTrust will not issue any EV Certificate to the Applicant, without first taking appropriate steps for obtaining clearance from the relevant government agency, if either the Applicant, the Contract Signer, or Certificate Approver or if the Applicant's Jurisdiction of Incorporation or Registration or Place of Business is:

(a) Identified on any government denied list, list of prohibited persons, or other list that prohibits doing business with such organization or person under the laws of the country of GeoTrust's jurisdiction(s) of operation; and

(b) Has its Jurisdiction of Incorporation or Registration or Place of Business in any country with which the laws of GeoTrust's jurisdiction prohibit doing business

GeoTrust also takes reasonable steps to verify with the following lists and regulations:

(A) GeoTrust will take reasonable steps to verify with the following US Government Denied lists and regulations:
(B) BIS Denied Persons List
(C) BIS Denied Entities List
(D) US Treasury Department List of Specially Designated Nationals and Blocked Persons
(E) US Government export regulations

24. Final Cross-Correlation and Due Diligence

GeoTrust requires that after all of the verification processes and procedures are completed, an EV verification specialist who is not responsible for the collection of information reviews that GeoTrust has performed all verification steps. That person may also be responsible for placing the final verification call to the Contract Signer and, if successful, issue the certificate.

25. Certificate Renewal Verification Requirements.

Before renewing an EV Certificate, GeoTrust performs all authentication and verification tasks required by the Guidelines and this procedure to ensure that the renewal request is properly

authorized by the Applicant and that the information displayed in the EV Certificate is still accurate and valid.

G. CERTIFICATE STATUS CHECKING AND REVOCATION ISSUES

26. EV Certificate Status Checking.

GeoTrust maintains an online 24/7 Repository mechanism whereby Internet browsers can automatically check online the current status of all certificates.

(1) For EV Certificates:

(A) CRLs are be updated and reissued at least every seven (7) days, and the nextUpdate field value SHALL NOT be more than ten (10) days; or

(B) OCSP. If used, GeoTrust's Online Certificate Status Protocol (OCSP) is updated at least every four (4) days, and with a maximum expiration time of ten (10) days.

(2) For GeoTrust's subordinate CA Certificate for EV:

(A) CRLs. Are updated and reissued at least every twelve (12) months, and with a maximum expiration time of twelve (12) months; or

(B) OCSP. If used, GeoTrust's OCSP for CA Certificates for EV will be updated at least every twelve (12) months, and with a maximum expiration time of twelve (12) months.

GeoTrust operates and maintain its CRL and/or OCSP capability with resources sufficient to provide a commercially reasonable response time for the number of queries generated by all of the EV Certificates issued by it.

Revocation entries on a CRL or OCSP are not removed until after the expiration date of the revoked EV Certificate.

27. EV Certificate Revocation.

In addition to any revocation circumstances listed in Section (III) I (1) of this CPS, GeoTrust will revoke an EV Certificate it has issued upon the occurrence of any of the following events:

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

(5) GeoTrust receives notice or otherwise become 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) The CA receives notice or otherwise become aware of a material change in the information contained in the EV Certificate;

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

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

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

(10) GeoTrust's right to issue EV Certificates under the Guidelines expires or is revoked or terminated [*unless GeoTrust makes arrangements to continue maintaining the CRL/OCSP Repository*];

(11) GeoTrust's Private Key for its EV issuing CA Certificate has been compromised;

(13) GeoTrust 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 GeoTrust's jurisdiction of operation.

28. EV Certificate Problem Reporting and Response Capability.

GeoTrust provides Subscribers, Relying Parties, Application Software Vendors, and other third parties with an online form to report complaints or suspected Private Key compromise, EV Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to EV Certificates ("Certificate Problem Reports"), and a 24x7 capability to accept and acknowledge such Reports, at: http://www.geotrust.com/ev.

GeoTrust will begin investigation of all Certificate Problem Reports within twenty-four (24) hours and decide whether revocation or other appropriate action is warranted based on at least the following criteria:

(i) The nature of the alleged problem;
(ii) Number of Certificate Problem Reports received about a particular EV Certificate or website;
(iii) The identity of the complainants (for example, complaints from a law enforcement official that a web site is engaged in illegal activities have more weight than a complaint from a consumer alleging they never received the goods they ordered); and
(iv) Relevant legislation in force.

