GeoTrust

Certification Practices Statement

Version 1.1.13

Effective Date: November 7, 2013

GeoTrust, Inc
350 Ellis Street
Mountain View, CA 94043 USA
+1 650.527.8000
www.geotrust.com

GeoTrust Certification Practices Statement

Revision date: November 6, 2013

Trademark Notices

Table of Contents

1. INTRODUCTION

This document is the GeoTrust Certification Practice Statement ("CPS"). It states the practices that GeoTrust certification authorities ("CAs") employ in providing certification services that include, but are not limited to, issuing, managing, revoking, and renewing certificates.

1.1 Overview

This GeoTrust Certificate Practice Statement (the "CPS") presents the principles and procedures employed in the issuance and life cycle management of GeoTrust digital certificates. This CPS and any and all amendments thereto are incorporated by reference GeoTrust Certificates under this CPS.

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.

The GeoTrust CA conforms to the Internet Engineering Task Force (IETF) RFC 3647 for Certificate Policy and Certification Practice Statement construction. GeoTrust CAs conform to the current version of the CA/Browser Forum (CABF) requirements including:

- Guidelines for the Issuance and Management of Extended Validation (EV) Certificates,
- Guidelines for the Issuance and Management of Extended Validation (EV) Code-Signing Certificates, and,
- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates,

published at www.cabforum.org. In the event of any inconsistency between this document and those Requirement, those Requirements take precedence over this document.

At this time, Symantec's Extended Validation (EV) SSL certificates, Extended Validation (EV) Code-Signing certificates and Domain-validated (DV) and Organization-validated (OV) SSL certificates issued by GeoTrust CAs under this CPS conform with the CABF Requirements. Such DV and OV certificates are issued containing the corresponding policy identifier(s) specified in section 1.2 indicating adherence to and conformance with these requirements. GeoTrust CAs shall also assert that all Certificates issued containing these policy identifier(s) are issued and managed in conformance with the CABF Requirements.

CAs shall disclose all Cross Certificates that identify the CA as the Subject in the established trust relationship.

1.2 Document Name and Identification

This document is the GeoTrust Certification Practice Statement. The object identifier (OID) values corresponding to the GeoTrust Certificate Policy are as follows:

GeoTrust Certificate Policy for Extended Validation (EV) certificates: 1.3.6.1.4.1.14370.1.6
GeoTrust Certificate Policy certificates (non-EV): 1.3.6.1.4.1.14370.1.7

Symantec has assigned a reserved OID value for asserting conformance with the current version of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-

Trusted Certificates. This OID value is reserved for use by any brand of Symantec CA as a means of asserting compliance with these CABF Requirements and as such does not distinguish a particular brand or class of Certificate.

The Symantec Reserved Certificate Policy identifier:
Symantec/id-CABF-OVandDVvalidation: 2.16.840.1.113733.1.7.54

1.3 PKI Participants

1.3.1 Certification Authorities

The term Certification Authority (CA) is a trusted third-party entity that issues Certificates and performs all of the functions associated with issuing such Certificates under this CPS. The GeoTrust CA also issues certificates to subordinate CAs, including CAs owned by third parties. All such subordinate CAs are required to operate in conformance with this CPS.

1.3.2 Registration Authorities

A Registration Authority is an entity that performs identification and authentication of certificate applicants for end-user certificates, initiates or passes along revocation requests for certificates for end-user certificates, and approves applications for renewal or re-keying of certificates on behalf of a GeoTrust CA. GeoTrust may act as an RA for certificates it issues.

Third parties, who enter into a contractual relationship with GeoTrust, may operate their own RA and authorize the issuance of certificates by a GeoTrust CA. Third party RAs must abide by all the requirements of the GeoTrust CPS and the terms of their agreement with GeoTrust. RAs may, however implement more restrictive practices based on their internal requirements.

1.3.3 Subscribers

Subscribers include all end users (including entities) of certificates issued by a GeoTrust CA. A subscriber is the entity named as the end-user Subscriber of a certificate. End-user Subscribers may be individuals, organizations or, infrastructure components such as firewalls, routers, trusted servers or other devices used to secure communications within an Organization.

CAs are technically also subscribers of GeoTrust certificates either as a CA issuing a self signed Certificate to itself, or as a CA issued a Certificate by a superior CA. References to “end entities” and “subscribers” in this CPS, however, apply only to end-user Subscribers.

1.3.4 Relying Parties

A Relying Party is an individual or entity that acts in reliance of a certificate and/or a digital signature issued by a GeoTrust CA. A Relying Party may, or may not also be a Subscriber of GeoTrust certificates.

1.3.6 Other Participants

No Stipulation

1.4 Certificate Usage

1.4.1 Appropriate Certificate Usages

GeoTrust Certificates are X.509 Certificates with SSL Extensions, Code Signing and/or Client Authentication Extensions (as appropriate) that chain to a GeoTrust Trusted Root.

GeoTrust **SSL 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. GeoTrust may issue Wildcard Certificates, which are X.509 Certificates with SSL Extensions 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. In addition, GeoTrust may also enable the Certificate for use as a client Certificate.

GeoTrust **Publisher Certificates** may only be used for the purposes of (i) identification of the Publisher as the party accessing the code signing portal, and (ii) locally signing the code for subsequent resigning by the appropriate Code Confirmation certificate.

GeoTrust **Code Confirmation** Certificates allow GeoTrust to use the associated Private Key to digitally resign application code which has been digitally signed by a Publisher Certificate Private Key, upon request of code confirmation from the Publisher.

GeoTrust **My Credential**™ client Certificates are X.509 Certificates with S/MIME Extensions issued which facilitate secure electronic commerce by providing limited authentication of a Subscriber's client and permitting secure VPN access and S/MIME communications between a Relying Party and the Subscriber's client.

True Credentials® and **True Credential Express** Client Certificates are X.509 Certificates with S/MIME Extensions which facilitate secure electronic commerce by providing limited authentication of a Subscriber's client and permitting SSL Client Authentication, secure VPN access and S/MIME communications between a Relying Party and the Subscriber's client, and in some instances may also be used for code signing and document signing.

RapidSSL, RapidSSL Wildcard and **RapidSSL Enterprise** Certificates are X.509 Certificates with SSL Extensions that chain to GeoTrust's trusted root(s). RapidSSL certificates facilitate secure electronic commerce by providing limited authentication of a Subscriber's server and 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.

RapidSSL Wildcard Certificates 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.

The **RapidSSL Enterprise** Certificate is intended for use only within the enterprise intranet. RapidSSL Enterprise Certificates are only available to Symantec Managed PKI for SSL customers.

GeoTrust FreeSSL Server Certificates are X.509 Certificates with SSL Extensions that chain to GeoTrust's trusted root(s) 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.

1.4.2 Prohibited Certificate Uses

The GeoTrust CA and CAs subordinate to the GeoTrust CA shall not issue any certificate that can be used for man-in-the-middle (MITM) or traffic management of domain names or IPs that the

certificate holder does not legitimately own or control. Such certificate usage is expressly prohibited.

Certificates shall be used only to the extent the use is consistent with applicable law, and in particular shall be used only to the extent permitted by applicable export or import laws.

GeoTrust Certificates are not designed, intended, or authorized for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage. Client Certificates are intended for client applications and shall not be used as server or organizational Certificates.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The organization administering this CPS is Symantec Corporation. Inquiries should be addressed as follows:

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527-8000 (voice)
+1 (650) 527-8050 (fax)
practices@symantec.com

1.5.2 Contact Person

Address inquiries about the CPS to *practices@symantec.com* or to the following address:

Symantec Corporation Practices
350 Ellis Street
Mountain View, CA 94043
USA

1.5.3 CPS Approval Procedure

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

1.6 Definitions and Acronyms

See Appendix A for a table of acronyms and definitions

2. Publication and Repository Responsibilities

2.1 Repositories

GeoTrust shall operate CRLs that will be available to both Subscribers and Relying Parties of GeoTrust Certificates. Each CRL is signed by the issuing CA. The procedures for revocation are as stated elsewhere in this CPS.

2.2 Publication of Certificate Information

GeoTrust retains copies of all Certificates for the life of the CA, but does not archive or retain expired or superseded CRLs.

2.3 Time or Frequency of Publication

Updates to this CPS are published in accordance with Section 9.12. Updates to Subscriber Agreements and Relying Party Agreements are published as necessary. Certificates are published after issuance. Certificate status information is published in accordance with the provisions of this CPS.

2.4 Access Controls on Repository

Information published in the repository portion of the GeoTrust web site is publicly-accessible information. Read only access to such information is unrestricted.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

Certificates contain an X.501 distinguished name in the Subject name field and consist of the components specified in the table below.

Attribute	***Value***
Country (C) =	2 letter ISO country code or not used.
Organization (O) =	The Organization attribute is used as follows: • Subscriber organizational name for web server Certificates and individual Certificates that have an organization affiliation, or • A domain name, or "GeoTrust Verified Site" or similar language in the Organization field (for web server certificates that have domain control validation only and no organization verification), or • When applicable, wording to the effect that the organization has not been authenticated.
Organizational Unit (OU) =	GeoTrust Certificates may contain multiple OU attributes. Such attributes may contain one or more of the following: • Subscriber organizational unit (for organizational Certificates and individual Certificates that have an organization affiliation) • Text to describe the type of Certificate. • Text to describe the entity that performed the verification • "Domain Control Validated", where appropriate • Business registration number, if available

Attribute	*Value*
	• The address of the customer
State or Province (S) =	When used, indicates the Subscriber's State or Province
Locality (L) =	When used, indicates the Subscriber's Locality
Common Name (CN) =	This attribute may include: • Domain name (for web server Certificates) • Organization name (for code/object signing Certificates and RapidSSL Enterprise) • Name of individual (for certificates issued to individuals). • IP Address (TrueBusiness ID) or Private IP Address (RapidSSL Enterprise) • Host name (RapidSSL Enterprise)
E-Mail Address (E) =	When used, the e-mail address associated with the certificate

Table 1 – Distinguished Name Attributes in Subscriber Certificates

EV SSL certificate content and profile requirements are discussed in Appendix A3 to this CPS.

3.1.1.1 CABF Naming Requirements

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the CA / Browser Forum requirements as set forth in the GeoTrust Supplemental Procedures, in section 9 of Appendix B1, Appendix C and Appendix D, respectively.

3.1.2 Need for Names to be Meaningful

Domain names do not have to be meaningful or unique, but must match a second level domain name as posted by InterNIC.

3.1.3 Anonymity or Pseudonymity of Subscribers

With the exception of **True Credential** and **True Credential Express**, Subscribers are not permitted to use pseudonyms (names other than a Subscriber's true personal or organizational name).

3.1.4 Rules for Interpreting Various Name Forms

No stipulation

3.1.5 Uniqueness of Names

No stipulation

3.1.6 Recognition, Authentication, and Role of Trademarks

Certificate Applicants are prohibited from using names in their Certificate Applications that infringe upon the Intellectual Property Rights of others. GeoTrust, however, does not verify whether a Certificate Applicant has Intellectual Property Rights in the name appearing in a Certificate Application or arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any domain name, trade name, trademark, or service mark. GeoTrust is entitled, without liability to any Certificate Applicant, to reject or suspend any Certificate Application because of such dispute.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The certificate applicant must demonstrate that it rightfully holds the private key corresponding to the public key to be listed in the Certificate. The method to prove possession of a private key shall be PKCS #10, another cryptographically equivalent demonstration, or another GeoTrust-approved method. This requirement does not apply where a key pair is generated by a CA on behalf of a Subscriber, for example where pre-generated keys are placed on smart cards.

3.2.2 Authentication of Organization Identity

Whenever an organization name is included in the Certificate, GeoTrust or the RA 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
(i) verify the validity of the registration through the authority that issued it, or
(ii) verify the validity of the registration through a reputable third party database or other resource, or
(iii) verify the validity of the Organization through a trusted third party, or
(iv) confirm that the Organization exists if such Organization is not the type that is typically registered or is capable of being verified under clause (b).

Additional procedures are performed for specific types of Certificates as described in Table 2 below.

Certificate Type	***Additional Procedures***
Extended Validation (EV) Certificates	Supplemental validation procedures for issuing EV SSL Certificates are described in Appendix A1 to this CPS. Supplemental validation procedures for issuing EV Code-Signing Certificates are described in Appendix B to this CPS.
Organization Validated (OV) and Domain Validated (DV) Certificates	GeoTrust's procedures for issuing OV and DV certificates, distinguished throughout the CPS as 'CABF requirements for OV and DV certificates'.
Hardware Protected EV Code-Signing Certificate	GeoTrust verifies that the key pair was generated on FIPS 140 certified hardware

Table 2 – Specific Authentication Procedures

3.2.2.1 CABF Verification Requirements for Organization Applicants

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the CA / Browser Forum requirements as set forth in the GeoTrust Supplemental Procedures, in section 11 of Appendix B1, Appendix C and Appendix D, respectively..

3.2.2.2 Mozilla Verification Requirements for Organization Applicants

For requests for internationalized domain names (IDNs) in Certificates, GeoTrust performs domain name owner verification to detect cases of homographic spoofing of IDNs. GeoTrust

employs an automated process that searches various 'whois' services to find the owner of a particular domain. A search failure result is flagged for manual review and the RA manually rejects the Certificate Request. Additionally, the RA rejects any domain name that visually appears to be made up of multiple scripts within one hostname label.

GeoTrust actively participates in the CA/Browser Forum providing input to the standards for IDN Certificates and fully commits to conforming with standards drafted by that body.

3.2.3 Authentication of Domain Name

When a domain name is included in a Certificate together with an organization name, GeoTrust or the RA 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 name verification as described above is performed for **TrueBusiness ID, Enterprise SSL** and **Enterprise SSL Premium**, **RapidSSL Enterprise** and **FreeSSL Server** Certificates.

True Business ID Certificates may contain an IP address in the *CommonName* field. **RapidSSL Enterprise** Certificates may contain a private IP address in the *CommonName* field.

When a domain name is included in a Certificate without authentication of the entity owning the domain name, GeoTrust or an RA will verify that the Subscriber has control over such domain name at the time it submitted its enrolment form by accessing a third party database of domain names and their owners. To do this, GeoTrust will send an e-mail message to one of the following e-mail addresses requesting confirmation of the Certificate order and authorization to issue the Certificate in the domain name:

(a) an e-mail address listed as the administrative or technical contact for the domain name in an official InterNIC domain name registry that includes the domain name,
(b) a limited list of the most commonly used generic e-mail addresses for authorized persons at domain names (e.g., "*admin@domain.com*," or "*hostmaster@domain.com*" for the domain name domain.com), or
(c) using a manual process of verification conducted by GeoTrust, to an e-mail address identified as the registered owner of the domain per the *whois* database. Optionally, a verification phone call may be substituted to the domain owner phone number listed in the *whois*.

Upon receipt of a confirming e-mail message authorizing issuance of the Certificate, GeoTrust will issue the Certificate as described below. Additionally, a confirmatory phone call to the applicant may be performed for Domain Control Certificate applications.

Domain name control is performed for the products listed in the table below.

Product Name
GeoTrust Power Server ID Certificates
GeoTrust QuickSSL Certificates
GeoTrust QuickSSL Premium Certificates
GeoTrust RapidSSL Certificates
GeoTrust RapidSSL Wildcard Certificates
GeoTrust FreeSSL Server Certificates

3.2.4 Authentication of individual identity

An Applicant for a GeoTrust **My Credential** Certificate shall complete a GeoTrust My Credential enrollment application on behalf of Subscriber in a form prescribed by GeoTrust. All applications are subject to review, approval and acceptance by GeoTrust. All Applicants are required to include an e-mail contact address ("Contact Address") and telephone number ("Telephone Number") within the My Credential enrollment application and prove control over the Contact Address and Telephone Number. GeoTrust does not otherwise verify the accuracy of the information contained in the Applicant's enrollment form or otherwise check for errors and omissions.

True Credential Subscribers must provide the following data in or with the CSR: *Common Name* and *E-mail Address* of Subscriber. Company's Administrator will have sole responsibility for approving all Certificate requests for issuance.

Once approved, GeoTrust will process the Certificate applications without confirming the information on the Certificates. Company will be required to agree to terms and conditions of use as necessary for issuance of Certificates through an enrolment agreement, and Subscribers receiving Certificates via the Service may be required to agree to additional terms and conditions of use as necessary to receive a Certificate authorized by the Administrator.

3.2.5 Non-Verified Subscriber Information

Non-verified Subscriber information includes:

- Organization Unit (OU) with certain exceptions[1]
- Country Code (within the **Power Server ID** and **Quick SSL** Certificate)
- Customer specified host name or organizational unit (within the **RapidSSL Enterprise** certificate)
- Any other information designated as non-verified in the certificate.

3.2.6 Validation of Authority

GeoTrust will take reasonable steps to establish that a Certificate request made on behalf of that Organization is legitimate and properly authorized. 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.

3.2.7 Criteria for Interoperation

No Stipulation

[1] Domain-validated and organization-validated certificates that attest compliance with CA/Browser guidelines may contain Organizational Unit values that are validated.

3.3 Identification and Authentication for Re-key Requests

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 key generation tools. For purposes of this CPS, both a "rekey" and "renewal" as defined above will be treated as a renewal Certificate.

New certificate information submitted for renewal Certificates are subject to the same authentication steps outlined in this CPS as apply to initial issuance of a Certificate.

3.4 Identification and Authentication for Revocation Request

The only persons permitted to request revocation of a Certificate issued by GeoTrust are the Subscriber (including designated representatives), the administrative contact or the technical contact, or an enterprise Administrator.

To request revocation, a Subscriber or Authorized requester 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. 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.

Enterprise Administrators may revoke certificates through a Web based application.

4. Certificate Life-Cycle Operations

4.1 Certificate Application

4.1.1 Who Can Submit A Certificate Application?

Below is a list of people who may submit certificate applications:

- Any individual who is the subject of the certificate,
- Any authorized representative of an Organization or entity,
- Any authorized representative of a CA,
- Any authorized representative of an RA.

4.1.2 Enrollment Process and Responsibilities

4.1.2.1 End-User Certificate Subscribers

All end-user Certificate Subscribers shall manifest assent to the relevant Subscriber Agreement and undergo an enrollment process consisting of:

- completing a Certificate Application and providing true and correct information,
- generating, or arranging to have generated, a key pair,
- delivering his, her, or its public key, directly or through an RA, to GeoTrust
- demonstrating possession of the private key corresponding to the public key delivered to GeoTrust.

RapidSSL Enterprise certificate enrolments are only available through the Symantec Managed PKI (MPKI) for SSL program.

4.1.2.2 CABF Certificate Application Requirements

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the CA / Browser Forum requirements as set forth in the GeoTrust Supplemental Procedures, in section 10 of Appendix B1, Appendix C and Appendix D, respectively.

4.1.2.3 CA and RA Certificates

Subscribers of CA and RA Certificates enter into a contract with GeoTrust. CA and RA Applicants shall provide their credentials to demonstrate their identity and provide contact information during the contracting process. During this contracting process or, at the latest, prior to the Key Generation Ceremony to create a CA or RA key pair, the applicant shall cooperate with GeoTrust to determine the appropriate distinguished name and the content of the Certificates to be issued by the applicant.

[29] On an exceptionary basis there may be instances where subscriber certificates will be issued directly from the root. This exception shall only be used in the event of a subscriber certificate with a key pair size and length that is 2048 bit or less

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

GeoTrust or an RA shall perform identification and authentication of all required Subscriber information in terms of Section 3.2.

At certain times during the enrolment process in which GeoTrust is not able to verify information in an enrolment 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 enrolment form for a Certificate.

4.2.2 Approval or Rejection of Certificate Applications

GeoTrust or an RA will approve an application for a certificate if the following criteria are met:

- Successful identification and authentication of all required Subscriber information in terms of Section 3.2
- Payment has been received

GeoTrust or an RA will reject a certificate application if:

- identification and authentication of all required Subscriber information in terms of Section 3.2 cannot be completed, or
- The Subscriber fails to furnish supporting documentation upon request, or
- The Subscriber fails to respond to notices within a specified time, or
- Payment has not been received, or
- they believe that issuing a certificate to the Subscriber may bring the GeoTrust PKI into disrepute

4.2.3 Time to Process Certificate Applications

GeoTrust begins processing certificate applications within a reasonable time of receipt. There is no time stipulation to complete the processing of an application unless otherwise indicated in the relevant Subscriber Agreement, CPS or other Agreement between GeoTrust PKI participants.

A certificate application remains active until rejected or issued.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

A Certificate is created and issued following the approval of a Certificate Application by GeoTrust or following receipt of an RA's request to issue the Certificate. GeoTrust creates and issues to a Certificate Applicant a Certificate based on the information in a Certificate Application following approval of such Certificate Application.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificates

GeoTrust shall, either directly or through an RA, notify Subscribers that they have created such Certificates, and provide Subscribers with access to the Certificates by notifying them that their Certificates are available. Certificates shall be made available to end-user Subscribers, either by allowing them to download them from a web site, an application programming interface (API) or via a message sent to the Subscriber containing the Certificate.

4.3.3 CABF Requirement for Certificate Issuance by a Root CA

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the CA / Browser Forum requirements as set forth in the GeoTrust Supplemental Procedures, in section 12 of Appendix B1, Appendix C and Appendix D, respectively.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The applicant expressly indicates acceptance of a Certificate by downloading and/or using such Certificate.

4.4.2 Publication of the Certificate by the CA

GeoTrust may publish the Certificates it issues in a publicly accessible repository.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

RAs may receive notification of the issuance of certificates they approve.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Usage

Use of the Private key corresponding to the public key in the certificate shall only be permitted once the Subscriber has agreed to the Subscriber Agreement and accepted the certificate. The certificate shall be used lawfully in accordance with GeoTrust's Subscriber Agreement and the terms of this CPS. Certificate use must be consistent with the KeyUsage field extensions included in the certificate (e.g., if Digital Signature is not enabled then the certificate must not be used for signing).

Subscribers shall protect their private keys from unauthorized use and shall discontinue use of the private key following expiration or revocation of the certificate. Parties other than the Subscriber shall not archive the Subscriber Private Key except as set forth in section 4.12.

The Certificate shall not be installed on more than a single server at a time unless the Subscriber enrollment and corresponding fees have stipulated installation on multiple servers.

4.5.2 Relying Party Public Key and Certificate Usage

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. Reliance on a certificate must be reasonable under the circumstances. If the circumstances indicate a need for additional assurances, the Relying Party must obtain such assurances for such reliance to be deemed reasonable.

Before any act of reliance, Relying Parties shall independently assess:

- the appropriateness of the use of a Certificate for any given purpose and determine that the Certificate will, in fact, be used for an appropriate purpose that is not prohibited or otherwise restricted by this CPS. GeoTrust is not responsible for assessing the appropriateness of the use of a Certificate.
- That the certificate is being used in accordance with the KeyUsage field extensions included in the certificate (e.g., if Digital Signature is not enabled then the certificate may not be relied upon for validating a Subscriber's signature).
- The status of the certificate and all the CAs in the chain that issued the certificate. If any of the Certificates in the Certificate Chain have been revoked, the Relying Party is solely responsible to investigate whether reliance on a digital signature performed by an end user Subscriber Certificate prior to revocation of a Certificate in the Certificate chain is reasonable. Any such reliance is made solely at the risk of the Relying party.

Assuming that the use of the Certificate is appropriate, Relying Parties shall utilize the appropriate software and/or hardware to perform digital signature verification or other cryptographic operations they wish to perform, as a condition of relying on Certificates in connection with each such operation. Such operations include identifying a Certificate Chain and verifying the digital signatures on all Certificates in the Certificate Chain.

4.6 Certificate Renewal

4.6.1 Circumstances for Certificate Renewal

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 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.

4.6.2 Who May Request Renewal

Only the subscriber for an individual certificate or an authorized representative for an Organizational certificate may request certificate renewal

4.6.3 Processing Certificate Renewal Requests

See section 4.2.

4.6.4 Notification of New Certificate Issuance to Subscriber

Notification of issuance of certificate renewal to the Subscriber is in accordance with Section 4.3.2.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Conduct constituting Acceptance of renewed certificate is in accordance with Section 4.4.1.

4.6.6 Publication of the Renewal Certificate by the CA

No stipulation.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

RAs may receive notification of the issuance of certificates they approve.

4.7 Certificate Re-Key

See Section 3.3.

4.7.1 Circumstances for Re-Key

See Section 3.3.

4.7.2 Who May Request Certification of a New Public Key

Only the subscriber for an individual certificate or an authorized representative for an Organizational certificate may request certificate renewal/rekey.

4.7.3 Processing Certificate Re-Keying Requests

The provisions of Section 4.6.3 apply.

4.7.4 Notification of New Certificate Issuance to Subscriber

Notification of issuance of a re-keyed certificate to the Subscriber is in accordance with Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Conduct constituting Acceptance of a re-keyed certificate is in accordance with Section 4.4.1.

4.7.6 Publication of the Re-Keyed Certificate by the CA

GeoTrust does not publish certificates it issues.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

RAs may receive notification of the issuance of certificates they approve.

4.8 Certificate Modification

4.8.1 Circumstances for Certificate Modification

Certificate modification refers to the application for the issuance of a new certificate due to changes in the information in an existing certificate (other than the subscriber's public key). Certificate modification is considered a Certificate Application in terms of Section 4.1.

4.8.2 Who May Request Certificate Modification

See Section 4.1.1.

4.8.3 Processing Certificate Modification Requests

GeoTrust or an RA shall perform identification and authentication of all required Subscriber information in terms of Section 3.2.

4.8.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

See Section 4.4.1.

4.8.6 Publication of the Modified Certificate by the CA

Not applicable.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

A Subscriber may request revocation of its Certificate at any time for any of the following reasons. A Subscriber shall request GeoTrust (or an enterprise Administrator) to revoke 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 SSL Certificate is installed on more than a single server at a time without permission of GeoTrust.
- If customer or subscriber has failed to meet its material obligations under the Subscriber and /or Enrolment Agreement
- If an RA reasonably determines that a Publisher Certificate is being used in a manner that compromises the trust status of relying parties.
- If GeoTrust determines in its sole discretion that any material fact contained in the Publisher Certificate is no longer true.

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.

In the event that GeoTrust ceases operations and there is no plan for transition of GeoTrust's services to a successor or no plan to otherwise address such event, all Certificates issued by GeoTrust shall be revoked prior to the date that GeoTrust ceases operations, and GeoTrust shall notify the technical contact provided by Publisher by e-mail message of the revocation and the reason for the revocation.

4.9.1.1 CABF Requirements for Reasons for Revocation

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the CA / Browser Forum requirements as set forth in the GeoTrust Supplemental Procedures, in section 13 of Appendix B1, Appendix C and Appendix D, respectively.

4.9.2 Who Can Request Revocation

The only persons permitted to request revocation of a Certificate issued by GeoTrust are the Subscriber (including designated representatives), the administrative contact or the technical contact, an enterprise Administrator, GeoTrust and Microsoft (under certain circumstances).

4.9.3 Procedure for Revocation Request

4.9.3.1 Procedure for Requesting the Revocation of an End-User Subscriber Certificate

See Section 3.4.

4.9.3.2 CABF Requirements for Certificate Revocation Process

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the CA / Browser Forum requirements as set forth in the GeoTrust Supplemental Procedures, in section 13 of Appendix B1 and C and section 13.1 of Appendix D, respectively.

4.9.3.2 Procedure for Requesting the Revocation of a CA or RA Certificate

A CA or RA requesting revocation of its CA or RA Certificate is required to communicate the request to GeoTrust and GeoTrust will seek confirmation of the request. GeoTrust will then revoke the Certificate. RapidSSL for Enterprise certificates are revoked through the Symantec MPKI for SSL Service and do not require an out-of-band confirmation.

GeoTrust may also initiate CA or RA Certificate revocation.

4.9.4 Revocation Request Grace Period

Revocation requests shall be submitted as promptly as possible within a commercially reasonable time. There is no grace period available to the Subscriber prior to revocation.

4.9.5 Time within Which CA Must Process the Revocation Request

GeoTrust takes commercially reasonable steps to process revocation requests without delay.

4.9.6 Revocation Checking Requirements for Relying Parties

Relying Parties shall check the status of Certificates on which they wish to rely. One method by which Relying Parties may check Certificate status is by consulting the most recent CRL from the CA that issued the Certificate on which the Relying Party wishes to rely. Certificate Revocation Lists are available at *www.geotrust.com*. Certificate Revocation Lists are available at *www.FreeSSL.com/legal and www.RapidSSL.com/legal* for FreeSSL certificates and RapidSSL certificates respectively.

4.9.7 CRL Issuance Frequency

GeoTrust shall post the CRL online at least weekly (but no later than twenty-four (24) hours after revocation of a Certificate) in a DER format except as otherwise provided in GeoTrust's Business Continuity Plan. If a Certificate listed in a CRL expires, it may be removed from later-issued CRLs after the Certificate's expiration.

4.9.7.1 CABF Requirements for CRL Issuance

CRL issuance for EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the CA / Browser Forum requirements as set forth in the GeoTrust Supplemental Procedures, in section 13 of Appendix B1 and C, and section 13.2.2 of Appendix D, respectively.

4.9.8 Maximum Latency for CRLs

CRLs are posted to the repository within a commercially reasonable time after generation.

4.9.9 On-Line Revocation/Status Checking Availability

The CRL is available at: *www.geotrust.com*. Certificate Revocation Lists are available at *www.FreeSSL.com/legal and www.RapidSSL.com/legal* for FreeSSL certificates and RapidSSL certificates respectively.

4.9.9.1 CABF Requirements for OCSP Availability

OCSP availability for EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the CA / Browser Forum requirements as set forth in the GeoTrust Supplemental Procedures, in section 13 of Appendix B1 and C, and section 13.2.2 of Appendix D, respectively.

4.9.10 On-Line Revocation Checking Requirements

A Relying Party must check the status of a certificate on which he/she/it wishes to rely.

4.9.11 Other Forms of Revocation Advertisements Available

Not Applicable.

4.9.12 Special Requirements Regarding Key Compromise

In the event of compromise of a GeoTrust Private Key used to sign Certificates, 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.

4.9.13 Circumstances for Suspension

GeoTrust does not support Certificate suspension for the Certificates.

4.9.14 Who can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits of Suspension Period

Not applicable.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The status of certificates is available via CRL at GeoTrust's website or the RapidSSL/FreeSSL website.

4.10.2 Service Availability

Certificate Status Services are available 24×7 without scheduled interruption.

Certificate status services for EV SSL Certificates, EV Code Signing, and Organization-validated and Domain-validated SSL Certificates, conform to the CA / Browser Forum requirements as set forth in the GeoTrust Supplemental Procedures, in section 13 of Appendix B1 and C and section 13.2.3 of Appendix D, respectively.

4.10.3 Optional Features

Not applicable.

4.11 End of Subscription

A subscriber may end a subscription for a GeoTrust certificate by:
• Allowing his/her/its certificate to expire without renewing or re-keying that certificate
• Revoking of his/her/its certificate before certificate expiration without replacing the certificates.

4.12 Key Escrow and Recovery

The Root Keys for each CA Certificate were generated and are stored in hardware and are backed up but not escrowed. GeoTrust CA participants may escrow end-user Subscriber private keys.

4.12.1 Key Escrow and Recovery Policy and Practices

The private keys of end-user Subscribers may be escrowed.

When applicable, private keys are stored in GeoTrust's premises in encrypted PKCS#12 structures. A unique symmetric key is generated for each Subscriber's private key. A PKCS#12 structure is generated with the Subscriber's private key and certificate. The PKCS#12 structure is encrypted with the symmetric key using 128-bit AES. The symmetric key is then encrypted with the public key of the Enterprise's Master Key Recovery Certificate using 128-bit AES. The encrypted PKCS#12 and the encrypted symmetric key are stored in GeoTrust's premises.

Recovery of a private key and digital certificate requires the Administrator who has access to the Master Key Recovery Certificate to securely access their Enterprise account with GeoCenter and select the enrolment record associated with the private key that is to be recovered. The Administrator then downloads the encrypted PKCS#12 and initiates the Recovery process. A

java applet is downloaded to the local workstation and the Administrator is prompted to identify the location of the Master Key Recovery certificate and the password for accessing the Master Key Recovery certificate. The java applet accesses the private key of the Master Key Recovery certificate and uses the private key to decrypt the encrypted symmetric key. The symmetric key is then displayed, and the Administrator can use the symmetric key to access the encrypted PKCS#12.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

See section 4.12.1.

5. Facility, Management, and Operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

GeoTrust's CA and RA operations are conducted within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information and systems whether covert or overt.

GeoTrust's CAs are physically located in a highly secure facility which includes the following:

- Slab to slab barriers
- Electronic control access systems
- Alarmed doors and video monitoring
- Security logging and audits
- Card key access for specially approved employees with defined levels of management approval required

5.1.2 Physical Access

Only authorized GeoTrust employees can access the GeoTrust CA facility using biometrics, and proximity card access

5.1.3 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.

5.1.4 Water Exposures

GeoTrust has taken reasonable precautions to minimize the impact of water exposure to GeoTrust systems.

5.1.5 Fire Prevention and Protection

GeoTrust has taken reasonable precautions to prevent and extinguish fires or other damaging exposure to flame or smoke. GeoTrust's fire prevention and protection measures have been designed to comply with local fire safety regulations.

5.1.6 Media Storage

All media containing production software and data, audit, archive, or backup information is stored within multiple GeoTrust facilities in TL-15 rated safes with appropriate physical and logical access controls designed to limit access to authorized personnel and protect such media from accidental damage.

5.1.7 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.

5.1.8 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.

5.2 Procedural Controls

5.2.1 Trusted Roles

Trusted Persons include all employees, contractors, and consultants that have access to or control authentication or cryptographic operations that may materially affect:

- the validation of information in Certificate Applications;
- the acceptance, rejection, or other processing of Certificate Applications, revocation requests, renewal requests, or enrollment information;
- the issuance, or revocation of Certificates, including personnel having access to restricted portions of its repository;
- the handling of Subscriber information or requests.

Trusted Persons include, but are not limited to:

- customer service personnel,
- cryptographic business operations personnel,
- security personnel,
- system administration personnel,
- designated engineering personnel, and
- executives that are designated to manage infrastructural trustworthiness.

GeoTrust considers the categories of personnel identified in this section as Trusted Persons having a Trusted Position. Persons seeking to become Trusted Persons by obtaining a Trusted Position must successfully complete the screening requirements set out in this CPS.

5.2.2 Number of Persons Required per Task

GeoTrust has established, maintains, and enforces rigorous control procedures to ensure the segregation of duties based on job responsibility and to ensure that Trusted Persons are required to perform sensitive tasks.

Policy and control procedures are in place to ensure segregation of duties based on job responsibilities. The most sensitive tasks, such as access to and management of CA

cryptographic hardware (cryptographic signing unit or CSU) and associated key material, require Trusted Persons. These internal control procedures are designed to ensure that trusted personnel are required to have either physical or logical access to the device. Access to CA cryptographic hardware is strictly allowed by Trusted Persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction.

5.2.3 Identification and Authentication for Each Role

For all personnel seeking to become Trusted Persons, verification of identity is performed through the personal (physical) presence of such personnel before Trusted Persons performing GeoTrust Human Resources or security functions and a check of well-recognized forms of identification (e.g., passports and driver's licenses). Identity is further confirmed through the background checking procedures in CPS § 5.3.1.

GeoTrust ensures that personnel have achieved Trusted Status and departmental approval has been given before such personnel are:

- issued access devices and granted access to the required facilities;
- issued electronic credentials to access and perform specific functions on the GeoTrust CA, RA, or other IT systems.

5.2.4 Roles Requiring Separation of Duties

Roles requiring Separation of duties include (but are not limited to):

- the validation of information in Certificate Applications;
- the acceptance, rejection, or other processing of Certificate Applications, revocation requests, or renewal requests, or enrollment information;

5.3 Personnel Controls

Personnel seeking to become Trusted Persons must present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily, as well as proof of any government clearances, if any, necessary to perform certification services under government contracts. Background checks are repeated at least every 5 years for personnel holding Trusted Positions.

5.3.1 Qualifications, Experience, and Clearance Requirements

GeoTrust requires that personnel seeking to become Trusted Persons present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily, as well as proof of any government clearances, if any, necessary to perform certification services under government contracts.

5.3.2 Background Check Procedures

Prior to commencement of employment in a Trusted Role, GeoTrust conducts background checks which include the following:

- confirmation of previous employment,
- check of professional reference,
- confirmation of the highest or most relevant educational degree obtained,
- search of criminal records (local, state or provincial, and national),
- check of credit/financial records,
- search of driver's license records, and

- search of Social Security Administration records.

To the extent that any of the requirements imposed by this section cannot be met due to a prohibition or limitation in local law or other circumstances, GeoTrust will utilize a substitute investigative technique permitted by law that provides substantially similar information, including but not limited to obtaining a background check performed by the applicable governmental agency.

The factors revealed in a background check that may be considered grounds for rejecting candidates for Trusted Positions or for taking action against an existing Trusted Person generally include (but are not limited to) the following:

- Misrepresentations made by the candidate or Trusted Person,
- Highly unfavorable or unreliable professional references,
- Certain criminal convictions, and
- Indications of a lack of financial responsibility.

Reports containing such information are evaluated by human resources and security personnel, who determine the appropriate course of action in light of the type, magnitude, and frequency of the behavior uncovered by the background check. Such actions may include measures up to and including the cancellation of offers of employment made to candidates for Trusted Positions or the termination of existing Trusted Persons.

The use of information revealed in a background check to take such actions is subject to the applicable federal, state, and local laws.

5.3.3 Training Requirements

For EV SSL Certificates, EV Code Signing, and Organization-validated and Domain-validated SSL Certificates, personnel training is provided as set forth in the GeoTrust Supplemental Procedures, in section 14.1 of Appendix B1, Appendix C and Appendix D, respectively.

5.3.4 Retraining Frequency and Requirements

GeoTrust provides refresher training and updates to their personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily.

5.3.5 Job Rotation Frequency and Sequence

Not applicable.

5.3.6 Sanctions for Unauthorized Actions

Appropriate disciplinary actions are taken for unauthorized actions or other violations of GeoTrust policies and procedures. Disciplinary actions may include measures up to and including termination and are commensurate with the frequency and severity of the unauthorized actions.

5.3.7 Independent Contractor Requirements

In limited circumstances, independent contractors or consultants may be used to fill Trusted Positions. Any such contractor or consultant is held to the same functional and security criteria that apply to a GeoTrust employees in a comparable position.

Independent contractors and consultants who have not completed or passed the background check procedures specified in CPS Section 5.3.2 are permitted access to GeoTrust's secure facilities only to the extent they are escorted and directly supervised by Trusted Persons at all times.

5.3.8 Documentation Supplied to Personnel

GeoTrust provides its employees the requisite training and other documentation needed to perform their job responsibilities competently and satisfactorily.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

GeoTrust records CA event data.

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the CA /Browser Forum requirements as set forth in the GeoTrust Supplemental Procedures in section 15, Appendix B1, Appendix C and Appendix D, respectively.

5.4.2 Frequency of Processing Log

GeoTrust CA event journal data is archived both daily and monthly. Event journals are subject to review.

5.4.3 Retention Period for Audit Log

Audit logs shall be retained onsite for at least two (2) months after processing and thereafter archived in accordance with Section 5.5.2.

5.4.4 Protection of Audit Log

Audit logs are protected in accordance with Section 5.1.6

5.4.5 Audit Log Backup Procedures

See Section 5.4.3

5.4.6 Audit Collection System (Internal vs. External)

No stipulation.

5.4.7 Notification to Event-Causing Subject

Where an event is logged by the audit collection system, no notice is required to be given to the individual, organization, device, or application that caused the event.

5.4.8 Vulnerability Assessments

No Stipulation.

5.4.9 Archive Collection System (Internal or External)

No Stipulation.

5.4.10 Procedures to Obtain and Verify Archive Information

Only authorized Trusted Personnel are able to obtain access to the archive. The integrity of the information is verified when it is restored.

5.5 Records Archival

5.5.1 Types of Records Archived

GeoTrust archives the following type of records:

- Certificate application information
- Documentation supporting certificate applications
- Certificate lifecycle information e.g., revocation, rekey and renewal application information

5.5.2 Retention Period for Archive

Records shall be retained for at least 3 years, at least 5 years for CA key pairs and 7 years for EV Certificates following the date the Certificate expires or is revoked.

5.5.3 Protection of Archive

GeoTrust protects the archive so that only authorized Trusted Persons are able to obtain access to the archive. The archive is protected against unauthorized viewing, modification, deletion, or other tampering by storage within a Trustworthy System. The media holding the archive data and the applications required to process the archive data shall be maintained to ensure that the archive data can be accessed for the time period set forth in this CPS.

5.5.4 Archive Backup Procedures

No Stipulation.

5.5.5 Requirements for Time-Stamping of Records

Certificates, CRLs, and other revocation database entries shall contain time and date information. Such time information need not be cryptographic-based.

5.5.6 Archive Collection System (Internal or External)

No stipulation.

5.5.7 Procedures to Obtain and Verify Archive Information

Only authorized Trusted Personnel are able to obtain access to the archive. The integrity of the information is verified when it is restored.