GeoTrust takes reasonable steps to provide continuous 24/7 ability to internally respond to any high priority Certificate Problem Report, and where appropriate, forward such complaints to law enforcement and/or revoke an EV Certificate that is the subject of such a complaint.

H. EMPLOYEE AND THIRD PARTY ISSUES

29. Trustworthiness and Competence

(a) Identity and Background Verification.

Any person employed by GeoTrust for engagement in the EV Certificate process, whether as an employee, agent, or an independent contractor, is subject to following additional procedures:

Verify the identity of such person. Verification the identity of such person should be performed through:

(A) The personal (physical) presence of such person before trusted persons including notary publics, or persons who perform human resource or security functions, and

(B) The verification of well-recognized forms of government-issued photo identification (e.g., passports and/or driver's licenses); and

Verify the trustworthiness of such person. Verification of trustworthiness shall include background checks which address at least the following *[or their equivalent]*:

(A) Confirmation of previous employment,
(B) Check of professional references;
(C) Confirmation of the highest or most relevant educational degree obtained,
(D) Search of criminal records (local, state or provincial, and national) where allowed by the jurisdiction where the person will be employed, and

In the case of employees of GeoTrust at the time of the adoption of the Guidelines whose identity and background has not previously been verified as set forth above, GeoTrust shall conduct such verification within three (3) months of the date of adoption of the Guidelines.

(b) Training and Skills Level.

GeoTrust will provide all personnel performing validation duties ("Validation Specialists") with skills training that covers basic Public Key Infrastructure (PKI) knowledge, authentication and verification policies and procedures, common threats to the validation process including phishing and other social engineering tactics, and the Guidelines.

GeoTrust will maintain records of such training and ensure that personnel entrusted with Validation Specialist duties meet a minimum skills requirement that enable them to perform such duties satisfactorily

Validation Specialists engaged in EV Certificate issuance must maintain adequate skill levels in order to have issuance privilege, consistent with GeoTrust's training and performance programs.

GeoTrust will ensure that its Validation Specialists qualify for each skill level required by the corresponding validation task before granting privilege to perform said task.

GeoTrust will require all Validation Specialists to pass an internal examination on the EV Certificate validation criteria outlined in the Guidelines.

(c) Separation of Duties.

GeoTrust will enforce rigorous control procedures for the separation of validation duties to ensure that no one person can single-handedly validate and authorize the issuance of an EV Certificate. The final due diligence steps as outlined in Section 24 of this Appendix may be performed by one of the persons. For example, one Validation Specialist reviews and verifies all Applicant information and a second Validation Specialist approves issuance of the EV Certificate.

Such controls will be auditable.

30. Delegation of Functions to Registration Authorities and Subcontractors

GeoTrust may delegate the performance of all or any part of a requirement of these procedures and the Guidelines to a registration agent (RA) or subcontractor, except for the performance of the final cross-correlation and due diligence requirements of Section 24 of the Guidelines.

I. DATA AND RECORD ISSUES

31. Documentation and Audit Trail Requirements

(a) GeoTrust records every action taken to process an EV Certificate Request and to issue an EV Certificate, including all information generated or received in connection with an EV Certificate Request, and every action taken to process the Request, including time, date, and personnel involved in the action. These records are available as auditable proof of the CA's practices. This also applies to all registration agents (RAs) and subcontractors as well.

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

(i) CA key lifecycle management events, including:
- (a) Key generation, backup, storage, recovery, archival, and destruction; and
- (b) Cryptographic device lifecycle management events

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

(iii) Security events, including:
- (a) Successful and unsuccessful PKI system access attempts;
- (b) PKI and security system actions performed;
- (c) Security profile changes;
- (d) System crashes, hardware failures, and other anomalies;
- (e) Firewall and router activities; and
- (f) Entries to and exits from CA facility

(iv) Log entries will include the following elements:
- (a) Date and time of entry;
- (b) Identity of the persona and entity making the journal entry; and
- (ç Description of entry

32. Document Retention

(a) Audit Log Retention

Audit logs for EV Certificates are made available to independent auditors upon request. Audit logs are retained for at least seven (7) years.