5.6 Key Changeover

GeoTrust CA key pairs are retired from service at the end of their respective lifetimes as defined in this CPS. GeoTrust CA Certificates may be renewed. 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.

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 hardware cryptographic modules. 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 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.

GeoTrust Root CA key pair lifetimes

- Root 1 – Equifax Secure Certificate Authority: Expires Aug 22, 2018
- Root 2 – GeoTrust Global CA: Expires May 21, 2022
- Root 3 – GeoTrust Universal CA: Expires March 04, 2029
- Root 4 – Equifax Secure eBusiness CA-1: Expires Jun 21, 2020
- Root 5 – Equifax Secure Global eBusiness CA-1: Expires Jun 21, 2020
- Root 6 – GeoTrust Global CA2: Expires March 04, 2019
- Root 7 – GeoTrust Universal CA2: Expires March 04, 2029
- Root 8 – Equifax Secure eBusiness CA-2: Expires Jun 21, 2020
- Root 9 – GeoTrust CA for Adobe: Expires 15 Jan 2015
- Root 10 – GeoTrust Mobile Device Root – Unprivileged: Expires Jul 29 2023
- Root 11 – GeoTrust Mobile Device Root – Privileged: Expires Jul 29 2023
- Root 12 – GeoTrust CA for UTI: Expires 23 Jan 2024
- Root 13 – GeoTrust True Credentials CA 2: Expires Jun 21, 2020
- Root 14 – GeoTrust Primary Certification Authority: Expires July 16, 2036
- Root 15 – GeoTrust Primary Certification Authority - G2: Expires January 18, 2038
- Root 16 – GeoTrust Primary Certification Authority – G3: Expires December 1, 2037
- Root 16 – GeoTrust Primary Certification Authority – G4: Expires December 1, 2037

New Roots and CAs created after publication of this CPS will have the following maximum validity periods:

- Self-signed Root CA Certificates: 30 years
- Intermediate CA Certificates: 15 years

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

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

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

In the event of the corruption of computing resources, software, and/or data, such an occurrence is reported to GeoTrust Security. Appropriate escalation, incident investigation, and incident response will ensue.

5.7.3 Entity Private Key Compromise 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 e-mail and notify Relying Parties and others via the CRL and additional notice posted at *www.geotrust.com* or *www.rapidssl.com*, and shall revoke all Certificates issued with such GeoTrust Root Key(s).

5.7.4 Business Continuity Capabilities after a Disaster

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.

GeoTrust has developed a Disaster Recovery Plan (DRP) for its PKI services including the GeoTrust PKI service. The DRP identifies conditions for activating the plan and what constitutes an acceptable system outage and recovery time.

The DRP defines the procedures for the teams to maintain or reconstitute GeoTrust business operations following interruption to or failure of critical business processes by using backup data and backup copies of the GeoTrust keys. Specifically, GeoTrust's DRP includes:

- Emergency procedures,
- Fallback procedures,
- Resumption procedures,
- Recovery time objective (RTO),
- Frequency for taking backup copies of essential business information and software,
- Requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location,
- Separation distance of the Disaster recovery site to the CA's main site,
- Procedures for securing the Disaster facility during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site,

GeoTrust's DRP identifies administrative requirements including:

- maintenance schedule for the plan;
- Awareness and education requirements;
- Responsibilities of the individuals; and
- Regular testing of contingency plans.

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.

Additionally, for EV SSL Certificates, EV Code Signing, and Organization-validated and Domain-validated SSL Certificates, GeoTrust's DRP includes the CA / Browser Forum requirements as set forth in the GeoTrust Supplemental Procedures, in section 16 of Appendix B1 and C and section 16.4 of Appendix D, respectively.

5.8 CA or RA Termination

In the event that it is necessary for GeoTrust or its CAs to cease operation, GeoTrust makes a commercially reasonable effort to notify Subscribers, Relying Parties, and other affected entities of such termination in advance of the CA termination. Where CA termination is required, 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, and
- Provisions needed for the transition of the CA's services to a successor CA.

5.9 Data Security

For the issuance of EV SSL Certificates, EV Code Signing, and Organization-validated and Domain-validated SSL Certificates, GeoTrust conforms to the CA / Browser Forum requirements for Data Security as set forth in the GeoTrust Supplemental Procedures, in section 16 of Appendix B1, Appendix C and Appendix D, respectively.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

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. 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.

At a minimum, the cryptographic modules used for key generation and storage meet the requirements of FIPS 140-1 level 3. The Root Keys for each CA Certificate are generated and are stored in hardware and are backed up but not escrowed. The Root Keys for each of the CA Certificates may be used for Certificate signing, CRL signing, and off-line CRL signing.

GeoTrust CA Key Pairs are maintained in a trusted and highly secured environment with backup and key recovery procedures.

Supplementary practices in Appendix B and C identify additional requirements for Certificates conforming to the CA/Browser Forum requirements.

6.1.2 Private Key Delivery to Subscriber

Not Applicable

6.1.3 Public Key Delivery to Certificate Issuer

End-user Subscribers and RAs submit their public key to GeoTrust for certification electronically through the use of a PKCS#10 Certificate Signing Request (CSR) or other digitally signed package in a session secured by Secure Sockets Layer (SSL). Where CA, RA, or end-user Subscriber key pairs are generated by GeoTrust, this requirement is not applicable.

6.1.4 CA Public Key Delivery to Relying Parties

GeoTrust makes the CA Certificate available to Subscribers and Relying Parties through their inclusion in 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 sites at *www.geotrust.com/resources, www.RapidSSL.com/legal and www.FreeSSL.com/legal*.

6.1.5 Key Sizes

Key pairs shall be of sufficient length to prevent others from determining the key pair's private key using cryptanalysis during the period of expected utilization of such key pairs. The current GeoTrust Standard for minimum key sizes for its Roots and CAs is the use of key pairs equivalent in strength to 1024 bit RSA or higher.

GeoTrust recommends that Registration Authorities and end-user Subscribers generate 2048 bit RSA key pairs. GeoTrust will continue to approve end entity certificates generated with a key pair size of less than 2048 bit RSA, DSA, ECDSA within a selected group and closed eco system.

6.1.5.1 CABF Requirements for Key Sizes

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the CA /Browser Forum requirements as set forth in the GeoTrust Supplemental Procedures, in section 9.5, Appendix B1, Appendix C and Appendix D, respectively.

GeoTrust Root CA Certificates meet the following requirements for algorithm type and key size:

[1] GeoTrust reserves the right to issue a minimal undisclosed number of SSL server certificates intended to be used by client software other than standard web browsers. These certificates contain a critical EKU extension without the serverAuth flag and with a special flag 2.16.840.1.113733.1.8.54.1 that indicates that it should not be used with standard web browsers

[21]Under special circumstances where the Customers, Subscribers, and/or Relying Parties application do not support key sizes or key pairs of of 2048 bit strength or greater, Symantec reserves the right to issue certificates with non-standard minimum key sizes and key pairs of less than 2048 bit RSA or DSA for PCAs and CAs. Such certificates will have the serverAuth flag removed and a designated OID 2.16.840.1.113733.1.8.54.1 set in the EKU field. The Customers, Subscribers, and Relying Parties will use such certificates at their own risk.

	Validity period beginning on or before 31 Dec 2010	Validity period beginning after 31 Dec 2010
Digest algorithm	MD5 Not Recommended, SHA-1, SHA-256, SHA-384 or SHA-512	SHA-1*, SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	2048**	2048
Minimum DSA modulus size (bits)	N/A	2048
ECC curve	NIST P-256, P-384 or P-521	NIST P-256, P-384 or P-521

Table 4A – Algorithms and key sizes for Root CA Certificates

GeoTrust Subordinate CA Certificates meet the following requirements for algorithm type and key size:

	Validity period beginning on or before 31 Dec 2010 and ending on or before 31 Dec 2013	Validity period beginning after 31 Dec 2010 or ending after 31 Dec 2013
Digest algorithm	SHA-1, SHA-256, SHA-384 or SHA-512	SHA-1*, SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	1024	2048
Minimum DSA modulus size (bits)	N/A	2048
ECC curve	NIST P-256, P-384 or P-521	NIST P-256, P-384 or P-521

Table 4B – Algorithms and key sizes for Subordinate CA Certificates

GeoTrust CAs shall only issue Subscriber certificates with keys containing the following algorithm types and key sizes.

	Validity period ending on or before 31 Dec 2013	Validity period ending after 31 Dec 2013
Digest algorithm	SHA-1*, SHA-256, SHA-384 or SHA-512	SHA-1*, SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	1024	2048
Minimum DSA modulus size (bits)	2048	2048
ECC curve	NIST P-256, P-384 or P-521	NIST P-256, P-384 or P-521

Table 4C – Algorithms and key sizes for Subscriber Certificates

* SHA-1 may be used until SHA-256 is supported widely by browsers used by a substantial portion of relying parties worldwide.
** A Root CA Certificate issued prior to 31 Dec 2010 with an RSA key size less than 2048 bits may still serve as a trust anchor Subscriber Certificates issued in accordance with these Requirements.

GeoTrust CAs shall reject a certificate request if the requested Public Key does meet the minimum algorithm key sizes set forth in this section.

6.1.6 Public Key Parameters Generation and Quality Checking

Not Applicable

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

Refer to section 7.1.2.1

6.2 Private Key Protection and Cryptographic Module Engineering Controls

GeoTrust has implemented a combination of physical, logical, and procedural controls to ensure the security of GeoTrust CA private keys. GeoTrust shall encrypt its Private Key with an algorithm and key-length that, according to the state of the art, are capable of withstanding cryptanalytic attacks for the residual life of the encrypted key or key part. Protection of the Private Key outside the validated cryptographic module must consist of physical security, encryption, or a combination of both, implemented in a manner that prevents disclosure of the Private Key. GeoTrust shall implement physical and logical safeguards to prevent unauthorized certificate issuance.

Subscribers are required by contract to take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of private keys in accordance with section 4.5.1.

6.2.1 Cryptographic Module Standards and Controls

For issuing Root CA key pair generation and CA private key storage, GeoTrust uses hardware cryptographic modules that, at a minimum, are certified at or meet the requirements of FIPS 140-1 Level 3.

6.2.2 Private Key (m of n) Multi-Person Control

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. 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.

The CA Private Key shall be backed up, stored, and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment.

6.2.3 Private Key Escrow

The Root Keys for each CA Certificate are backed up but not escrowed.

6.2.4 Private Key Backup

GeoTrust CA Key Pairs are maintained in a trusted and highly secured environment with backup procedures.

6.2.5 Private Key Archival

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.

6.2.6 Private Key Transfer Into or From Cryptographic Module

Private key transfer into or from a cryptographic module is performed in secure fashion in accordance to manufacturing guidelines of module.

6.2.7 Private Key Storage on Cryptographic Module

Private key storage on cryptographic modules is secure in accordance to manufacturing guidelines of module.

6.2.8 Method of Activating Private Key

All GeoTrust PKI Participants shall protect the activation data for their private keys against loss, theft, modification, unauthorized disclosure, or unauthorized use.

6.2.9 Method of Deactivating Private Key

GeoTrust RA private keys (used for authentication to the RA application) are deactivated upon system log off. GeoTrust RAs are required to log off their workstations when leaving their work area.

Subscribers have an obligation to adequately protect their private key(s).

6.2.10 Method of Destroying Private Key

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.

Cryptographic devices are physically destroyed or zeroized in accordance the manufacturers' guidance prior to disposal.

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

No stipulation.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

A Certificate's period of validity typically begins on the date the Certificate is issued (or such later date as specified in the Certificate), and ends on the date and time it expires as noted in the Certificate unless the Certificate is revoked before its expiration. The Operational Period for key pairs is the same as the Operational Period for the associated Certificates, except that they may continue to be used for decryption and signature verification.

6.3.2.1 CABF Validity Period Requirements

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the CA /Browser Forum requirements as set forth in the GeoTrust Supplemental Procedures, in section 9.4 of Appendix B1, Appendix C and Appendix D, respectively.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

GeoTrust RAs are required to select strong passwords to protect their private keys. Password selection guidelines require that system logon passwords:

• be generated by the user;
• have at least eight characters;
• have at least one alphabetic and one numeric character;
• have at least one lower-case letter;
• not contain many occurrences of the same character;
• not be the same as the operator's profile name; and
• not contain a long substring of the user's profile name.

6.4.2 Activation Data Protection

GeoTrust Shareholders are required to safeguard their Secret Shares and sign an agreement acknowledging their Shareholder responsibilities.

GeoTrust RAs are required to store their Administrator/RA private keys in encrypted form using password protection.

GeoTrust strongly recommends that end-user Subscribers store their private keys in encrypted form and protect their private keys through the use of a hardware token and/or strong passphrase. The use of two factor authentication mechanisms (e.g., token and passphrase, biometric and token, or biometric and passphrase) is encouraged.

6.4.3 Other Aspects of Activation Data

6.4.3.1 Activation Data Transmission

To the extent activation data for private keys are transmitted, GeoTrust CA Participants shall protect the transmission using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys. To the extent Windows or network logon user name/password combination is used as activation data for an end-user Subscriber, the passwords transferred across a network shall be protected against access by unauthorized users.

6.4.3.2 Activation Data Destruction

When applicable, activation data for CA private keys shall be decommissioned using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of the private keys protected by such activation data.

6.5 Computer Security Controls

GeoTrust performs all CA and RA functions using Trustworthy Systems.

6.5.1 Specific Computer Security Technical Requirements

GeoTrust requires the use of passwords that have a minimum character length and a combination of alphanumeric and special characters. GeoTrust requires that passwords be changed on a periodic basis.

6.5.1.1 CABF Requirements for System Security

EV SSL Certificates, EV Code Signing, and domain validated and organization validated SSL Certificates conform to the CA /Browser Forum requirements as set forth in the GeoTrust Supplemental Procedures, in section 16.5 of Appendix B1, Appendix C and Appendix D, respectively.

6.5.2 Computer Security Rating

No Stipulation

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

No Stipulation

6.6.2 Security Management Controls

No Stipulation

6.6.3 Life Cycle Security Controls

No Stipulation

6.7 Network Security Controls

No Stipulation

6.8 Time Stamping

Certificates, CRLs, and other revocation database entries shall contain time and date information. Such time information need not be cryptographic-based.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

GeoTrust Certificates generally conform to (a) ITU-T Recommendation X.509 Version 3 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997, and (b) RFC *5280*: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002 ("RFC *5280*"). Certificate extensions and their criticality, as well as cryptographic algorithm object identifiers, are populated according to the IETF RFC*5280* standards and recommendations. As applicable to the Certificate type, GeoTrust Certificates conform to the current version of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.

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. The policy constraints extensions and policy qualifiers syntax and semantics, when used, conform to the RFC *5280* standards.

EV Certificate content and profile requirements are discussed in Section 6 of Appendix B3 to this CPS.

[27] Geo Trust certificates that do not conform to the current version of the CA/Browser Forum Baseline Requirements that have a key pair and key length size less than 2048bit may have server auth removed and/or a designated OID of 2.16.840.1.113733.1.8.54.1.

7.1.1 Version Number(s)

CA certificates shall be X.509 Version 1 or Version 3 CA Certificates. End-user Subscriber Certificates shall be X.509 Version 3.

7.1.2.1 Key Usage

X.509 Version 3 Certificates are generally populated in accordance with RFC 5280: Internet X.509 Public Key Infrastructure Certificate.

[28]Geo Trust certificates that have a non-standard key pair and key length size of less than 2048bit are authorized to be used within a selected group and closed eco system.

7.1.2.2 Certificate Policies Extension

CertificatePolicies extension of X.509 Version 3 Certificates are not generally used. *CertificatePolicies* extension for EV certificate is populated per Appendix B3 to this CPS.

7.1.2.2.1 CABF Requirement for Certificate Policies Extension

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the CA / Browser Forum requirements as set forth in the GeoTrust Supplemental Procedures, in section 9.3 of Appendix B1, Appendix C, and Appendix D, respectively.

7.1.2.3 Subject Alternative Names

The *subjectAltName* extension of X.509 Version 3 Certificates, when used, is populated in accordance with RFC 5280.

7.1.2.4 Basic Constraints

End-user Subscriber Certificates BasicConstraints extension, shall be populated with a value of an empty sequence.

7.1.2.5 Extended Key Usage

No Stipulation

7.1.2.6 CRL Distribution Points

Most GeoTrust X.509 Version 3 end user Subscriber Certificates and CA Certificates include the *cRLDistributionPoints* extension containing the URL of the location where a Relying Party can obtain a CRL to check the CA Certificate's status.

7.1.2.7 Authority Key Identifier

GeoTrust generally populates the Authority Key Identifier extension of X.509 Version 3 end user Subscriber Certificates and Intermediate CA Certificates.

7.1.2.8 Subject Key Identifier

Where GeoTrust populates X.509 certificates with a *subjectKeyIdentifier* extension, the *keyIdentifier* is based on the public key of the Subject of the Certificate and is generated in accordance with one of the methods described in RFC *5280*.

7.1.3 Algorithm Object Identifiers

Cryptographic algorithm object identifiers, are populated according to the IETF RFC*5280* standards and recommendations.

7.1.4 Name Forms

GeoTrust populates Certificates in accordance with Section 3.1.1. The Issuer Name shall be populated in each Certificate issued containing the Country, Organization Name and the Common Name of the Issuer CA.

7.1.5 Name Constraints

No stipulation

7.1.6 Certificate Policy Object Identifier

Only applicable to EV certificates in accordance with Appendix B3 to this CPS.

7.1.6.1 CABF Requirement for Certificate Policy Object identifier

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the CA / Browser Forum requirements as set forth in the GeoTrust Supplemental Procedures, in section 9.3 of Appendix B1, Appendix C and Appendix D, respectively.

7.1.7 Usage of Policy Constraints Extension

No stipulation

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation

7.2 CRL Profile

As applicable to the Certificate type, corresponding CRLs conform to the current version of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.

7.2.1 Version Number(s)

No stipulation

7.2.2 CRL and CRL Entry Extensions

No stipulation

7.3 OCSP Profile

OCSP (Online Certificate Status Protocol) is a way to obtain timely information about the revocation status of a particular certificate. GeoTrust does not provide OCSP for checking certificate status requests except in the case of True Business ID with EV, True Credentials for Adobe, and My Credential for Adobe.

OCSP responders conform to RFC 2560.

CABF Requirement for OCSP Signing

For EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates, GeoTrust provides OCSP responses as set forth in the GeoTrust Supplemental Procedures, in section 13 of Appendix B1 and C, and section 13.2.5 and Appendix D, respectively.

7.3.1 Version Number(s)

No Stipulation

7.3.2 OCSP Extensions

No Stipulation

8. Compliance Audit and Other Assessments

8.1 Frequency and Circumstances of Assessment

Compliance Audits are conducted at least annually. Audits are conducted over unbroken sequences of audit periods with each period no longer than one year duration.

CABF Requirement for Self-Audits
For EV SSL Certificates, EV Code Signing, and Organization-validated and Domain-validated SSL Certificates, GeoTrust shall conduct self-audits as set forth in the GeoTrust Supplemental Procedures, in section 17.5 of Appendix B1 and C, and section 17.8 of Appendix D, respectively.

8.2 Identity/Qualifications of Assessor

GeoTrust's CA compliance audits are performed by a public accounting firm that:

- Demonstrates proficiency in conducting the WebTrust for Certification Authorities v2.0 or later,
- Demonstrates proficiency in public key infrastructure technology, information security tools and techniques, security auditing, and the third-party attestation function,
- 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.
- Is bound by law, government regulation, or professional code of ethics; and
- maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage.

8.3 Assessors Relationship to Assessed Entity

Compliance audits of GeoTrust's operations are performed by a public accounting firm that is independent of GeoTrust.

8.4 Topics Covered by Assessment

The scope of GeoTrust's annual WebTrust for Certification Authorities v2.0 or later (or equivalent) audit includes CA environmental controls, key management operations and Infrastructure/ Administrative CA controls, certificate life cycle management and CA business practices disclosure.

8.5 Actions Taken as a Result of Deficiency

With respect to compliance audits of GeoTrust's operations, significant exceptions or deficiencies identified during the Compliance 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 GeoTrust CA, a corrective action plan will be developed 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.

8.6 Communications of Results

GeoTrust makes its annual Audit Report publicly available no later than three (3) months after the end of the audit period. In the event of a delay greater than three months, GeoTrust shall provide an explanatory letter signed by the Qualified Auditor. A copy of GeoTrust's WebTrust for CA audit report can be found at from the GeoTrust Website by clicking on the WebTrust Seal.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

GeoTrust, is entitled to charge end-user Subscribers for the issuance, management, and renewal of Certificates.

9.1.2 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.

9.1.3 Revocation or Status Information Access Fees

GeoTrust does not charge a fee as a condition of making the CRLs required by this CPS available in a repository or otherwise available to Relying Parties. GeoTrust is, however, entitled to 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 their repositories by third parties that provide products or services that utilize such Certificate status information without GeoTrust's prior express written consent.

9.1.4 Fees for Other Services

GeoTrust does not charge a fee for access to this CPS. Any use made for purposes other than simply viewing the document, such as reproduction, redistribution, modification, or creation of derivative works, shall be subject to a license agreement with the entity holding the copyright to the document.

9.1.5 Refund Policy

GeoTrust's refund policy is available for review on the GeoTrust web sites at *www.geotrust.com/resources, www.RapidSSL.com/legal or www.FreeSSL.com/legal*. 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.

In most cases, 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.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

GeoTrust, through its parent company, maintains commercial general liability insurance coverage.

9.2.2 Other Assets

Enterprise Customers shall have sufficient financial resources to maintain their operations and perform their duties, and they must be reasonably able to bear the risk of liability to Subscribers and Relying Parties. Symantec's financial resources are set forth in disclosures appearing at: *http://investor.symantec.com/phoenix.zhtml?c=89422&p=irol-irhome*

9.2.3 Extended Warranty Coverage

The GeoSure Protection Plan is an extended warranty program that provides certain GeoTrust certificate subscribers with protection against loss or damage that is due to a defect in GeoTrust's issuance of the certificate or other malfeasance caused by GeoTrust's negligence or breach of its contractual obligations, provided that the subscriber of the certificate has fulfilled its obligations under the applicable service agreement. For general information concerning the GeoSure Protection Plan, and a discussion of which Certificates are covered by it, see *www.geotrust.com/resources/cps/pdfs/GeoSure_Plan_v3.0.pdf*.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

Certain information regarding Subscribers that is submitted on enrolment 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.

9.3.2 Information Not Within the Scope of Confidential Information

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 is not within the scope of confidential information.

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.

9.3.3 Responsibility to Protect Confidential Information

GeoTrust secures private information from compromise and disclosure to third parties.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

GeoTrust has implemented a privacy policy, which is located at: *www.geotrust.com/resources/legal/privacy.asp, www.RapidSSL.com/legal or www.FreeSSL.com/legal*.

9.4.2 Information Treated as Private

Any information about Subscribers that is not publicly available through the content of the issued certificate, certificate directory and online CRLs is treated as private.

9.4.3 Information Not Deemed Private

Subject to local laws, all information made public in a certificate is deemed not private.

9.4.4 Responsibility to Protect Private Information

GeoTrust PKI participants receiving private information shall secure it from compromise and disclosure to third parties and shall comply with all local privacy laws in their jurisdiction.

9.4.5 Notice and Consent to Use Private Information

Unless where otherwise stated in this CPS, the applicable Privacy Policy or by agreement, private information will not be used without the consent of the party to whom that information applies. This section is subject to applicable privacy laws.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

GeoTrust shall be entitled to disclose Confidential/Private Information if, in good faith, GeoTrust believes that:

- disclosure is necessary in response to subpoenas and search warrants.
- disclosure is necessary in response to judicial, administrative, or other legal process during the discovery process in a civil or administrative action, such as subpoenas, interrogatories, requests for admission, and requests for production of documents.

This section is subject to applicable privacy laws.

9.4.7 Other Information Disclosure Circumstances

No Stipulation

9.5 Intellectual Property Rights

The allocation of Intellectual Property Rights among GeoTrust PKI Participants other than Subscribers and Relying Parties is governed by the applicable agreements among such GeoTrust PKI Participants. The following subsections of Section 9.5 apply to the Intellectual Property Rights in relation to Subscribers and Relying Parties.

9.5.1 Property Rights in Certificates and Revocation Information

CAs retain all Intellectual Property Rights in and to the Certificates and revocation information that they issue. GeoTrust and customers grant permission to reproduce and distribute Certificates on a nonexclusive royalty-free basis, provided that they are reproduced in full. GeoTrust and customers shall grant permission to use revocation information to perform Relying Party functions subject to the applicable CRL Usage Agreement or any other applicable agreements.

9.5.2 Property Rights in the CPS

GeoTrust PKI Participants acknowledge that GeoTrust retains all Intellectual Property Rights in and to this CPS.

9.5.3 Property Rights in Names

A Certificate Applicant retains all rights it has (if any) in any trademark, service mark, or trade name contained in any Certificate Application and distinguished name within any Certificate issued to such Certificate Applicant.

9.5.4 Property Rights in Keys and Key Material

Key pairs corresponding to Certificates of CAs and end-user Subscribers are the property of the CAs and end-user Subscribers that are the respective Subjects of these Certificates, regardless of the physical medium within which they are stored and protected, and such persons retain all Intellectual Property Rights in and to these key pairs. Without limiting the generality of the foregoing, GeoTrust's root public keys and the root Certificates containing them, including all self-signed Certificates, are the property of GeoTrust. GeoTrust licenses software and hardware manufacturers to reproduce such root Certificates to place copies in trustworthy hardware devices or software.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

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 (with the exception of True Credentials and True Credential Express Client Certificates). The nature of the steps GeoTrust takes to verify the information contained in a Certificate is set forth in this CPS.

9.6.1.1 CABF Warranties and Obligations

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the CA / Browser Forum requirements as set forth in the GeoTrust Supplemental Procedures, in sections 7.1 and 18 of Appendix B1 and C, and sections 7.1 (CA Warranties) and 18.3 (Root CA Obligations) of Appendix D, respectively.

9.6.2 RA Representations and Warranties

RAs warrant that:

- There are no material misrepresentations of fact in the Certificate known or originating from the entities approving the Certificate Application or issuing the Certificate,
- There are no errors in the information in the Certificate that were introduced by entities approving the Certificate Application as a result of a failure to reasonable care in managing the Certificate Application,
- Their Certificates meet all material requirements of this CPS, and
- Revocation services (when applicable) and use of a repository comply with the applicable CPS in all material aspects.

Subscriber Agreements may include additional representations and warranties.

9.6.3 Subscriber Representations and Warranties

Subscribers warrant that:

- Each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the Subscriber and the Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created,
- Their private key is protected and that no unauthorized person has ever had access to the Subscriber's private key; further, the Subscriber shall immediately request revocation of a certificate if the related private key is compromised,
- All representations made by the Subscriber in the Certificate Application the Subscriber submitted are true,
- All information supplied by the Subscriber and contained in the Certificate is true,
- The Certificate is being used exclusively for authorized and legal purposes, consistent with this CPS, and
- The Subscriber is an end-user Subscriber and not a CA, and is not using the private key corresponding to any public key listed in the Certificate for purposes of digitally signing any Certificate (or any other format of certified public key) or CRL, as a CA or otherwise.

Subscriber Agreements may include additional representations and warranties.

9.6.4 Relying Party Representations and Warranties

Relying Parties acknowledge that they have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a Certificate, that they are solely responsible for deciding whether or not to rely on such information, and that they shall bear the legal consequences of their failure to perform the Relying Party obligations in terms of this CPS.

9.6.5 Representations and Warranties of Other Participants

No stipulation

9.7 Disclaimer of Warranties

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall disclaim GeoTrust's possible warranties, including any warranty of merchantability or fitness for a particular purpose, outside the context of the GeoSure Protection Plan.

9.8 Limitation of Liability

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall disclaim GeoTrust liability outside the context of the GeoSure Protection Plan. To the extent GeoTrust has issued and managed the Certificate(s) at issue in compliance with its Certification Practice Statement, GeoTrust shall have no liability to the Subscriber, any Relying Party, or any other third parties for any damages or losses suffered as a result of the use or reliance on such Certificate(s).

The liability (and/or limitation thereof) of Subscribers shall be as set forth in the applicable Subscriber agreements.

The liability (and/or limitation thereof) of enterprise RAs and the applicable CA shall be set out in the agreement(s) between them.

The liability (and/or limitation thereof) of Relying Parties shall be as set forth in the applicable Relying Party Agreements.

9.9 Indemnities

9.9.1 Indemnification by Subscribers

To the extent permitted by applicable law, Subscriber are required to indemnify GeoTrust for:

- Falsehood or misrepresentation of fact by the Subscriber on the Subscriber's Certificate Application,
- Failure by the Subscriber to disclose a material fact on the Certificate Application, if the misrepresentation or omission was made negligently or with intent to deceive any party,
- The Subscriber's failure to protect the Subscriber's private key, to use a Trustworthy System, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's private key, or
- The Subscriber's use of a name (including without limitation within a common name, domain name, or e-mail address) that infringes upon the Intellectual Property Rights of a third party.

The applicable Subscriber Agreement may include additional indemnity obligations.

9.9.2 Indemnification by Relying Parties

To the extent permitted by applicable law, Relying Parties shall indemnify GeoTrust for:

- The Relying Party's failure to perform the obligations of a Relying Party,
- The Relying Party's reliance on a Certificate that is not reasonable under the circumstances, or
- The Relying Party's failure to check the status of such Certificate to determine if the Certificate is expired or revoked.

9.9.3 Indemnification of Application Software Suppliers

Notwithstanding any limitations on its liability to Subscribers and Relying Parties, the CA understands and acknowledges that the Application Software Suppliers who have a Root Certificate distribution agreement in place with the GeoTrust Root CA do not assume any obligation or potential liability of the CA under these Requirements or that otherwise might exist because of the issuance or maintenance of Certificates or reliance thereon by Relying Parties or others.

Thus the CA shall defend, indemnify, and hold harmless each Application Software Supplier for any and all claims, damages, and losses suffered by such Application Software Supplier related to a Certificate issued by the CA, regardless of the cause of action or legal theory involved. This does not apply, however, to any claim, damages, or loss suffered by such Application Software Supplier related to a Certificate issued by the CA where such claim, damage, or loss was directly caused by such Application Software Supplier's software displaying as not trustworthy a Certificate that is still valid, or displaying as trustworthy: (1) a Certificate that has expired, or (2) a Certificate that has been revoked (but only in cases where the revocation status is currently available from the CA online, and the application software either failed to check such status or ignored an indication of revoked status).

9.10 Term and Termination

9.10.1 Term

The CPS becomes effective upon publication in the GeoTrust repository. Amendments to this CPS become effective upon publication in the GeoTrust repository.

9.10.2 Termination

This CPS as amended from time to time shall remain in force until it is replaced by a new version.

9.10.3 Effect of Termination and Survival

Upon termination of this CPS, GeoTrust PKI Participants are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

9.11 Individual Notices and Communications with Participants

Unless otherwise specified by agreement between the parties, GeoTrust PKI Participants shall use commercially reasonable methods to communicate with each other, taking into account the criticality and subject matter of the communication.

9.12 Amendments

9.12.1 Procedure for Amendment

GeoTrust may change this CPS at any time without prior notice. The CPS and any amendments thereto are available through *www.geotrust.com/resources, www.RapidSSL.com/legal or www.FreeSSL.com/legal*. Amendments to this CPS will be evidenced by a new version number and date, except where the amendments are purely clerical.

9.12.2 Notification Mechanism and Period

No stipulation

9.12.2.1 Comment Period

Not applicable

9.12.2.2 Mechanism to Handle Comments

Not applicable

9.12.3 Circumstances under Which OID must be Changed

Not applicable

9.13 Dispute Resolution Provisions

9.13.1 Disputes among GeoTrust, Affiliates and Customers

Disputes among GeoTrust PKI participants shall be resolved pursuant to provisions in the applicable agreements among the parties.

9.13.2 Disputes with End-User Subscribers or Relying Parties

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 Santa Clara County, California, United States of America. 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.

9.14 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 California, 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

9.15 Compliance with Applicable Law

This CPS is subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information. Symantec licenses its CAs in each jurisdiction that it operates where licensing is required by the law of such jurisdiction for the issuance of Certificates.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

Not Applicable

9.16.2 Assignment

Not Applicable

9.16.3 Severability

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

9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)

Not Applicable

9.16.5 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.

9.17 Other Provisions

Not Applicable

Appendices

Appendix A: Table of Acronyms and Definitions

Table of Acronyms

Term	Definition
AICPA	American Institute of Certified Public Accountants.
ANSI	The American National Standards Institute.
ACS	Authenticated Content Signing
BIS	The United States Bureau of Industry and Science of the United States Department of Commerce
CA	Certificate Authority
ccTLD	Country Code Top-Level Domain
CICA	Canadian Instituted of Chartered Accountants
CP	Certificate Policy
CPS	Certificate Practice Statement
CRL	Certificate Revocation List
DBA	Doing Business As
DNS	Domain Name System
DV	Domain Validated (Certificate)
EAL	Evaluation Assurance Level
EV	Extended Validation
FIPS	United State Federal Information Processing Standards.
FQDN	Fully Qualified Domain Name
ICC	International Chamber of Commerce.
IM	Instant Messaging
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ISO	International Organization for Standardization
LSVA	Logical security vulnerability assessment.
NIST	(US Government) National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol.
OID	Object Identifier
OV	Organization Validated (Certificate)
PCA	Primary Certification Authority.
PIN	Personal identification number.
PKCS	Public-Key Cryptography Standard.
PKI	Public Key Infrastructure.
PMA	Policy Management Authority.
QGIS	Qualified Government Information Source
QIIS	Qualified Independent Information Source
RA	Registration Authority.
RFC	Request for comment.
S/MIME	Secure multipurpose Internet mail extensions.
SSL	Secure Sockets Layer.
TLD	Top-Level Domain
TLS	Transport Layer Security
VOID	Voice Over Internet Protocol

Definitions

Term	Definition
Administrator	A Trusted Person within the organization that performs validation and other CA or RA Functions.
Administrator Certificate	A Certificate issued to an Administrator that may only be used to perform CA or RA functions.
Affiliate	A leading trusted third party, for example in the technology, telecommunications, or financial services industry, that has entered into an agreement with GeoTrust as a distribution and services channel within a specific territory. In the CAB Forum context, the term "*Affiliate*" refers to: A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.
Applicant	The Private Organization or Government Entity that applies for (or seeks renewal of) an EV Certificate naming it as the Subject.
Applicant Representative	An individual person employed by the Applicant for an EV certificate: (i) who signs and submits, or approves an EV Certificate Request on behalf of an Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of an Applicant.
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.
Attestation Letter	A letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information.
Audit Report	A report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the mandatory provisions of these Requirements.
Certificate	A message that, at least, states a name or identifies the CA, identifies the Subscriber, contains the Subscriber's public key, identifies the Certificate's Operational Period, contains a Certificate serial number, and is digitally signed by the CA.
Certificate Applicant	An individual or organization that requests the issuance of a Certificate by a CA.
Certificate Application	A request from a Certificate Applicant (or authorized agent of the Certificate Applicant) to a CA for the issuance of a Certificate.
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 of an EV Certificate 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.
Certificate Chain	An ordered list of Certificates containing an end-user Subscriber Certificate and CA Certificates, which terminates in a root Certificate.
Certificate Data	Certificate requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA's possession or control or to which the CA has access.
Certificate Management Control Objectives	Criteria that an entity must meet in order to satisfy a Compliance Audit.
Certificate Management Process	Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.
Certificate Policy	A set of rules that indicates teh applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.
Certificate Problem Report	Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates
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 Revocation List (CRL)	A periodically (or exigently) issued list, digitally signed by a CA, of identified Certificates that have been revoked prior to their expiration dates in accordance with CP § 3.4. The list generally indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the revoked Certificates' serial numbers, and the specific times and reasons for revocation.
Certificate Signing Request	A message conveying a request to have a Certificate issued.
Certification Authority (CA)	An entity authorized to issue, manage, revoke, and renew Certificates.
Certificate Practices Statement (CPS)	A statement of the practices that GeoTrust or an Affiliate employs in approving or rejecting Certificate Applications and issuing, managing, and revoking Certificates.
Challenge Phrase	A secret phrase chosen by a Certificate Applicant during enrolment for a Certificate. When issued a Certificate, the Certificate Applicant becomes a Subscriber and a CA or RA can use the Challenge Phrase to authenticate the Subscriber when the Subscriber seeks to revoke or renew the Subscriber's Certificate.
Class	A specified level of assurances as defined within the CP. See CP § 1.1.1.
Code Confirmation Certificate	A Certificate issued by GeoTrust in order for GeoTrust to use the associated Private Key to digitally resign enrollment form code which has been digitally signed by a Publisher Certificate Private Key, upon request of code confirmation from the Publisher.
Compromise	A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred. With respect to private keys, a Compromise is a loss, theft, disclosure, modification, unauthorized use, or other compromise of the security of such private key.
Confidential/Private Information	Information required to be kept confidential and private pursuant to CP § 2.8.1.
Contract Signer	A Contract Signer is a natural person who is employed by the Applicant, or an authorized the Applicant to sign Subscriber Agreements on behalf of the Applicant for an EV Certificate.
Country	A Country shall mean a Sovereign state as defined in the Guidelines.
Cross Certificate	A certificate that is used to establish a trust relationship between two Root CAs.
CRL Usage Agreement	An agreement setting forth the terms and conditions under which a CRL or the information in it can be used.
Delegated Third Party	A natural person or Legal Entity that is not the CA but is authorized by the CA to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.
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.
Domain Authorization	Correspondence or other documentation provided by a Domain Name Registrant attesting to the authority of an Applicant to request a Certificate for a specific Domain Namespace.
Domain Name	The label assigned to a node in the Domain Name System.
Domain Namespace	The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.
Domain Name Registrant	Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.
Domain Name Registrar	A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).
Enterprise RA	An employee or agent of an organization unaffiliated with teh CA who authorizes issuance of Certificates to that organization.

Expiry Date	The "Not After" date in a Certificate that defines the end of a Certificate's validity period.
EV Certificate:	A digital certificate that contains information specified in the EV Guidelines and that has been validated in accordance with the Guidelines.
EV OID	An identifying number, called an "object identifier," that is included in the certificatePolicies field of an EV certificate that: (i) indicates which CA policy statement relates to that certificate, and which, (ii) by pre-agreement with one or more Application Software Vendor, marks the certificate as being an EV Certificate.
Exigent Audit/ Investigation	An audit or investigation by GeoTrust where GeoTrust has reason to believe that an entity's failure to meet GeoTrust CA Standards, an incident or Compromise relating to the entity, or an actual or potential threat to the security of the GeoTrust CA posed by the entity has occurred.
Extended Validation	Validation Procedures defined by the Guidelines for Extended Validation Certificates published by a forum consisting of major certification authorities and browser vendors.
Fully-Qualified Domain Name	A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.
Government Entity	A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).
Intellectual Property Rights	Rights under one or more of the following: any copyright, patent, trade secret, trademark, and any other intellectual property rights.
Intermediate Certification Authority (Intermediate CA)	A Certification Authority whose Certificate is located within a Certificate Chain between the A Certification Authority whose Certificate is located within a Certificate Chain between the end-user Subscriber's Certificate.
International Organization	An International Organization is an organization founded by a constituent document, e.g., charter, treaty, convention, or similar document, signed by, or on behalf of, a minimum of two or more Sovereign State governments.
Internal Server Name	A Server Name (which may or may not include an Unregistered Domain Name) that is not resolvable using the public DNS.
Issuing CA	In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.
Key Compromise	A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, an unauthorized person has had access to it, or there exists a practical technique by which an unauthorized person may discover its value.
Key Generation Ceremony	A procedure whereby a CA's or RA's key pair is generated, its private key is transferred into a cryptographic module, its private key is backed up, and/or its public key is certified.
Key Generation Script	A documented plan of procedures for the generation of a CA Key Pair.
Key Pair	The Private Key and its associated Public Key.
Legal Entity	An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.
Nonverified Subscriber Information	Information submitted by a Certificate Applicant to a CA or RA, and included within a Certificate, that has not been confirmed by the CA or RA and for which the applicable CA and RA provide no assurances other than that the information was submitted by the Certificate Applicant.
Non-repudiation	An attribute of a communication that provides protection against a party to a communication falsely denying its origin, denying that it was submitted, or denying its delivery. Denial of origin includes the denial that a communication originated from the same source as a sequence of one or more prior messages, even if the identity associated with the sender is unknown. Note: only an adjudication by a court, arbitration panel, or other tribunal can ultimately prevent repudiation. For example, a digital signature verified with reference to a GeoTrust Certificate may provide proof in support of a determination of Non-repudiation by a tribunal, but does not by itself constitute Non-repudiation.
Object Identifier	A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.
OCSP (Online Certificate Status	An online Certificate-checking protocol for providing Relying Parties with real-time Certificate status information.