(b) Retention of Documentation

GeoTrust retains all documentation relating to all EV Certificate Requests and verification thereof, and all EV Certificates and revocation thereof, for at least seven (7) years after any EV Certificate based on that documentation ceases to be valid. GeoTrust maintains current an internal database of all previously revoked EV Certificates and previously rejected EV Certificate Requests due to suspected phishing or other fraudulent usage or concerns.

33. Reuse and Updating Information and Documentation

(a) Use of Documentation to Support Multiple EV Certificates

GeoTrust may issue multiple EV Certificates listing the same Subject and based on a single EV Certificate Request, subject to the aging and updating requirement in (b) below.

(b) Use of Pre-Existing Information or Documentation

(1) Each EV Certificate issued by GeoTrust will be supported by a valid current EV Certificate Request and a Subscriber Agreement signed by the Applicant Representative on behalf of the Applicant.

(2) The age of information used by GeoTrust to verify such an EV Certificate Request will not exceed the Maximum Validity Period for such information set forth in these procedures and the Guidelines, based on the earlier of the date the information was obtained (e.g., the date of a confirmation phone call) or the date the information was last updated by the source (e.g., if an online database was accessed by GeoTrust on July 1, but contained data last updated by the vendor on February 1, then the date of information would be considered to be February 1).

(3) In the case of outdated information, GeoTrust repeats the verification processes required in the Guidelines.

34. Data Security

Sections IV and V of the GeoTrust CPS describe GeoTrust's Security Controls.

J. COMPLIANCE

35. Audit Requirements

(a) Pre-Issuance Readiness Audit

Before issuing EV Certificates, GeoTrust shall successfully complete a point-in-time readiness assessment audit against the WebTrust EV Program, or a point-in-time readiness assessment audit against equivalent audit procedures approved by the CA/Browser Forum.

(b) Regular Self Audits

During the period in which it issues EV Certificates, GeoTrust will control its service quality by performing ongoing self audits against a randomly selected sample of at least three percent (3%) of the EV Certificates it has issued in the period beginning immediately after the last sample was taken.

(c) Annual Independent Audit

GeoTrust undergoes an annual (i) WebTrust Program for CAs audit and (ii) WebTrust EV Program audit, or an equivalent for both (i) and (ii) as approved by the CA/Browser Forum. Such audits cover all CA obligations under the Guidelines regardless of whether they are performed directly by GeoTrust or delegated to an RA or subcontractor.

The audit report is made publicly available by GeoTrust.

(d) Auditor Qualifications

All audits required under the Guidelines will be performed by a Qualified Auditor. A Qualified Auditor shall:

(1) Be an independent public accounting firm that has proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function and be currently licensed to perform WebTrust for CA audits and WebTrust EV Program audits, or to perform such alternate equivalent audits approved by the CA/Browser Forum as will be performed; and

(2) Be a member of the American Institute of Certified Public Accountants (AICPA), or by a non-US equivalent that requires that audits be completed under defined standards that include the possession of certain skill sets, quality assurance measures such as peer review, competency testing, standards with respect to proper assignment of staff to engagements, and requirements for continuing professional education; and

(3) Maintain Professional Liability/Errors & Omissions insurance, with policy limits of at least $1 million in coverage

(e) Root Key Generation

For CA root keys generated after the release of the Guidelines, GeoTrust's Qualified Auditor may witness the root key generation ceremony in order to observe the process and the controls over the integrity and confidentiality of the CA root keys produced. The Qualified Auditor will then issue a report opining that GeoTrust, during its root key and certificate generation process:

- Documented its Root CA key generation and protection procedures in its Certificate Policy , version, date and its Certification Practices Statement, version, date (CP and CPS);
- Included appropriate detailed procedures and controls in a documented plan of procedures to be performed for the generation of the root certification authority key pair (the "Root Key Generation Script") for the Root CA;
- Maintained effective controls to provide reasonable assurance that the Root CA was generated and protected in conformity with the procedures described in its CP/CPS and with its Root Key Generation Script; and
- Performed, during the root key generation process, all the procedures required by its Root Key Generation Script.
- A video of the entire key generation ceremony will be recorded for auditing purposes.