Protocol)	
OCSP Responder	An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.
Offline CA	GeoTrust PCAs, Issuing Root CAs and other designated intermediate CAs that are maintained offline for security reasons in order to protect them from possible attacks by intruders by way of the network. These CAs do not directly sign end user Subscriber Certificates.
Online CA	CAs that sign end user Subscriber Certificates are maintained online so as to provide continuous signing services.
Online Certificate Status Protocol (OCSP)	A protocol for providing Relying Parties with real-time Certificate status information.
Operational Period	The period starting with the date and time a Certificate is issued (or on a later date and time certain if stated in the Certificate) and ending with the date and time on which the Certificate expires or is earlier revoked.
Parent Company	A parent company is defined as a company that owns a majority of the Subsidiary Company and this can be verified by referencing a QIIS or from financial statement supplied by a registered Chartered Professional Accountant (CPA) or equivalent outside of the USA.
PKCS #10	Public-Key Cryptography Standard #10, developed by RSA Security Inc., which defines a structure for a Certificate Signing Request.
PKCS #12	Public-Key Cryptography Standard #12, developed by RSA Security Inc., which defines a secure means for the transfer of private keys.
Primary Certification Authority (PCA)	A CA that acts as a root CA for a specific Class of Certificates, and issues Certificates to CAs subordinate to it.
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.
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.
Public Key Infrastructure	The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based public key cryptographic system.
Publicly-Trusted Certificate	A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software.
Qualified Auditor	A natural person or Legal Entity that meets the requirements of Section 17.6 (Auditor Qualifications).
Registered Domain Name	A Domain Name that has been registered with a Domain Name Registrar.
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).
Registration Authority (RA)	An entity approved by a CA to assist Certificate Applicants in applying for Certificates, and to approve or reject Certificate Applications, revoke Certificates, or renew Certificates.

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.
Reliable Method of Communication	A method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative.
Relying Party	An individual or organization that acts in reliance on a certificate and/or a digital signature.
Relying Party Agreement	An agreement used by a CA setting forth the terms and conditions under which an individual or organization acts as a Relying Party.
Repository	An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.
Reseller	An entity marketing services on behalf of GeoTrust or an Affiliate to specific markets.
Reserved IP Address	An IPv4 or IPv6 address that the IANA has marked as reserved: http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml
Root CA	The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.
Root Certificate	The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.
RSA	A public key cryptographic system invented by Rivest, Shamir, and Adelman.
RSA Secure Server Certification Authority (RSA Secure Server CA)	The Certification Authority that issues Secure Server IDs.
RSA Secure Server Hierarchy	The PKI hierarchy comprised of the RSA Secure Server Certification Authority.
Secret Share	A portion of a CA private key or a portion of the activation data needed to operate a CA private key under a Secret Sharing arrangement.
Secret Sharing	The practice of splitting a CA private key or the activation data to operate a CA private key in order to enforce multi-person control over CA private key operations under CP § 6.2.2.
Secure Server ID	A Class 3 organizational Certificate used to support SSL sessions between web browsers and web servers.
Secure Sockets Layer (SSL)	The industry-standard method for protecting Web communications developed by Netscape Communications Corporation. The SSL security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a Transmission Control Protocol/Internet Protocol connection.
Sovereign State	A Sovereign state is a state, or country, that administers its own government, and is not dependent upon, or subject to, another power.
Subject	The holder of a private key corresponding to a public key. The term “Subject” can, in the case of an organizational Certificate, refer to the equipment or device that holds a private key. A Subject is assigned an unambiguous name, which is bound to the public key contained in the Subject’s Certificate.
Subject Identity Information	Information that identifies the Certificate Subject. Subject Identity Information does not include a domain name listed in the *subjectAltName* extension or the Subject *commonName* field.
Subordinate CA	A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.
Subscriber	In the case of an individual Certificate, a person who is the Subject of, and has been issued, a Certificate. In the case of an organizational Certificate, an organization that owns the equipment or device that is the Subject of, and that has been issued, a Certificate. A Subscriber is capable of using, and is authorized to use, the private key that corresponds to the public key listed in the Certificate.
Subscriber Agreement	An agreement used by a CA or RA setting forth the terms and conditions under which an individual or organization acts as a Subscriber.

Subsidiary Company	A subsidiary company is defined as a company that is majority 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.
Symantec	Means, with respect to each pertinent portion of this CPS, Symantec Corporation and/or any wholly owned Symantec subsidiary responsible for the specific operations at issue.
Terms of Use	Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with these Requirements when the Applicant/Subscriber is an Affiliate of the CA.
Trusted Person	An employee, contractor, or consultant of an entity within GeoTrust responsible for managing infrastructural trustworthiness of the entity, its products, its services, its facilities, and/or its practices as further defined in CP § 5.2.1.
Trusted Position	The positions within GeoTrust that must be held by a Trusted Person.
Trustworthy System	Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy. A trustworthy system is not necessarily a “trusted system” as recognized in classified government nomenclature.
Unregistered Domain Name	A Domain Name that is not a Registered Domain Name.
Valid Certificate	A Certificate that passes the validation procedure specified in RFC 5280.
Validation Specialists	Someone who performs the information verification duties specified by these Requirements.
Validity Period	The period of time measured from the date when the Certificate is issued until the Expiry Date.
Wildcard Certificate	A Certificate containing an asterisk (*) in the left-most position of any of the Subject Fully-Qualified Domain Names contained in the Certificate.

Appendix B1:

Supplemental Validation Procedures for Extended Validation (EV) SSL Certificates

Reference: *CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation (EV) Certificates, www.cabforum.org* .

Table of Contents

1. INTRODUCTION

This Appendix articulates supplemental procedures to GeoTrust's CPS for issuing Extended Validation Certificates ("EV Certificates") in conformance with the Guidelines for Extended Validation Certificates ("Guidelines"), published by the CA Browser Forum at *www.cabforum.org*, that describe certain of the minimum requirements that a Certificate Authority (CA) must meet in order to issue Extended Validation Certificates ("EV Certificates"). This Appendix addresses EV Certificates used for SSL/TLS authentication on the Internet.

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 a trustworthy confirmation of the identity of the entity that controls the website they are accessing.

2. BASIC CONCEPT OF THE EV CERTIFICATE

2.1 Purpose of EV SSL Certificates.

EV Certificates are intended for establishing Web-based data communication conduits via the TLS/SSL protocols and for verifying the authenticity of executable code.

2.1.1 Primary Purposes

The primary purposes of an EV Certificate are to:

□□□□**Identify the legal entity that controls a Web site:** Provide a reasonable assurance to the user of an Internet browser that the Web site 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 or other disambiguating information; and

□□□□**Enable encrypted communications with a Web site:** 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 Web site.

2.1.2 Secondary Purposes

The secondary purposes of an EV Certificate are to help establish the legitimacy of a business claiming to operate a Web site or distribute executable code, and to provide a vehicle that can be used to assist in addressing problems related to phishing, malware, and other forms of online identity fraud. By providing more reliable third-party verified identity and address information regarding the business, EV Certificates may help to:

□□□□Make it more difficult to mount phishing and other online identity fraud attacks using 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 to users; and

□□□□Assist law enforcement organizations in their investigations of phishing and other online identity fraud, including where appropriate, contacting, investigating, or taking legal action against the Subject. 7

2.1.3 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 References

See Baseline Requirements, which are available at www.cabforum.org.

4 Definitions

Capitalized Terms are defined in the Baseline Requirements except where provided below:

Accounting Practitioner: A certified public accountant, chartered accountant, or a person with an equivalent license within the country of the Applicant's Jurisdiction of Incorporation or Registration or any jurisdiction where the Applicant maintains an office or physical facility; provided that an accounting standards body in the jurisdiction maintains full (not "suspended" or "associate") membership status with the International Federation of Accountants.

Baseline Requirements: The Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates as published by the CA/Browser Forum and any amendments to such document.

Business Entity: Any entity that is neither a Private Organization nor a Government Entity as defined herein. Examples include general partnerships, unincorporated associations, and sole proprietorships.

Certificate Approver: A natural person who is either the Applicant, 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.

Certificate Requester: A natural person who is either the Applicant, employed by the Applicant, 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.

Confirmation Request: An appropriate out-of-band communication requesting verification or confirmation of the particular fact at issue.

Confirming Person: A position within an Applicant's organization that confirms the particular fact at issue.

Contract Signer: A natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant, and who has authority on behalf of the Applicant to sign Subscriber Agreements.

Control: "Control" (and its correlative meanings, "controlled by" and "under common control with") means possession, directly or indirectly, of the power to: (1) direct the management, personnel, finances, or plans of such entity; (2) control the election of a majority of the directors; or (3) vote that portion of voting shares required for "control" under the law of the entity's Jurisdiction of Incorporation or Registration but in no case less than 10%.

Country: A Country shall mean a Sovereign State as defined in these Guidelines.

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 share draft account, a current account, or a checking account. 8

Domain Authorization Document: Documentation provided by, or a CA's documentation of a communication with, the domain name registrar or the person or entity listed in WHOIS as the registering the domain name (including any private, anonymous, or proxy registration service) attesting that the Applicant has the exclusive right to use the specified domain name.
Enterprise EV Certificate: An EV Certificate that an Enterprise RA authorizes the CA to issue at third and higher domain levels.
Enterprise EV RA: An RA that is authorized by the CA to authorize the CA to issue EV Certificates at third and higher domain levels.
EV Authority: A source other than the Certificate Approver, through which verification occurs that the Certificate Approver is expressly authorized by the Applicant, as of the date of the EV Certificate Request, to take the Request actions described in these Guidelines.
EV Certificate: A certificate that contains subject information specified in these Guidelines and that has been validated in accordance with these Guidelines.
EV Certificate Beneficiaries: Persons to whom the CA and its Root CA make specified EV Certificate Warranties.
EV Certificate Renewal: The process whereby an Applicant who has a valid unexpired and non-revoked EV Certificate makes an application, to the CA that issued the original certificate, for a newly issued EV Certificate for the same organizational name and Domain Name prior to the expiration of the Applicant's existing EV Certificate but with a new 'valid to' date beyond the expiry of the current EV Certificate.
EV Certificate Reissuance: The process whereby an Applicant who has a valid unexpired and non-revoked EV Certificate makes an application, to the CA that issued the original certificate, for a newly issued EV Certificate for the same organizational name and Domain Name prior to the expiration of the Applicant's existing EV Certificate but with a 'valid to' date that matches that of the current EV Certificate.
EV Certificate Request: A request from an Applicant to the CA requesting that the CA issue an EV Certificate to the Applicant, which request is validly authorized by the Applicant and signed by the Applicant Representative.
EV Certificate Warranties: In conjunction with the CA issuing an EV Certificate, the CA and its Root CA, during the period when the EV Certificate is Valid, promise that the CA has followed the requirements of these Guidelines and the CA's EV Policies in issuing the EV Certificate and in verifying the accuracy of the information contained in the EV Certificate.
EV OID: An identifying number, in the form of an "object identifier," that is included in the *certificatePolicies* field of a certificate that: (i) indicates which CA policy statement relates to that certificate, and (ii) by pre-agreement with one or more Application Software Supplier, marks the certificate as being an EV Certificate.
EV Policies: Auditable EV Certificate practices, policies and procedures, such as a certification practice statement and certificate policy, that are developed, implemented, and enforced by the CA and its Root CA.
EV Processes: The keys, software, processes, and procedures by which the CA verifies Certificate Data under this Guideline, issues EV Certificates, maintains a Repository, and revokes EV Certificates.
Extended Validation Certificate: See EV Certificate.
Government Agency: In the context of a Private Organization, the government agency in the Jurisdiction of Incorporation under whose authority the legal existence of Private Organizations is established (e.g., the government agency that issued the Certificate of Incorporation). In the context of Business Entities, the government agency in the jurisdiction of operation that registers business entities. In the case of a Government Entity, the entity that enacts law, regulations, or decrees establishing the legal existence of Government Entities.

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.).
Guidelines: This document.
Incorporating Agency: In the context of a Private Organization, the government agency in the Jurisdiction of Incorporation under whose authority the legal existence of Private Organizations is established (e.g., the government agency that issues Certificates of Incorporation). In the context of a Government Entity, the entity that enacts law, regulations, or decrees establishing the legal existence of Government Entities. 9

Independent Confirmation From Applicant: Confirmation of a particular fact received by the CA pursuant to the provisions of the Guidelines or binding upon the Applicant.
Individual: A natural person.
International Organization: An organization founded by a constituent document, e.g., a charter, treaty, convention or similar document, signed by, or on behalf of, a minimum of two Sovereign State governments.
Jurisdiction of Incorporation: In the context of a Private Organization, the country and (where applicable) the state or province or locality 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 context of a Government Entity, the country and (where applicable) the state or province where the Entity's legal existence was created by law.
Jurisdiction of Registration: In the case of a Business Entity, the state, province, or locality where the organization has registered its business presence by means of filings by a Principal Individual involved in the business.
Latin Notary: A person with legal training whose commission under applicable law not only includes authority to authenticate the execution of a signature on a document but also responsibility for the correctness and content of the document. A Latin Notary is sometimes referred to as a Civil Law Notary.
Legal Existence: A Private Organization, Government Entity, or Business Entity has Legal Existence if it has been validly formed and not otherwise terminated, dissolved, or abandoned.
Legal Practitioner: A person who is either a lawyer or a Latin Notary as described in these Guidelines and competent to render an opinion on factual claims of the Applicant.
Maximum Validity Period: 1. The maximum time period for which the issued EV Certificate is valid. 2. The maximum period after validation by the CA that certain Applicant information may be relied upon in issuing an EV Certificate pursuant to these Guidelines.
Notary: A person whose commission under applicable law includes authority to authenticate the execution of a signature on a document.
Parent Company: A company that Controls a Subsidiary Company.
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: An individual of a Private Organization, Government Entity, or Business Entity that is either an owner, partner, managing member, director, or officer, 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 Organization: A non-governmental legal entity (whether ownership interests are privately held or publicly traded) whose existence was created by a filing with (or an act of) the Incorporating Agency in its Jurisdiction of Incorporation.
Qualified Auditor: An independent public accounting firm that meets the auditing qualification requirements specified in Section 17.6 of these Guidelines.
Qualified Government Information Source: A database maintained by a Government Entity (e.g. SEC filings) that meets the requirements of Section 11.10.6.
Qualified Government Tax Information Source: A Qualified Governmental Information Source that specifically contains tax information relating to Private Organizations, Business Entities, or Individuals.
Qualified Independent Information Source: A regularly-updated and current, 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.
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 to (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 Office of the Comptroller of the Currency or Office of Thrift Supervision. 10

Registered Agent: An individual or entity that is: (i) authorized by the Applicant to receive service of process and business communications on behalf of the Applicant; and (ii) listed in the official records of the Applicant's Jurisdiction of Incorporation as acting in the role specified in (i) above.
Registered Office: The official address of a company, as recorded with the Incorporating Agency, to which official documents are sent and at which legal notices are received.
Registration Number: The unique number assigned to a Private Organization by the Incorporating Agency in such entity's Jurisdiction of Incorporation.
Regulated Financial Institution: A financial institution that is regulated, supervised, and examined by governmental, national, state or provincial, or local authorities.
Root Key Generation Script: A documented plan of procedures to be performed for the generation of the Root CA Key Pair**.**
Signing Authority: One or more Certificate Approvers designated to act on behalf of the Applicant.
Sovereign State: A state or country that administers its own government, and is not dependent upon, or subject to, another power.
Subsidiary Company: A company that is controlled by a Parent Company.
Superior Government Entity: Based on the structure of government in a political subdivision, the Government Entity or Entities that have the ability to manage, direct and control the activities of the Applicant.
Suspect code: Code that contains malicious functionality or serious vulnerabilities, including spyware, malware and other code that installs without the user's consent and/or resists its own removal, and code that can be exploited in ways not intended by its designers to compromise the trustworthiness of the platforms on which it executes.
Translator: An individual or Business Entity that possesses the requisite knowledge and expertise to accurately translate the words of a document written in one language to the native language of the CA.
Verified Accountant Letter: A document meeting the requirements specified in Section 11.10.2 of these Guidelines
Verified Legal Opinion: A document meeting the requirements specified in Section 11.10.1 of these Guidelines.
WebTrust EV Program: The additional audit procedures specified for CAs that issue EV Certificates by the AICPA/CICA to be used in conjunction with its WebTrust Program for Certification Authorities.
WebTrust Program for CAs: The then-current version of the AICPA/CICA WebTrust Program for Certification Authorities.
WebTrust Seal of Assurance: An affirmation of compliance resulting from the WebTrust Program for CAs.

5 Abbreviations and Acronyms

Abbreviations and Acronyms are defined in the Baseline Requirements except as otherwise defined herein:
BIPM International Bureau of Weights and Measures
BIS (US Government) Bureau of Industry and Security
CEO Chief Executive Officer
CFO Chief Financial Officer
CIO Chief Information Officer
CISO Chief Information Security Officer
COO Chief Operating Officer
CPA Chartered Professional Accountant
CSO Chief Security Officer
EV Extended Validation

gTLD Generic Top-Level Domain 11

IFAC International Federation of Accountants
IRS Internal Revenue Service
ISP Internet Service Provider
QGIS Qualified Government Information Source
QTIS Qualified Government Tax Information Source
QIIS Qualified Independent Information Source
SEC (US Government) Securities and Exchange Commission
UTC(k) National realization of Coordinated Universal Time

6 Conventions

Terms not otherwise defined in these Guidelines shall be as defined in applicable agreements, user manuals, certification practice statements (CPS), and certificate policies (CP) of the CA issuing EV Certificates.

The key words "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in these Guidelines shall be interpreted in accordance with RFC 2119.

7 Certificate Warranties and Representations

7.1 EV Certificate Warranties

When the CA issues an EV Certificate, the CA and its Root CA represent and warrant to the Certificate Beneficiaries listed in Section 7.1.1 of the Baseline Requirements, during the period when the EV Certificate is Valid, that the CA has followed the requirements of these Guidelines and its EV Policies in issuing and managing the EV Certificate and in verifying the accuracy of the information contained in the EV Certificate. The EV Certificate Warranties specifically include, but are not limited to, the following:

(A) **Legal Existence:** The CA 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;

(B) **Identity:** The CA 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;

(C) **Right to Use Domain Name:** The CA has taken all steps reasonably necessary to verify that, as of the date the EV Certificate was issued, the Subject named in the EV Certificate has the exclusive right to use all the Domain Name(s) listed in the EV Certificate;

(D) **Authorization for EV Certificate:** The CA has taken all steps reasonably necessary to verify that the Subject named in the EV Certificate has authorized the issuance of the EV Certificate;

(E) **Accuracy of Information:** The CA 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;

(F) **Subscriber Agreement:** The Subject named in the EV Certificate has entered into a legally valid and enforceable Subscriber Agreement with the CA that satisfies the requirements of these Guidelines or, if they are affiliated, the Applicant Representative has acknowledged and accepted the Terms of Use;

(G) **Status:** The CA 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

(H) **Revocation:** The CA will follow the requirements of these Guidelines and revoke the EV Certificate for any of the revocation reasons specified in these Guidelines. 12

7.2 By the Applicant

EV Certificate Applicants make the commitments and warranties set forth in Section 10.3.2 of these Guidelines for the benefit of the CA and Certificate Beneficiaries.

8 Community and Applicability

8.1 Issuance of EV Certificates

The CA MAY issue EV Certificates, provided that the CA and its Root CA satisfy the requirements in these Guidelines and the Baseline Requirements.

If a court or government body with jurisdiction over the activities covered by these Guidelines determines that the performance of any mandatory requirement is illegal, then such requirement is considered reformed to the minimum extent necessary to make the requirement valid and legal. This applies only to operations or certificate issuances that are subject to the laws of that jurisdiction. The parties involved SHALL notify the CA / Browser Forum of the facts, circumstances, and law(s) involved, so that the CA/Browser Forum may revise these Guidelines accordingly.

8.2 EV Policies

8.2.1 Implementation

Each CA MUST develop, implement, enforce, display prominently on its Web site, and periodically update as necessary its own auditable EV Certificate practices, policies and procedures, such as a Certification Practice Statement (CPS) and Certificate Policy (CP) that:

(A) Implement the requirements of these 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 ETSI TS 102 042 V2.1.1; and

(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.

8.2.2 Disclosure

Each CA MUST publicly disclose their EV Policies through an appropriate and readily accessible online means that is available on a 24x7 basis. The CA is also REQUIRED to publicly disclose its CA business practices as required by both WebTrust for CAs and ETSI TS 102 042 V2.1.1. The disclosures MUST be structured in accordance with either RFC 2527 or RFC 3647.

8.3 Commitment to Conform with Recommendations

Each CA SHALL publicly give effect to these Guidelines and represent that they will adhere to the latest published version by incorporating them into their respective EV Policies, using a clause such as the following (which must include a link to the official version of these Guidelines):

[Name of CA] conforms to the current version of the CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Certificates 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, the CA MUST include (directly or by reference) the applicable requirements of these Guidelines in all contracts with Subordinate CAs, RAs, Enterprise RAs, and subcontractors that involve or relate to the issuance or maintenance of EV Certificates. The CA MUST enforce compliance with such terms.

8.4 Insurance

Each CA SHALL maintain the following insurance related to their respective performance and obligations under these Guidelines: 13

(A) Commercial General Liability insurance (occurrence form) with policy limits of at least two million US dollars in coverage; and
(B) Professional Liability/Errors and Omissions insurance, with policy limits of at least five million US dollars 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.
Such insurance MUST be with a company rated no less than A- as to Policy Holder's Rating in the current edition of Best's Insurance Guide (or with an association of companies each of the members of which are so rated).
A CA MAY self-insure for liabilities that arise from such party's performance and obligations under these Guidelines provided that it has at least five hundred million US dollars in liquid assets based on audited financial statements in the past twelve months, and a quick ratio (ratio of liquid assets to current liabilities) of not less than 1.0.

8.5 Obtaining EV Certificates

8.5.1 General

The CA MAY only issue EV Certificates to Applicants that meet the Private Organization, Government Entity, Business Entity and Non-Commercial Entity requirements specified below.

8.5.2 Private Organization Subjects

An Applicant qualifies as a Private Organization if:
(1) The entity's legal existence is created or recognized by a by a filing with (or an act of) the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration (e.g., by issuance of a certificate of incorporation, registration number, etc.) or created or recognized by a Government Agency (e.g. under a charter, treaty, convention, or equivalent recognition instrument);
(2) The entity designated with the Incorporating or Registration Agency a Registered Agent, a Registered Office (as required under the laws of the Jurisdiction of Incorporation or Registration), or an equivalent facility;
(3) The entity is not designated on the records of the Incorporating or Registration Agency by labels such as "inactive," "invalid," "not current," or the equivalent;
(4) The entity has a verifiable physical existence and business presence;
(5) The entity's Jurisdiction of Incorporation, Registration, Charter, or License, and/or its Place of Business is not 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 entity is not listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.

8.5.3 Government Entity Subjects

An Applicant qualifies as a Government Entity if:
(1) The entity's legal existence was established by the political subdivision in which the entity operates;
(2) The entity is not 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 entity is not listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.

8.5.4 Business Entity Subjects

An Applicant qualifies as a Business Entity if: 14

(1) The entity is a legally recognized entity that filed certain forms with a Registration Agency in its jurisdiction, the Registration Agency issued or approved the entity's charter, certificate, or license, and the entity's existence can be verified with that Registration Agency;
(2) The entity has a verifiable physical existence and business presence;
(3) At least one Principal Individual associated with the entity is identified and validated by the CA;
(4) The identified Principal Individual attests to the representations made in the Subscriber Agreement;
(5) the CA verifies the entity's use of any assumed name used to represent the entity pursuant to the requirements of Section 11.3 herein;
(6) The entity and the identified Principal Individual associated with the entity are not located or residing in any country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and
(7) The entity and the identified Principal Individual associated with the entity are not listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.

8.5.5 Non-Commercial Entity Subjects

An Applicant qualifies as a Non-Commercial Entity if:
(A) The Applicant is an International Organization Entity, created under a charter, treaty, convention or equivalent instrument that was signed by, or on behalf of, more than one country's government. The CA/Browser Forum may publish a listing of Applicants who qualify as an International Organization for EV eligibility; and
(B) The Applicant is not headquartered in any country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and
(C) The Applicant is not listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.
Subsidiary organizations or agencies of an entity that qualifies as a Non-Commercial Entity also qualifies for EV Certificates as a Non-Commercial Entity.

9 EV Certificate Content and Profile

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.

9.1 Issuer Information

Issuer Information listed in an EV Certificate MUST conform with Section 9.1 of the Baseline Requirements.

9.2 Subject Information

Subject to the requirements of these Guidelines, the EV Certificate and certificates issued to Subordinate CAs that are not controlled by the same entity as the CA MUST include the following information about the Subject organization in the fields listed:

9.2.1 Subject Organization Name Field

Certificate field: subject:organizationName (OID 2.5.4.10)
Required/Optional: Required
Contents: This field MUST contain 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 by the CA as provided herein. A CA MAY abbreviate the organization prefixes or suffixes in the organization name, e.g., if the official record shows "Company Name Incorporated" the CA MAY include "Company Name, Inc." 15

When abbreviating a Subject's full legal name as allowed by this subsection, the CA MUST use abbreviations that are not misleading in the Jurisdiction of Incorporation or Registration.
In addition, an assumed name or DBA 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 names or the organization name by itself exceeds 64 characters, the CA MAY abbreviate parts of the organization name, and/or omit non-material words in the organization name in such a way that the text in this field does not exceed the 64-character limit; provided that the CA checks this field in accordance with section 10.11.1 and a Relying Party will not be misled into thinking that they are dealing with a different organization. In cases where this is not possible, the CA MUST NOT issue the EV Certificate.

9.2.2 Subject Alternative Name Extension

Certificate field: subjectAltName:dNSName
Required/Optional: Required
Contents: This extenstion MUST contain one or more host Domain Name(s) owned or controlled by the Subject and to be associated with the 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.

9.2.3 Subject Common Name Field

Certificate field: subject:commonName (OID: 2.5.4.3)
Required/Optional: Deprecated (Discouraged, but not prohibited)
Contents: If present, this field MUST contain a single Domain Name(s) owned or controlled by the Subject and to be associated with the 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.

9.2.4 Subject Business Category Field

Certificate field: *subject:businessCategory* (OID: 2.5.4.15)
Required/Optional: Required
Contents: This field MUST contain one of the following strings: "Private Organization", "Government Entity", "Business Entity", or "Non-Commercial Entity" depending upon whether the Subject qualifies under the terms of Section 8.2.2, 8.2.3, 8.2.4 or 8.2.5 of these Guidelines, respectively.

9.2.5 Subject Jurisdiction of Incorporation or Registration Field

Certificate fields:
Locality (if required):
subject:jurisdictionOfIncorporationLocalityName (OID: 1.3.6.1.4.1.311.60.2.1.1)
ASN.1 - X520LocalityName as specified in RFC 5280
State or province (if required):
subject:jurisdictionOfIncorporationStateOrProvinceName (OID: 1.3.6.1.4.1.311.60.2.1.2)
ASN.1 - X520StateOrProvinceName as specified in RFC 5280
Country:
subject:jurisdictionOfIncorporationCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3)
ASN.1 – *X520countryName* as specified in RFC 5280
Required/Optional: Required 16

Contents: These fields MUST NOT contain information that is not relevant to the level of the Incorporating Agency or Registration Agency. For example, the Jurisdiction of Incorporation for an Incorporating Agency or Jurisdiction of Registration for a Registration Agency that operates at the country level MUST include the country information but MUST NOT include the state or province or locality information. Similarly, the jurisdiction for the applicable Incorporating Agency or Registration Agency at the state or province level MUST include both country and state or province information, but MUST NOT include locality information. And, the jurisdiction for the applicable Incorporating Agency or Registration Agency at the locality level MUST include the country and state or province information, where the state or province regulates the registration of the entities at the locality level, as well as the locality information. Country information MUST be specified using the applicable ISO country code. State or province or locality information (where applicable) for the Subject's Jurisdiction of Incorporation or Registration MUST be specified using the full name of the applicable jurisdiction.

9.2.6 Subject Registration Number Field

Certificate field: Subject:serialNumber (OID: 2.5.4.5)

Required/Optional: Required

Contents: For Private Organizations, this field MUST contain the Registration (or similar) Number assigned to the Subject by the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration, as appropriate. If the Jurisdiction of Incorporation or Registration does not provide a Registration Number, then the date of Incorporation or Registration SHALL be entered into this field in any one of the common date formats.

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

For Business Entities, the Registration Number that was received by the Business Entity upon government registration SHALL be entered in this field. For those Business Entities that register with an Incorporating Agency or Registration Agency in a jurisdiction that does not issue numbers pursuant to government registration, the date of the registration SHALL be entered into this field in any one of the common date formats.

9.2.7 Subject Physical Address of Place of Business Field

Certificate fields:

Number and street: subject:streetAddress (OID: 2.5.4.9)

City or town: subject:localityName (OID: 2.5.4.7)

State or province (where applicable): subject:stateOrProvinceName (OID: 2.5.4.8)

Country: subject:countryName (OID: 2.5.4.6)

Postal code: subject:postalCode (OID: 2.5.4.17)

Required/Optional: City, state, and country – Required; Street and postal code – Optional

Contents: This field MUST contain the address of the physical location of the Subject's Place of Business.

9.2.8 Other Subject Attributes

All other optional attributes, when present within the subject field, MUST contain information that has been verified by the CA. CAs SHALL NOT include Fully-Qualified Domain Names in Subject attributes except as specified in Sections 9.2.1 and SHALL NOT include any Subject Organization Information except as specified in Section 9.2. Optional subfields within the Subject field MUST either contain information verified by the CA or MUST be left empty. Metadata such as '.', '-', and ' ' characters, and/or any other indication that the field is empty, absent or incomplete, MUST not be used. 17

9.3 Certificate Policy Identification

9.3.1 EV Certificate Policy Identification Requirements

This section sets forth minimum requirements for the contents of EV Certificates as they relate to the identification of EV Certificate Policy.

9.3.2 EV Subscriber Certificates

Each EV Certificate issued by the CA to a Subscriber MUST contain a policy identifier defined by the CA in the certificate's certificatePolicies extension that: (i) indicates which CA policy statement relates to that Certificate, (ii) asserts the CA's adherence to and compliance with these Guidelines, and (iii), by pre-agreement with the Application Software Supplier, marks the Certificate as being an EV Certificate.

9.3.3 Root CA Certificates

The Application Software Supplier identifies Root CAs that are approved to issue EV Certificates by storing EV policy identifiers in metadata associated with Root CA Certificates.

9.3.4 EV Subordinate CA Certificates

(1) Certificates issued to Subordinate CAs that are not controlled by the issuing CA MUST contain one or more policy identifiers defined by the issuing CA that explicitly identify the EV Policies that are implemented by the Subordinate CA.

(2) Certificates issued to Subordinate CAs that are controlled by the Root CA MAY contain the special anyPolicy identifier (OID: 2.5.29.32.0).

9.3.5 Subscriber Certificates

A Certificate issued to a Subscriber MUST contain one or more policy identifier(s), defined by the Issuing CA, in the Certificate's certificatePolicies extension that indicates adherence to and compliance with these Guidelines. Each CA SHALL document in its Certificate Policy or Certification Practice Statement that the Certificates it issues containing the specified policy identifier(s) are managed in accordance with these Guidelines.

9.4 Maximum Validity Period For EV Certificate

The validity period for an EV Certificate SHALL NOT exceed twenty seven months. It is RECOMMENDED that EV Subscriber Certificates have a maximum validity period of twelve months.

9.5 Subscriber Public Key

The requirements in Section 9.5 of the Baseline requirements apply equally to EV Certificates.

9.6 Certificate Serial Number

The requirements in Section 9.6 of the Baseline requirements apply equally to EV Certificates.

9.7 Additional Technical Requirements for EV Certificates

Both Appendix A – Minimum Cryptographic Algorithms of the Baseline Requirements and Key Sizes and Appendix B – Certificate Extensions of the Baseline Requirements apply to EV Certificates with the following exceptions:

1) If a Subordinate CA Certificates is issued to a Subordinate CA not controlled by the entity that controls the Root CA, the policy identifiers in the certificatePolicies extension MUST include the CA's Extended Validation policy identifier. Otherwise, it MAY contain the anyPolicy identifier.

2) The following fields MUST be present if the Subordinate CA is not controlled by the entity that controls the Root CA.

certificatePolicies:policyQualifiers:policyQualifierId
□□id-qt 1 [RFC 5280]
certificatePolicies:policyQualifiers:qualifier:cPSuri
□□HTTP URL for the Root CA's Certification Practice Statement 18

3) The certificatePolicies extension in EV Certificates issued to Subscribers MUST include the following:

certificatePolicies:policyIdentifier (Required)
□□The Issuer's EV policy identifier
certificatePolicies:policyQualifiers:policyQualifierId (Required)
□□id-qt 1 [RFC 5280]
certificatePolicies:policyQualifiers:qualifier:cPSuri (Required)
□□HTTP URL for the Subordinate CA's Certification Practice Statement
4) The cRLDistribution Point extension MUST be present in Subscriber Certificates if the certificate does not specify OCSP responder locations in an authorityInformationAccess extension.

10 EV Certificate Request Requirements

10.1 General Requirements

10.1.1 Documentation Requirements

The documentation requirements in Section 10.1 of the Baseline requirements apply equally to EV Certificates.

10.1.2 Role Requirements

The following Applicant roles are required for the issuance of an EV Certificate.
□□□□**Certificate Requester:** The EV Certificate Request MUST be submitted by an authorized Certificate Requester. A Certificate Requester is a natural person who is either the Applicant, employed by the Applicant, 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 either the Applicant, 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.
□□□□**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 either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant, and who has authority on behalf of the Applicant to sign Subscriber Agreements.
(4) **Applicant Representative**: In the case where the CA and the Subscriber are affiliated, Terms of Use applicable to the requested EV Certificate MUST be acknowledged and agreed to by an authorized Applicant Representative. An Applicant Representative is a natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant, and who has authority on behalf of the Applicant to acknowledge and agree to the Terms of Use.
The Applicant MAY authorize one individual to occupy two or more of these roles. The Applicant MAY authorize more than one individual to occupy any of these roles.

10.2 EV Certificate Request Requirements

The Certificate Request requirements in Section 10.2 apply equally to EV Certificates subject to the additional more stringent ageing and updating requirement of Section 11.13 of these Guidelines. 19

10.3 Requirements for Subscriber Agreement and Terms of Use

Section 10.3 of the Baseline Requirements applies equally to EV Certificates. In cases where the Certificate Request does not contain all necessary information about the Applicant, the CA MUST additionally confirm the data with the Certificate Approver or Contract Signer rather than the Applicant.

11 Verification Requirements

11.1 General Overview

This part of the Guidelines sets forth Verification Requirements and Acceptable Methods of Verification for each such Requirement**.**

11.1.1 Verification Requirements – Overview

Before issuing an EV Certificate, the CA MUST ensure that all Subject organization information to be included in the EV Certificate conforms to the requirements of, and is verified in accordance with, these Guidelines and matches the information confirmed and documented by the CA pursuant to its verification processes. Such verification processes are intended to accomplish the following:

□□□□Verify Applicant's existence and identity, including;

(A) Verify the Applicant's legal existence and identity (as more fully set forth in Section 11.2 herein),

(B) Verify the Applicant's physical existence (business presence at a physical address), and

(C) Verify the Applicant's operational existence (business activity).

□□□□Verify the Applicant is a registered holder, or has exclusive control, of the Domain Name(s) to be included in the EV Certificate;

□□□□Verify the Applicant's authorization for the EV Certificate, including;

(A) Verify the name, title, and authority of the Contract Signer, Certificate Approver, and Certificate Requester,

(B) Verify that a Contract Signer signed the Subscriber Agreement or that a duly authorized Applicant Representative acknowledged and agreed to the Terms of Use; and

(C) Verify that a Certificate Approver has signed or otherwise approved the EV Certificate Request.

11.1.2 Acceptable Methods of Verification – Overview

As a general rule, the CA is responsible for taking all verification steps reasonably necessary to satisfy each of the Verification Requirements set forth in the subsections below. The Acceptable Methods of Verification set forth in each of Sections 11.2 through11.13 (which usually include alternatives) are considered to be the minimum acceptable level of verification required of the CA. In all cases, however, the CA is responsible for taking any additional verification steps that may be reasonably necessary under the circumstances to satisfy the applicable Verification Requirement.

11.2 Verification of Applicant's Legal Existence and Identity

11.2.1 Verification Requirements

To verify the Applicant's legal existence and identity, the CA MUST do the following.

(1) **Private Organization Subjects**

(A) **Legal Existence:** Verify that the Applicant is a legally recognized entity, in existence and validly formed (e.g., incorporated) with the Incorporating or Registration Agency in the Applicant's Jurisdiction of Incorporation or Registration, and not designated on the records of the Incorporating or Registration Agency by labels such as "inactive", "invalid", "not current", or the equivalent. 20

(B) **Organization Name:** Verify that the Applicant's formal legal name as recorded with the Incorporating or Registration Agency in the Applicant's Jurisdiction of Incorporation or Registration matches the Applicant's name in the EV Certificate Request.
(C) **Registration Number:** Obtain the specific Registration Number assigned to the Applicant by the Incorporating or Registration Agency in the Applicant's Jurisdiction of Incorporation or Registration. Where the Incorporating or Registration Agency does not assign a Registration Number, the CA SHALL obtain the Applicant's date of Incorporation or Registration.
(D) **Registered Agent:** Obtain the identity and address of the Applicant's Registered Agent or Registered Office (as applicable in the Applicant's Jurisdiction of Incorporation or Registration).
(2) **Government Entity Subjects**
(A) **Legal Existence:** Verify that the Applicant is a legally recognized Government Entity, in existence in the political subdivision in which such Government Entity operates.
(B) **Entity Name:** Verify that the Applicant's formal legal name matches the Applicant's name in the EV Certificate Request.
(C) **Registration Number:** The CA MUST attempt to obtain the Applicant's date of incorporation, registration, or formation, or the identifier for the legislative act that created the Government Entity. In circumstances where this information is not available, the CA MUST enter appropriate language to indicate that the Subject is a Government Entity.
(3) **Business Entity Subjects**
(A) **Legal Existence:** Verify that the Applicant is engaged in business under the name submitted by the Applicant in the Application.
(B) **Organization Name:** Verify that the Applicant's formal legal name as recognized by the Registration Authority in the Applicant's Jurisdiction of Registration matches the Applicant's name in the EV Certificate Request.
(C) **Registration Number:** Attempt to obtain the specific unique Registration Number assigned to the Applicant by the Registration Agency in the Applicant's Jurisdiction of Registration. Where the Registration Agency does not assign a Registration Number, the CA SHALL obtain the Applicant's date of Registration.
(D) **Principal Individual:** Verify the identity of the identified Principal Individual.
(4) **Non-Commercial Entity Subjects (International Organizations)**
(A) **Legal Existence:** Verify that the Applicant is a legally recognized International Organization Entity.
(B) **Entity Name:** Verify that the Applicant's formal legal name matches the Applicant's name in the EV Certificate Request.
(C) **Registration Number:** The CA MUST attempt to obtain the Applicant's date of formation, or the identifier for the legislative act that created the International Organization Entity. In circumstances where this information is not available, the CA MUST enter appropriate language to indicate that the Subject is an International Organization Entity.