K. OTHER CONTRACTUAL COMPLIANCE

36. Privacy/Confidentiality Issues

GeoTrust will comply with all applicable privacy laws and regulations, as well as its published privacy policy, in the collection, use and disclosure of non-public personal information as part of the EV Certificate vetting process.

37. Limitations on EV Certificate Liability

(a) CA Liability

(1) Subscribers and Relying Parties

In cases where GeoTrust has issued and managed the EV Certificate in compliance with the Guidelines and its CPS, GeoTrust shall not be liable to the EV Certificate Subscribers or Relying Parties or any other third parties for any losses suffered as a result of use or reliance on such EV Certificate. In cases where GeoTrust has not issued or managed the EV Certificate in complete compliance with the Guidelines and this CPS, GeoTrust's liability to the Subscriber for legally recognized and provable claims for losses or damages suffered as a result of the use or reliance on such EV Certificate shall not exceed$2,000. GeoTrust's liability to Relying Parties or any other third parties for legally recognized and provable claims for losses or damages suffered as a result of the use or reliance on such EV Certificate shall not exceed $2,000.

(2) Indemnification of Application Software Vendors
Notwithstanding any limitations on its liability to Subscribers and Relying Parties, GeoTrust understands and acknowledges that the Application Software Vendors who have a root certificate distribution agreement in place with GeoTrust do not assume any obligation or potential liability of GeoTrust under the Guidelines or that otherwise might exist because of the issuance or maintenance of EV Certificates or reliance thereon by Relying Parties or others. GeoTrust shall defend, indemnify, and hold harmless each Application Software Vendor for any and all claims, damages, and losses suffered by such Application Software Vendor related to an EV Certificate issued by GeoTrust, regardless of the cause of action or legal theory involved. This shall not apply, however, to any claim, damages, or loss suffered by such Application Software Vendor related to an EV Certificate issued by GeoTrust where such claim, damage, or loss was directly caused by such Application Software Vendor's software displaying as not trustworthy an EV Certificate that is still valid, or displaying as trustworthy: (1) an EV Certificate that has expired, or (2) an EV Certificate that has been revoked (but only in cases where the revocation status is currently available from GeoTrust online, and the browser software either failed to check such status or ignored an indication of revoked status).

L. DEFINITIONS

Applicant: The Private Organization or Government Entity that applies for (or seeks renewal of) an EV Certificate naming it as the Subject.

Application Software Vendor: A developer of Internet browser software or other software that displays or uses certificates and distributes root certificates, such as KDE, Microsoft Corporation, Mozilla Corporation, Opera Software ASA, and Red Hat, Inc.

Demand Deposit Account: a deposit account held at a bank or other financial institution, the funds deposited in which are payable on demand. The primary purpose of demand accounts is to facilitate cashless payments by means of check, bank draft, direct debit, electronic funds transfer, etc. Usage varies among countries, but a demand deposit account is commonly known as: a checking account, a share draft account, a current account, or a checking account.

Government Entity: A government-operated legal entity, agency, department, ministry, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).

Incorporating or Registration Agency: In the case of a Private Organization, the government agency in the Jurisdiction of Incorporation or Registration under whose authority the legal existence of the Private Organization was established (e.g., the government agency that issued the Certificate of Incorporation). In the case of a Government Entity, the entity that enacted the law, regulation, or decree establishing the legal existence of the Government Entity.

Jurisdiction of Incorporation or Registration: In the case of a Private Organization, the country and (where applicable) the state or province where the organization's legal existence was established by a filing with (or an act of) an appropriate government agency or entity (e.g., where it was incorporated). In the case of a Government Entity, the country and (where applicable) the state or province where the Entity's legal existence was created by law.

Place of Business: The location of any facility (such as a factory, retail store, warehouse, etc) where the Applicant's business is conducted.