11.2.2 Acceptable Method of Verification

(1) **Private Organization Subjects:** All items listed in Section 11.2.1(1) MUST be verified directly with, or obtained directly from, the Incorporating or Registration Agency in the Applicant's Jurisdiction of Incorporation or Registration. Such verification MAY be through use of a Qualified Government Information Source operated by, or on behalf of, the Incorporating or Registration Agency, or by direct contact with the Incorporating or Registration Agency in person or via mail, e-mail, Web address, or telephone, using an address or phone number obtained directly from the Qualified Government Information Source, Incorporating or Registration Agency, or from a Qualified Independent Information Source.
(2) **Government Entity Subjects:** All items listed in Section 11.2.1(2) MUST either be verified directly with, or obtained directly from, one of the following: (i) a Qualified Government Information Source in the political subdivision in which such Government Entity operates; (ii) a superior governing Government Entity in the same 21

political subdivision as the Applicant (e.g. a Secretary of State may verify the legal existence of a specific State Department), or (iii) from a judge that is an active member of the federal, state or local judiciary within that political subdivision, or (iv) an attorney representing the Government Entity.
Any communication from a judge SHALL be verified in the same manner as is used for verifying factual assertions that are asserted by an Attorney as set forth in Section 11.10.1.
Such verification MAY be by direct contact with the appropriate Government Entity in person or via mail, e-mail, Web address, or telephone, using an address or phone number obtained from a Qualified Independent Information Source.
(3) **Business Entity Subjects:** All items listed in Section 11.2.1(3) above, MUST be verified directly with, or obtained directly from, the Registration Agency in the Applicant's Jurisdiction of Registration. Such verification MAY be performed by means of a Qualified Government Information Source, a Qualified Governmental Tax Information Source, or by direct contact with the Registration Agency in person or via mail, e-mail, Web address, or telephone, using an address or phone number obtained directly from the Qualified Government Information Source, Qualified Governmental Tax Information Source or Registration Agency, or from a Qualified Independent Information Source. In addition, the CA MUST validate a Principal Individual associated with the Business Entity pursuant to the requirements in subsection (4), below.
(4) **Principal Individual:** A Principal Individual associated with the Business Entity MUST be validated in a face-to-face setting. The CA MAY rely upon a face-to-face validation of the Principal Individual performed by the Registration Agency, provided that the CA has evaluated the validation procedure and concluded that it satisfies the requirements of the Guidelines for face-to-face validation procedures. Where no face-to-face validation was conducted by the Registration Agency, or the Registration Agency's face-to-face validation procedure does not satisfy the requirements of the Guidelines, the CA SHALL perform face-to-face validation.
(A) **Face-To-Face Validation:** The face-to-face validation MUST be conducted before either an employee of the CA, a Latin Notary, a Notary (or equivalent in the Applicant's jurisdiction), a Lawyer, or Accountant (Third-Party Validator). The Principal Individual(s) MUST present the following documentation (Vetting Documents) directly to the Third-Party Validator:
(i) A Personal Statement that includes the following information:
1. Full name or names by which a person is, or has been, known (including all other names used);
2. Residential Address at which he/she can be located;
3. Date of birth; and
4. An affirmation that all of the information contained in the Certificate Request is true and correct.
(ii) A current signed government-issued identification document that includes a photo of the Individual and is signed by the Individual such as:
1. A passport;
2. A driver's license;
3. A personal identification card;
4. A concealed weapons permit; or
5. A military ID.
(iii) At least two secondary documentary evidences to establish his/her identity that include the name of the Individual, one of which MUST be from a financial institution.
1. Acceptable financial institution documents include:
a. A major credit card, provided that it contains an expiration date and it has not expired'
b. A debit card from a regulated financial institution, provided that it contains an expiration date and it has not expired,
c. A mortgage statement from a recognizable lender that is less than six months old,
d. A bank statement from a regulated financial institution that is less than six months old. 22

2. Acceptable non-financial documents include:
a. Recent original utility bills or certificates from a utility company confirming the arrangement to pay for the services at a fixed address (not a mobile/cellular telephone bill),
b. A copy of a statement for payment of a lease, provided that the statement is dated within the past six months,
c. A certified copy of a birth certificate,
d. A local authority tax bill for the current year,
e. A certified copy of a court order, such as a divorce certificate, annulment papers, or adoption papers.
The Third-Party Validator performing the face-to-face validation MUST:
(i) Attest to the signing of the Personal Statement and the identity of the signer; and
(ii) Identify the original Vetting Documents used to perform the identification. In addition, the Third-Party Validator MUST attest on a copy of the current signed government-issued photo identification document that it is a full, true, and accurate reproduction of the original.
(B) **Verification of Third-Party Validator:** The CA MUST independently verify that the Third-Party Validator is a legally-qualified Latin Notary or Notary (or legal equivalent in the Applicant's jurisdiction), lawyer, or accountant in the jurisdiction of the Individual's residency, and that the Third-Party Validator actually did perform the services and did attest to the signature of the Individual.
(C) **Cross-checking of Information:** The CA MUST obtain the signed and attested Personal Statement together with the attested copy of the current signed government-issued photo identification document. The CA MUST review the documentation to determine that the information is consistent, matches the information in the application, and identifies the Individual. The CA MAY rely on electronic copies of this documentation, provided that:
(i) the CA confirms their authenticity (not improperly modified when compared with the underlying original) with the Third-Party Validator; and
(ii) electronic copies of similar kinds of documents are recognized as legal substitutes for originals under the laws of the CA's jurisdiction.
(5) **Non-Commercial Entity Subjects (International Organization):** All items listed in Section 11.2.1 (4) MUST be verified either:
(A) With reference to the constituent document under which the International Organization was formed; or
(B) Directly with a signatory country's government in which the CA is permitted to do business. Such verification may be obtained from an appropriate government agency or from the laws of that country, or by verifying that the country's government has a mission to represent it at the International Organization; or
(C) Directly against any current list of qualified entities that the CA/Browser Forum may maintain at www.cabforum.org.
(D) In cases where the International Organization applying for the EV Certificate is an organ or agency - including a non-governmental organization of a verified International Organization, then the CA may verify the International Organization Applicant directly with the verified umbrella International Organization of which the Applicant is an organ or agency.

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

11.3.1 Verification Requirements

If, in addition to the Applicant's formal legal name, as recorded with the applicable Incorporating Agency or Registration Agency in the Applicant's Jurisdiction of Incorporation or Registration, the Applicant's identity, as asserted in the EV Certificate, is to contain any assumed name (also known as "doing business as", "DBA", or "d/b/a" in the US, and "trading as" in the UK) under which the Applicant conducts business, the CA MUST verify that: (i) the 23

Applicant has registered its use of the assumed name with the appropriate government agency for such filings in the jurisdiction of its Place of Business (as verified in accordance with these Guidelines), and (ii) that such filing continues to be valid.

11.3.2 Acceptable Method of Verification

To verify any assumed name under which the Applicant conducts business:

(1) The CA MAY verify the assumed name through use of a Qualified Government Information Source operated by, or on behalf of, an appropriate government agency in the jurisdiction of the Applicant's Place of Business, or by direct contact with such government agency in person or via mail, e-mail, Web address, or telephone; or

(2) The CA MAY verify the assumed name through use of a Qualified Independent Information Source provided that the QIIS has verified the assumed name with the appropriate government agency.

(3) The CA MAY rely on a Verified Legal Opinion, or a Verified Accountant Letter that indicates the assumed name under which the Applicant conducts business, the government agency with which the assumed name is registered, and that such filing continues to be valid.

11.4 Verification of Applicant's Physical Existence

11.4.1 Address of Applicant's Place of Business

(1) **Verification Requirements:** To verify the Applicant's physical existence and business presence, the CA MUST verify that the physical address provided by the Applicant is an address where the Applicant or a Parent/Subsidiary Company conducts business operations (not, for example, a mail drop or P.O. box, or 'care of' (C/O) address, such as an address for an agent of the Organization), and is the address of the Applicant's Place of Business.

(2) **Acceptable Methods of Verification**

(A) **Place of Business in the Country of Incorporation or Registration**

(i) For Applicants whose Place of Business is in the same country as the Applicant's Jurisdiction of Incorporation or Registration and whose Place of Business is NOT the same as that indicated in the relevant Qualified Government Information Source used in Section 11.2 to verify legal existence: (1) For Applicants listed at the same Place of Business address in the current version of either at least one QGIS (other than that used to verify legal existence), QIIS or QTIS, the CA MUST confirm that the Applicant's address, as listed in the EV Certificate Request, is a valid business address for the Applicant or a Parent/Subsidiary Company by reference to such QGIS, QIIS, or QTIS, and MAY rely on the 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 either at least one QIIS or QTIS, the CA MUST confirm that the address provided by the Applicant in the EV Certificate Request is the Applicant's or a Parent/Subsidiary Company's business address, by obtaining documentation of a site visit to the business address, which MUST be performed by a reliable individual or firm. The documentation of the site visit MUST:

(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 the Applicant is conducting ongoing business activities at the site (not that it is just, for example, 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. 24

(2) For all Applicants, the CA MAY alternatively rely on a Verified Legal Opinion or a Verified Accountant Letter that indicates the address of the Applicant's or a Parent/Subsidiary Company's Place of Business and that business operations are conducted there.
(3) For Government Entity Applicants, the CA MAY rely on the address contained in the records of the QGIS in the Applicant's jurisdiction.
(4) For Applicants whose Place of Business is in the same country as the Applicant's Jurisdiction of Incorporation or Registration and where the QGIS used in Section 11.2 to verify legal existence contains a business address for the Applicant, the CA MAY rely on the address in the QGIS to confirm the Applicant's or a Parent/Subsidiary Company's address as listed in the EV Certificate Request, and MAY rely on the Applicant's representation that such address is its Place of Business.
(B) **Place of Business not in the Country of Incorporation or Registration:** The CA MUST rely on a Verified Legal Opinion or Verified Accountant's Letter that indicates the address of the Applicant's Place of Business and that business operations are conducted there.

11.4.2 Telephone Number for Applicant's Place of Business

(1) Verification Requirements: To further verify the Applicant's physical existence and business presence, as well as to assist in confirming other verification requirements, the CA MUST verify a main telephone number for one of the Applicant's Places of Business.
(2) Acceptable Methods of Verification: To verify the Applicant's telephone number, the CA MUST perform items A and either B or C as listed below:
(A) Confirm the Applicant's 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;
(B) Confirm that the telephone number is listed as one of the Applicant's or Parent/Subsidiary Company's or Principal Individual's (for business entities) telephone numbers, matching an address of one of the Applicant's Places of Business in records provided by the applicable phone company, or, alternatively, in at least one QIIS, QGIS, or QTIS;
(C) Rely on a Verified Legal Opinion or a Verified Accountant Letter to the effect that the Applicant's telephone number, as provided, is a main phone number for the Applicant's Place of Business.

11.5 Verification of Applicant's Operational Existence

11.5.1 Verification Requirements

If the Applicant, or a Parent or Affiliate of the Applicant, has been in existence for less than three years, as indicated by the records of the Incorporating Agency or Registration Agency, and is not listed in either the current version of one QIIS or QTIS, the CA MUST verify that the Applicant has the ability to engage in business. In other words, if the Applicant is a Subsidiary or Affiliate of an entity that the CA verified as in existence for three or more years, then the CA MAY rely on the existence of the Parent or Affiliate as verification of the Applicant's operational existence.

11.5.2 Acceptable Methods of Verification

To verify the Applicant's operational existence, the CA MUST perform one of the following:
(1) Verify that the Applicant has an active current Demand Deposit Account with a Regulated Financial Institution. The CA MUST receive authenticated documentation directly from a Regulated Financial Institution verifying that the Applicant has an active current Demand Deposit Account with the institution.
(2) Rely on a Verified Legal Opinion or a Verified Accountant Letter to the effect that the Applicant has an active current Demand Deposit Account with a Regulated Financial Institution.

11.6 Verification of Applicant's Domain Name

11.6.1 Verification Requirements

The CA MUST confirm that the Applicant: 25

(A) Is the registered holder of the Domain Name, or
(B) Has been granted the exclusive right to use the Domain Name by the registered holder of the Domain Name;
To verify the Applicant's registration, or exclusive control, of the Domain Name(s) to be listed in the EV Certificate, the CA MUST verify that each such 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). For Government Entity Applicants, the CA MAY rely on the Domain Name listed for that entity in the records of the QGIS in the Applicant's Jurisdiction.
The CA MUST compare any registration information that is publicly available from the WHOIS database with the verified Subject organization information and MUST confirm that it is neither misleading nor inconsistent.
The CA MUST further confirm that the Applicant is aware of its registration or exclusive control of the Domain Name.

11.6.2 Acceptable Methods of Verification

(1) **Applicant as Registered Holder:** Acceptable methods by which the CA MAY verify that the Applicant is the registered holder of the Domain Name include the following:
(A) Performing a WHOIS inquiry on the Internet for the Domain Name supplied by the Applicant, and obtaining a response indicating that the Applicant or a Parent/Subsidiary Company is the entity to which the Domain Name is registered; or
(B) Communicating with the contact listed on the WHOIS record to confirm that the Applicant is the registered holder of the Domain Name and having the contact update the WHOIS records to reflect the proper Domain Name registration. Confirmation that the registered owner of the Domain Name is a Parent/Subsidiary Company of the Applicant, or a registered trading name of the Applicant is sufficient to establish that the Applicant is the registered owner of the Domain Name;
(C) In cases where domain registration information is private, and the domain registrar offers services to forward communication to the registered domain holder, the CA MAY contact the Applicant through the domain registrar by e-mail or paper mail.
(2) **Applicant's Exclusive Right to Use:** In cases where the Applicant is not the registered holder of the Domain Name, the CA MUST verify the Applicant's exclusive right to use the Domain Name(s).
(A) In cases where the registered domain holder can be contacted using information obtained from WHOIS, or through the domain registrar, the CA MUST obtain positive confirmation from the registered domain holder by paper mail, e-mail, telephone, or facsimile that the Applicant has been granted the exclusive right to use the requested Fully Qualified Domain Name (FQDN).
If the Top-Level Domain is a generic top-level domain (gTLD) such as .com, .net, or .org in accordance with RFC 1591, the CA MUST obtain positive confirmation from the second-level domain registration holder. For example, if the requested FQDN is www1.www.example.com, the CA MUST obtain positive confirmation from the domain holder of example.com.
If the Top-Level Domain is a 2 letter Country Code Top-Level Domain (ccTLD), the CA MUST obtain positive confirmation from the domain holder at the appropriate domain level, based on the rules of the ccTLD. For example, if the requested FQDN is www.mysite.users.internet.co.uk, the CA MUST obtain positive confirmation from the domain holder of internet.co.uk.
In addition, the CA MUST verify the Applicant's exclusive right to use the Domain Name using one of the following methods:
(i) Relying on a Verified Legal Opinion or a Verified Accountant Letter to the effect that the Applicant has the exclusive right to use the specified Domain Name in identifying itself on the Internet; or
(ii) Relying on a representation from the Contract Signer, or the Certificate Approver, if expressly so authorized in a mutually-agreed-upon contract.

(B) In cases where the registered domain holder cannot be contacted, the CA MUST:
(i) Rely on a Verified Legal Opinion or a Verified Accountant Letter to the effect that the Applicant has the exclusive right to use the specified Domain Name in identifying itself on the Internet; and 26

(ii) Rely on a representation from the Contract Signer, or the Certificate Approver, if expressly so authorized in a mutually-agreed-upon contract, coupled with a practical demonstration by the Applicant establishing that it controls the 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.
(3) **Knowledge:** Acceptable methods by which the CA MAY verify that the Applicant is aware that it has exclusive control of the Domain Name include the following:
(A) Relying on a Verified Legal Opinion or a Verified Accountant Letter to the effect that the Applicant is aware that it has exclusive control of the Domain Name; or
(B) Obtaining a confirmation from the Contract Signer or Certificate Approver verifying that the Applicant is aware that it has exclusive control of the Domain Name.
(4) **Mixed Character Set Domain Names:** EV Certificates MAY include Domain Names containing mixed character sets only in compliance with the rules set forth by the domain registrar. The CA MUST visually compare any Domain Names with mixed character sets with known high risk domains. If a similarity is found, then the EV Certificate Request MUST be flagged as High Risk. The CA must perform reasonably appropriate additional authentication and verification to be certain beyond reasonable doubt that the Applicant and the target in question are the same organization.

11.7 Verification of Name, Title, and Authority of Contract Signer and Certificate Approver

11.7.1 Verification Requirements

For both the Contract Signer and the Certificate Approver, the CA MUST verify the following.
(1) **Name, Title and Agency:** The CA MUST verify the name and title of the Contract Signer and the Certificate Approver, as applicable. The CA MUST also verify that the Contract Signer and the Certificate Approver are agents representing the Applicant.
(2) **Signing Authority of Contract Signer:** The CA MUST verify that the Contract Signer is 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 the Applicant.
(3) **EV Authority of Certificate Approver:** The CA MUST verify, through a source other than the Certificate Approver him- or herself, that the Certificate Approver is expressly authorized by the Applicant to do the following, as of the date of the EV Certificate Request:
(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.

11.7.2 Acceptable Methods of Verification – Name, Title and Agency

Acceptable methods of verification of the name, title, and agency status of the Contract Signer and the Certificate Approver include the following.
(1) **Name and Title:** The CA MAY verify the name and title of the Contract Signer and the Certificate Approver by any appropriate method designed to provide reasonable assurance that a person claiming to act in such a role is in fact the named person designated to act in such role**.**
(2) **Agency:** The CA MAY verify the agency of the Contract Signer and the Certificate Approver by:
(A) Contacting the Applicant's Human Resources Department by phone or mail (at the phone number or address for the Applicant's Place of Business, verified in accordance with these 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 the Applicant (as described in Section 11.10.4), or a Verified Legal Opinion (as described in Section 11.10.1), or a Verified Accountant Letter (as described in Section 27

11.10.2) verifying that the Contract Signer and/or the Certificate Approver, as applicable, is either an employee or has otherwise been appointed as an agent of the Applicant.
(C) Obtaining confirmation from a QIIS or QGIS that the Contract Signer and/or Certificate Approver is an employee of the Applicant.
The CA MAY also verify the agency of the Certificate Approver via a certification from the Contract Signer (including in a contract between the CA and the Applicant signed by the Contract Signer), provided that the employment or agency status and Signing Authority of the Contract Signer has been verified.

11.7.3 Acceptable Methods of Verification – Authority

Acceptable methods of verification of the Signing Authority of the Contract Signer, and the EV Authority of the Certificate Approver, as applicable, include:
(1) **Legal Opinion:** The Signing Authority of the Contract Signer, and/or the EV Authority of the Certificate Approver, MAY be verified by reliance on a Verified Legal Opinion (as described in Section 11.10.1);
(2) **Accountant Letter:** The Signing Authority of the Contract Signer, and/or the EV Authority of the Certificate Approver, MAY be verified by reliance on a Verified Accountant Letter (as described in Section 11.10.2);
(3) **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 (i) certified by the appropriate corporate officer (e.g., secretary), and (ii) the CA 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;
(4) **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 the Applicant (as described in Section 11.10.4);
(5) **Contract between CA and Applicant:** The EV Authority of the Certificate Approver MAY be verified by reliance on a contract between the CA and the Applicant that designates the Certificate Approver with such EV Authority, provided that the contract is signed by the Contract Signer and provided that the agency and Signing Authority of the Contract Signer have been verified;
(6) **Prior Equivalent Authority:** The signing authority of the Contract Signer, and/or the EV authority of the Certificate Approver, MAY be verified by relying on a demonstration of Prior Equivalent Authority.
(A) Prior Equivalent Authority of a Contract Signer MAY be relied upon for confirmation or verification of the signing authority of the Contract Signer when the Contract Signer has executed a binding contract between the CA and the Applicant with a legally valid and enforceable seal or handwritten signature and only when the contract was executed more than 90 days prior to the EV Certificate application. The CA MUST record sufficient details of the previous agreement to correctly identify it and associate it with the EV application. Such details MAY include any of the following:
(i) Agreement title,
(ii) Date of Contract Signer's signature,
(iii) Contract reference number, and
(iv) Filing location.
(B) Prior Equivalent Authority of a Certificate Approver MAY be relied upon for confirmation or verification of the EV Authority of the Certificate Approver when the Certificate Approver has performed one or more of the following:
(i) Under contract to the CA, has served (or is serving) as an Enterprise RA for the Applicant, or
(ii) Has participated in the approval of one or more certificate requests, for certificates issued by the CA and which are currently and verifiably in use by the Applicant. In this case the CA MUST

have contacted the Certificate Approver by phone at a previously validated phone number or have accepted a signed and notarized letter approving the certificate request. 28

(7) **QIIS or QGIS**: The Signing Authority of the Contract Signer, and/or the EV Authority of the Certificate Approver, MAY be verified by a QIIS or QGIS that identifies the Contract Signer and/or the Certificate Approver as a corporate officer, sole proprietor, or other senior official of the Applicant.
8) **Contract Signer's Representation/Warranty:** Provided that the CA verifies that the Contract Signer is an employee or agent of the Applicant, the CA MAY rely on the signing authority of the Contract Signer by obtaining a duly executed representation or warranty from the Contract Signer that includes the following acknowledgments:
(A) That the Applicant authorizes the Contract Signer to sign the Subscriber Agreement on the Applicant's behalf,
(B) That the Subscriber Agreement is a legally valid and enforceable agreement,
(C) That, upon execution of the Subscriber Agreement, the Applicant will be bound by all of its terms and conditions,
(D) That serious consequences attach to the misuse of an EV certificate, and
(E) The contract signer has the authority to obtain the digital equivalent of a corporate seal, stamp or officer's signature to establish the authenticity of the company's Web site.
Note: An example of an acceptable representation/warranty appears in Appendix E.

11.7.4 Pre-Authorized Certificate Approver

Where the CA and Applicant contemplate the submission of multiple future EV Certificate Requests, then, after the CA:
□□□□Has verified the name and title of the Contract Signer and that he/she is an employee or agent of the Applicant; and
□□□□Has verified the Signing Authority of such Contract Signer in accordance with one of the procedures in Section 11.7.3.
The CA and the Applicant MAY enter into a written agreement, signed by the Contract Signer on behalf of the Applicant, whereby, for a specified term, the Applicant expressly authorizes one or more Certificate Approver(s) designated in such agreement to exercise EV Authority with respect to each future EV Certificate Request submitted on behalf of the Applicant and properly authenticated as originating with, or otherwise being approved by, such Certificate Approver(s). Such an agreement MUST provide that 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 procedures by which the Applicant can notify the CA that the EV Authority of any such Certificate Approver is revoked, and (iv) such other appropriate precautions as are reasonably necessary.