Principal Individual)s). Individuals of a Private Organization, Government Entity or Business Entity that are either owners, partners, managing members, directors or officers, as identified by their title of employment, or an employee, contractor or agent authorized by such entity or organization to conduct business related to the request, issuance and use of EV Certificates.

Private Key: The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

Private Organization: A non-governmental legal entity (whether ownership interests are privately held or publicly traded).

Public Key: The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

Qualified Government Information Source (QGIS): 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 by law and false or misleading reporting is punishable with criminal or civil penalties

Qualified Independent Information Sources (QIIS): 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.

Registered Agent: An individual or entity that is both: (1) authorized by the Applicant to receive service of process and business communications on behalf of the Applicant; and (2) listed in the official records of the Applicant's Jurisdiction of Incorporation or Registration as acting in the role specified in (a) above.

Registered Office: The official address of a company, as recorded with the Incorporating or Registration Agency, to which official documents are sent and legal notices received.

Registration Agency. A Governmental Agency that registers business information in connection with an entity's business formation or authorization to conduct business under a license, charter or other certification. A Registration Agency MAY include, but is not limited (i) a State Department of Corporations or a Secretary of State; (ii) a licensing agency, such as a State Department of Insurance; or (iii) a chartering agency, such as a state office or department of financial regulation, banking or finance, or a federal agency such as the Comptroller of Currency (OCC) or Office of Thrift Supervision (OTC)

Regulated Financial Institution: A financial institution that is regulated, supervised, and examined by governmental, national, state or provincial, or local authorities having regulatory

authority over such financial institution based on the governmental, national, state or provincial, or local laws under which such financial institution was organized and/or licensed.

Relying Party: Any person (individual or entity) that relies on a Valid EV Certificate. A Application Software Vendor is not considered a Relying Party when software distributed by such Vendor merely displays information regarding an EV Certificate.

Subscriber / Subscribing Organization: The organization identified as the Subject in the Subject:organizationName field of an EV Certificate issued pursuant to these Guidelines, as qualified by the Jurisdiction of Incorporation or Registration information in the EV Certificate.

Subscriber Agreement: An agreement between the CA and the Subject named or to be named in an EV Certificate that specifies the right sand responsibilities of the parties, and that complies with the requirements of these Guidelines.

Subsidiary Company. A subsidiary company is defined, for EV, as a company that is wholly owned by Applicant as verified by referencing a QIIS or from financial statement supplied by a registered Chartered Professional Accountant (CPA) or equivalent outside of the USA.

Valid: An EV Certificate that has not expired and has not been revoked.

Appendix A2

Minimum Cryptographic Algorithm and Key Sizes for EV Certificates

1. Root CA Certificates

	Certificate issued on or before 31 Dec 2010	Certificate issued after 31 Dec 2010
Digest algorithm	MD5 (NOT RECOMMENDED), SHA-1	SHA-1*, SHA-256, SHA-384 or SHA-512
RSA	2048 bit (An end-entity certificate MAY, in addition, chain to an EV-enabled 1024-bit RSA root CA certificate key.)	2048
ECC	224, 233, 256 or 283	224, 233, 256 or 283

2. Subordinate CA Certificates

	Certificate issued on or before 31 Dec 2010	Certificate issued after 31 Dec 2010
Digest algorithm	SHA-1	SHA-1*, SHA-256, SHA-384 or SHA-512
RSA	1024 or 2048	2048
ECC	224, 233, 256 or 283	224, 233, 256 or 283

3. Subscriber Certificates

	Certificate issued on or before 31 Dec 2010	Certificate issued after 31 Dec 2010
Digest algorithm	SHA-1	SHA1*, SHA-256, SHA-384 or SHA-512
RSA	1024 or 2048 (Note: subscriber certificates containing a 1024 bit RSA key MUST expire on or before 31 Dec 2010)	2048
ECC	224, 233, 256 or 283	224, 233, 256 or 283

*SHA-1 should be used until SHA-256 is supported widely by browsers used by a majority of relying parties worldwide.

Appendix A3

EV Certificates Required Certificate Extensions

1. Root CA Certificate

Root certificates generated after October 2006 MUST be X.509 v3.

(a) basicConstraints

If the certificate is v3 and is created after October 2006, this extension MUST appear as a critical extension in all CA certificates that contain Public Keys used to validate digital signatures on certificates. The cA field MUST be set true. The pathLenConstraint field SHOULD NOT be present.

(b) keyUsage

If the certificate is v3 and is created after October 2006, this extension MUST be present and MUST be marked critical. Bit positions for CertSign and cRLSign MUST be set. All other bit positions SHOULD NOT be set.

All other fields and extensions set in accordance to RFC 3280.

2. Subordinate CA Certificate

(a) certificatePolicies

MUST be present and SHOULD NOT be marked critical. The set of policy identifiers MUST include the identifier for the CA's extended validation policy if the certificate is issued to a subordinate CA that is not controlled by GeoTrust.

certificatePolicies:policyIdentifier (Required)
- anyPolicy if subordinate CA is controlled by Root CA
- explicit EV policy OID(s) if subordinate CA is not controlled by Root CA

The following fields MUST be present if the Subordinate CA is not controlled by GeoTrust.

certificatePolicies:policyQualifiers:policyQualifierId
- id-qt 2 [RFC 3280]

certificatePolicies:policyQualifiers:qualifier
- URI to the Certificate Practice Statement

(b) cRLDistributionPoint

MUST be present and MUST NOT be marked critical. If present, it MUST contain the HTTP URL of the CA's CRL service.

(c) authorityInformationAccess

SHOULD be present and MUST NOT be marked critical. SHALL contain the HTTP URL of the CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1).
An HTTP accessMethod
MAY be included for the CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2).

(d) basicConstraints

This extension MUST appear as a critical extension in all CA certificates that contain Public Keys used to validate digital signatures on certificates. The CA field MUST be set true. The pathLenConstraint field MAY be present.

(e) keyUsage

This extension MUST be present and MUST be marked critical. Bit positions for CertSign and cRLSign MUST be set. All other bit positions MUST NOT be set.

All other fields and extensions set in accordance to RFC 3280.

3. Subscriber Certificate

(a) certificate Policies

MUST be present and SHOULD NOT be marked critical. The set of policyIdentifiers MUST include the identifier for GeoTrust's extended validation policy.

certificatePolicies:policyIdentifier (Required)
- o EV policy OID

certificatePolicies:policyQualifiers:policyQualifierId (Required)
- o id-qt 2 [RFC 3280]

certificatePolicies:policyQualifiers:qualifier (Required)
- o URI to the Certificate Practice Statement

(b) cRLDistributionPoint

SHOULD be present and MUST NOT be marked critical. If present, it will contain the HTTP URL of GeoTrust's CRL service. This extension MUST be present if the certificate does not specify OCSP responder locations in an authorityInformationAccess extension. See section 26(b) for details.

(c) authorityInformationAccess

SHOULD be present and MUST NOT be marked critical. SHALL contain the HTTP URL of GeoTrust's's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1). An HTTP accessMethod MAY be included for the CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2). This extension MUST be present if the certificate does not contain a cRLDistributionPoint extension. See section 26(b) for details.

(d) basicConstraints (optional)

If present, the CA field MUST be set false.

(e) keyUsage (optional)

If present, bit positions for CertSign and cRLSign MUST NOT be set.

All other fields and extensions set in accordance to RFC 3280.

Appendix A4
Country Specific Organization Name Guidelines

E-1. Japan

This set of guidelines only applies to the companies that are incorporated and registered in Japan. The ASCII character names in the O field of EV certificates can be expressed either as an assumed English name, or as a Roman legal organization name.

Assumed English Name: Verify that Applicant's formal legal name recorded either on the audited Financial Statement filed with the Financial Services Agency or on the Articles of Incorporation matches Applicant's formal legal name recorded on the Certified Copy of Register. The Articles of Incorporation must be accompanied either by a document to prove the Articles of Incorporation as authentic and current signed with the original Japanese Corporate Stamp, or by a lawyer's opinion letter.

Roman Organization Name: Verify the Romanized transliteration of Applicant's formal legal name with either QIIS or a lawyer's opinion letter.