11.8 Verification of Signature on Subscriber Agreement and EV Certificate Requests

Both the Subscriber Agreement and each non-pre-authorized EV Certificate Request MUST be signed. The Subscriber Agreement MUST be signed by an authorized Contract Signer. The EV Certificate Request MUST be signed by the Certificate Requester submitting the document, unless the Certificate Request has been pre-authorized in line with Section 11.7.4 of these Guidelines. If the Certificate Requester is not also an authorized Certificate Approver, then an authorized Certificate Approver MUST independently approve the EV Certificate Request. In all cases, applicable signatures MUST be a legally valid and contain an 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.

11.8.1 Verification Requirements

(1) **Signature:** The CA MUST authenticate the signature of the Contract Signer on the Subscriber Agreement and the signature of the Certificate Requester on each EV Certificate Request in 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. 29

(2) **Approval Alternative:** In cases where an EV Certificate Request is signed and submitted by a Certificate Requester who does not also function as a Certificate Approver, approval and adoption of the EV Certificate Request by a Certificate Approver in accordance with the requirements of Section 11.9 can substitute for authentication of the signature of the Certificate Requester on such EV Certificate Request.

11.8.2 Acceptable Methods of Signature Verification

Acceptable methods of authenticating the signature of the Certificate Requester or Contract Signer include the following.

(1) A phone call to the Applicant's or Agent's phone number, as verified in accordance with these Guidelines, asking to speak to the Certificate Requester or Contract Signer, as applicable, 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.

(2) A letter mailed to the Applicant's or Agent's address, as verified through independent means in accordance with these Guidelines, for the attention 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.

(3) 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.

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

11.9 Verification of Approval of EV Certificate Request

11.9.1 Verification Requirements

In cases where an EV Certificate Request is submitted by a Certificate Requester, before the CA issues the requested EV Certificate, the CA MUST verify that an authorized Certificate Approver reviewed and approved the EV Certificate Request.

11.9.2 Acceptable Methods of Verification

Acceptable methods of verifying the Certificate Approver's approval of an EV Certificate Request include:

(1) Contacting the Certificate Approver by phone or mail at a verified phone number or address for the Applicant and obtaining oral or written confirmation that the Certificate Approver has reviewed and approved the EV Certificate Request;

(2) Notifying the Certificate Approver that one or more new EV Certificate Requests are available for review and approval at a designated access-controlled and secure Web site, followed by a login by, and an indication of approval from, the Certificate Approver in the manner required by the Web site; or

(3) Verifying the signature of the Certificate Approver on the EV Certificate Request in accordance with Section 11.8 of these Guidelines.

11.10 Verification of Certain Information Sources

11.10.1 Verified Legal Opinion

(1) **Verification Requirements:** Before relying on a legal opinion submitted to the CA, the CA MUST verify that such legal opinion meets the following requirements:

(A) **Status of Author:** The CA MUST verify that the legal opinion is authored by an independent legal practitioner retained by and representing the Applicant (or an in-house legal practitioner employed by the Applicant) (Legal Practitioner) who is either: 30

(i) A lawyer (or solicitor, barrister, advocate, or equivalent) licensed to practice law in the country of the Applicant's Jurisdiction of Incorporation or Registration or any jurisdiction where the Applicant maintains an office or physical facility, or
(ii) A notary that is a member of the International Union of Latin Notaries, and is licensed to practice in the country of the 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:** The CA MUST verify 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:** The CA MUST confirm the authenticity of the Verified Legal Opinion.
(2) **Acceptable Methods of Verification:** Acceptable methods of establishing the foregoing requirements for a Verified Legal Opinion are:
(A) **Status of Author:** The CA MUST verify 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;
(B) **Basis of Opinion:** The text of the legal opinion MUST make it clear that the Legal Practitioner is acting on behalf of the Applicant and that the conclusions of the legal opinion are based on the Legal Practitioner's stated familiarity with the relevant facts and the exercise of the practitioner's professional judgment and expertise. The legal opinion MAY also include disclaimers and other limitations customary in the Legal Practitioner's jurisdiction, provided that the scope of the disclaimed responsibility is not so great as to eliminate any substantial risk (financial, professional, and/or reputational) to the Legal Practitioner, should the legal opinion prove to be erroneous. An acceptable form of legal opinion is attached as Appendix B;
(C) **Authenticity:** To confirm the authenticity of the legal opinion, the CA MUST make a telephone call or send 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. If a phone number is not available from the licensing authority, the CA MAY use the number listed for the Legal Practitioner in records provided by the applicable phone company, QGIS, or QIIS.
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 the CA in Section 11.10.1 (2)(A), no further verification of authenticity is required.

11.10.2 Verified Accountant Letter

(1) **Verification Requirements:** Before relying on an accountant letter submitted to the CA, the CA MUST verify that such accountant letter meets the following requirements:
(A) **Status of Author:** The CA MUST verify that the accountant letter is authored by an independent Accounting Practitioner retained by and representing the Applicant (or an in-house professional accountant employed by the Applicant) who is a certified public accountant, chartered accountant, or has an equivalent license within the Applicant's Jurisdiction of Incorporation, Jurisdiction of Registration, or the jurisdiction where the Applicant maintains an office or physical facility. Verification of license MUST be through that jurisdiction's member of the International Federation of Accountants (IFAC) or through the regulatory organization in that jurisdiction appropriate to contact when verifying an accountant's license to practice in that jurisdiction.
(B) **Basis of Opinion:** The CA MUST verify that 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:** The CA MUST confirm the authenticity of the Verified Accountant Letter.
(2) **Acceptable Methods of Verification:** Acceptable methods of establishing the foregoing requirements for a Verified Accountant Letter are listed here. 31

(A) **Status of Author:** The CA MUST verify the professional status of the author of the accountant letter by directly contacting the authority responsible for registering or licensing such Accounting Practitioners in the applicable jurisdiction.
(B) **Basis of Opinion:** The text of the Verified Accountant Letter MUST make clear that the Accounting Practitioner is acting on behalf of the Applicant and that the information in the letter is based on the Accounting Practitioner's stated familiarity with the relevant facts and the exercise of the practitioner's professional judgment and expertise. The Verified Accountant Letter MAY also include disclaimers and other limitations customary in the Accounting Practitioner's jurisdiction, provided that the scope of the disclaimed responsibility is not so great as to eliminate any substantial risk (financial, professional, and/or reputational) to the Accounting Practitioner, should the Verified Accountant Letter prove to be erroneous. Acceptable forms of Verified Accountant Letter are attached as Appendix C.
(C) **Authenticity:** To confirm the authenticity of the accountant's opinion, the CA MUST make a telephone call or send a copy of the Verified 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 Practitioners and obtain confirmation from the Accounting Practitioner or the Accounting Practitioner's assistant that the accountant letter is authentic. If a phone number is not available from the licensing authority, the CA MAY use the number listed for the Accountant in records provided by the applicable phone company, QGIS, or QIIS.
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 the CA in Section 11.10.2 (2)(A), no further verification of authenticity is required.

11.10.3 Face-to-Face Validation

(1) **Verification Requirements:** Before relying on face-to-face vetting documents submitted to the CA, the CA MUST verify that the Third-Party Validator meets the following requirements:
(A) **Qualification of Third-Party Validator:** The CA MUST independently verify that the Third-Party Validator is a legally-qualified Latin Notary or Notary (or legal equivalent in the Applicant's jurisdiction), Lawyer, or Accountant in the jurisdiction of the individual's residency;
(B) **Document Chain of Custody:** The CA MUST verify that the Third-Party Validator viewed the Vetting Documents in a face-to-face meeting with the individual being validated;
(C) **Verification of Attestation:** If the Third-Party Validator is not a Latin Notary, then the CA MUST confirm the authenticity of the attestation and vetting documents.
(2) **Acceptable Methods of Verification:** Acceptable methods of establishing the foregoing requirements for vetting documents are:
(A) **Qualification of Third-Party Validator:** The CA MUST verify the professional status of the Third-Party Validator by directly contacting the authority responsible for registering or licensing such Third-Party Validators in the applicable jurisdiction;
(B) **Document Chain of Custody:** The Third-Party Validator MUST submit a statement to the CA which attests that they obtained the Vetting Documents submitted to the CA for the individual during a face-to-face meeting with the individual;
(C) **Verification of Attestation:** If the Third-Party Validator is not a Latin Notary, then the CA MUST confirm the authenticity of the vetting documents received from the Third-Party Validator. The CA MUST make a telephone call to the Third-Party Validator and obtain confirmation from them or their assistant that they performed the face-to-face validation. The CA 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 the CA in Section 11.10.3 (1)(A), no further verification of authenticity is required.

11.10.4 Independent Confirmation From Applicant

An Independent Confirmation from the 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: 32

(A) Received by the CA from a Confirming Person (someone other than the person who is the subject of the inquiry) that has the appropriate authority to confirm such a fact, and who represents that he/she has confirmed such fact;
(B) Received by the CA in a manner that authenticates and verifies the source of the confirmation; and
(C) Binding on the Applicant.
An Independent Confirmation from the Applicant MAY be obtained via the following procedure:
(1) **Confirmation Request:** The CA MUST initiate a Confirmation Request via an appropriate out-of-band communication, requesting verification or confirmation of the particular fact at issue as follows:
(A) **Addressee:** The Confirmation Request MUST be directed to:
(i) A position within the 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 QGIS, QIIS, QTIS, Verified Legal Opinion, Verified Accountant Letter, or by contacting the Applicant's Human Resources Department by phone or mail (at the phone number or address for the Applicant's Place of Business, verified in accordance with these Guidelines); or
(ii) The Applicant's Registered Agent or Registered Office in the Jurisdiction of Incorporation as listed in the official records of the Incorporating Agency, with instructions that it be forwarded to an appropriate Confirming Person; or
(iii) A named individual verified to be in the direct line of management above the Contract Signer or Certificate Approver by contacting the Applicant's Human Resources Department by phone or mail (at the phone number or address for the Applicant's Place of Business, verified in accordance with these Guidelines).
(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:
(1) The address of the Applicant's Place of Business as verified by the CA in accordance with these Guidelines, or
(2) The business address for such Confirming Person specified in a current QGIS, QTIS, QIIS, Verified Legal Opinion, or Verified Accountant Letter, or
(3) The address of the Applicant's Registered Agent or Registered Office listed in the official records of the Jurisdiction of Incorporation, or
(ii) By e-mail addressed to the Confirming Person at the business e-mail address for such person listed in a current QGIS, QTIS, QIIS, Verified Legal Opinion, or Verified Accountant Letter; or
(iii) By telephone call to the Confirming Person, where such person is contacted by calling the main phone number of the Applicant's Place of Business (verified in accordance with these Guidelines) and asking to speak to such person, and a person taking the call identifies him- or herself 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 QGIS, QTIS, QIIS, Verified Legal Opinion, or Verified Accountant Letter. The cover page must be clearly addressed to the Confirming Person.
(2) **Confirmation Response:** The CA MUST receive a response to the Confirmation Request from a Confirming Person that confirms the particular fact at issue. Such response MAY be provided to the CA by telephone, by e-mail, or by paper mail, so long as the CA can reliably verify that it was provided by a Confirming Person in response to the Confirmation Request.
(3) The CA MAY rely on a verified Confirming Person to confirm their own contact information: email address, telephone number, and facsimile number. The CA MAY rely on this verified contact information for future correspondence with the Confirming Person if:
(A) The domain of the e-mail address is owned by the Applicant and is the Confirming Person's own e-mail address and not a group e-mail alias; 33

(B) The Confirming Person's telephone/fax number is verified by the CA to be a telephone number that is part of the organization's telephone system, and is not the personal phone number for the person.

11.10.5 Qualified Independent Information Source

A Qualified Independent Information Source (QIIS) is a regularly-updated and current, 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. A commercial database is a QIIS if the following are true:

(1) Industry groups rely on the database for providing accurate location or contact information;

(2) The database distinguishes between self-reported data and data reported by independent information sources;

(3) The database provider identifies how frequently they update the information in their database;

(4) Changes in the data that will be relied upon will be reflected in the database in no more than 12 months; and

(5) The database provider uses authoritative sources independent of the Subject, or multiple corroborated sources, to which the data pertains.

Databases in which the CA or its owners or affiliated companies maintain a controlling interest, or in which any Registration Authorities or subcontractors to whom the CA has outsourced any portion of the vetting process (or their owners or affiliated companies) maintain any ownership or beneficial interest do not qualify as a QIIS. The CA MUST check the accuracy of the database and ensure its data is acceptable.

11.10.6 Qualified Government Information Source

A Qualified Government Information Source (QGIS) is a regularly-updated and current, 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 that it is 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. Nothing in these Guidelines shall prohibit the use of third-party vendors to obtain the information from the Government Entity provided that the third party obtains the information directly from the Government Entity.

11.10.7 Qualified Government Tax Information Source

A Qualified Government Tax Information Source is a Qualified Government Information Source that specifically contains tax information relating to Private Organizations, Business Entities or Individuals (e.g., the IRS in the United States).

11.11 Other Verification Requirements

11.11.1 High Risk Status

The requirements of Section 11.5 of the Baseline Requirements apply equally to EV Certificates.

11.11.2 Denied Lists and Other Legal Black Lists

(1) **Verification Requirements:** The CA MUST verify whether the Applicant, the Contract Signer, the Certificate Approver, the Applicant's Jurisdiction of Incorporation, Registration, or Place of Business:

(A) Is 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 the CA's jurisdiction(s) of operation; or

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

The CA MUST NOT issue any EV Certificate to the Applicant 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 on any such list.

(2) **Acceptable Methods of Verification:** The CA MUST take reasonable steps to verify with the following lists and regulations: 34

(A) If the CA has operations in the U.S., the CA MUST take reasonable steps to verify with the following US Government denied lists and regulations:
(i) BIS Denied Persons List - http://www.bis.doc.gov/dpl/thedeniallist.asp
(ii) BIS Denied Entities List - http://www.bis.doc.gov/Entities/Default.htm
(iii) US Treasury Department List of Specially Designated Nationals and Blocked Persons - http://www.treas.gov/ofac/t11sdn.pdf
(iv) US Government export regulations
(B) If the CA has operations in any other country, the CA MUST take reasonable steps to verify with all equivalent denied lists and export regulations (if any) in such other country.

11.11.3 Parent/Subsidiary/Affiliate Relationship

A CA verifying an Applicant using information of the Applicant's Parent, Subsidiary, or Affiliate, when allowed under section 11.4.1, 11.4.2, 11.5.1, or 11.6.1, MUST verify the Applicant's relationship to the Parent, Subsidiary, or Affiliate. Acceptable methods of verifying the Applicant's relationship to the Parent, Subsidiary, or Affiliate include the following:
(1) QIIS or QGIS: The relationship between the Applicant and the Parent, Subsidiary, or Affiliate is identified in a QIIS or QGIS;
(2) Independent Confirmation from the Parent, Subsidiary, or Affiliate: A CA MAY verify the relationship between an Applicant and a Parent, Subsidiary, or Affiliate by obtaining an Independent Confirmation from the appropriate Parent, Subsidiary, or Affiliate (as described in Section 11.10.4);
(3) Contract between CA and Parent, Subsidiary, or Affiliate: A CA MAY verify the relationship between an Applicant and a Parent, Subsidiary, or Affiliate by relying on a contract between the CA and the Parent, Subsidiary, or Affiliate that designates the Certificate Approver with such EV Authority, provided that the contract is signed by the Contract Signer and provided that the agency and Signing Authority of the Contract Signer have been verified;
(4) Legal Opinion: A CA MAY verify the relationship between an Applicant and a Parent, Subsidiary, or Affiliate by relying on a Verified Legal Opinion (as described in Section 11.10.1);
(5) Accountant Letter: A CA MAY verify the relationship between an Applicant and a Parent, Subsidiary, or Affiliate by relying on a Verified Accountant Letter (as described in Section 11.10.2); or
(6) Corporate Resolution: A CA MAY verify the relationship between an Applicant and a Subsidiary by relying on a properly authenticated corporate resolution that approves creation of the Subsidiary or the Applicant, provided that such resolution is (i) certified by the appropriate corporate officer (e.g., secretary), and (ii) the CA 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.

11.12 Final Cross-Correlation and Due Diligence

Except for Enterprise EV Certificates:
(1) The results of the verification processes and procedures outlined in these Guidelines are intended to be viewed both individually and as a group. Thus, after all of the verification processes and procedures are completed, the CA MUST have a person who is not responsible for the collection of information review all of the information and documentation assembled in support of the EV Certificate application and look for discrepancies or other details requiring further explanation.
(2) The CA MUST obtain and document further explanation or clarification from the Applicant, Certificate Approver, Certificate Requester, Qualified Independent Information Sources, and/or other sources of information, as necessary, to resolve those discrepancies or details that require further explanation.
(3) The CA MUST refrain from issuing an EV Certificate until the entire corpus of information and documentation assembled in support of the EV Certificate Request is such that issuance of the EV Certificate will not communicate factual information that the CA knows, or the exercise

of due diligence should discover from the assembled information and documentation, to be inaccurate,. If satisfactory explanation and/or additional documentation are not received within a reasonable time, the CA MUST decline the EV Certificate Request and SHOULD notify the Applicant accordingly. 35

(4) In the case where some or all of the documentation used to support the application is in a language other than the CA's normal operating language, the CA or its Affiliate MUST perform the requirements of this Final Cross-Correlation and Due Diligence section using employees under its control and having appropriate training, experience, and judgment in confirming organizational identification and authorization and fulfilling all qualification requirements contained in Section 14.1 of these Guidelines. When employees under the control of the CA do not possess the language skills necessary to perform the Final Cross-Correlation and Due Diligence a CA MAY:
(A) Rely on language translations of the relevant portions of the documentation, provided that the translations are received from a Translator; or
(B) When the CA has utilized the services of an RA, the CA MAY rely on the language skills of the RA to perform the Final Cross-Correlation and Due Diligence, provided that the RA complies with Section 11.12, Subsections (1), (2) and (3). Notwithstanding the foregoing, prior to issuing the EV Certificate, the CA MUST review the work completed by the RA and determine that all requirements have been met; or
(C) When the CA has utilized the services of an RA, the CA MAY rely on the RA to perform the Final Cross-Correlation and Due Diligence, provided that the RA complies with this section and is subjected to the Audit Requirements of Sections 17.5 and 17.6.
In the case of Enterprise EV Certificates to be issued in compliance with the requirements of Section 14.2 of these Guidelines, the Enterprise RA MAY perform the requirements of this Final Cross-Correlation and Due Diligence section.

11.13 Requirements for Re-use of Existing Documentation

11.13.1 For Validated Data

(1) The age of validated data used to support issuance of an EV Certificate (before revalidation is required) SHALL NOT exceed the following limits:
(A) Legal existence and identity – thirteen months;
(B) Assumed name – thirteen months;
(C) Address of Place of Business – thirteen months, but thereafter data MAY be refreshed by checking a Qualified Independent Information Source, even where a site visit was originally required;
(D) Telephone number for Place of Business – thirteen months;
(E) Bank account verification – thirteen months;
(F) Domain Name – thirteen months;
(G) Identity and authority of Certificate Approver – thirteen months, unless a contract is in place between the CA 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 the contract expires or is terminated.
(2) The age of information used by the CA to verify such an EV Certificate Request MUST NOT exceed the Maximum Validity Period for such information set forth above in subsection (1), based on the date the information was last updated by the QIIS, QGIS, or QTIS (e.g., if an online database was accessed by the CA on July 1, but contained data last updated by the QIIS, QGIS, or QTIS on February 1 of the same year, then the date on which the information was obtained would be considered to be February 1).
(3) The CA MAY issue multiple EV Certificates listing the same Subject and based on a single EV Certificate Request, subject to the aging and updating requirement stated above.
(4) Each EV Certificate issued by the CA MUST be supported by a valid current EV Certificate Request and a Subscriber Agreement signed by the appropriate Applicant Representative on behalf of the Applicant or Terms of Use acknowledged by the appropriate Applicant Representative.
(5) In the case of outdated information, the CA MUST repeat the verification processes required in these Guidelines. 36

11.13.2 Validation for Existing Subscribers
In conjunction with an EV Certificate Request placed by an Applicant who is already a customer of the CA, the CA MUST perform all authentication and verification tasks required by these Guidelines to ensure that the request is properly authorized by the Applicant and that the information in the EV Certificate will still be accurate and valid.
11.13.3 Exceptions
Notwithstanding the requirements set forth in Section **Error! Reference source not found.**, when performing the authentication and verification tasks for issuing an EV Certificate where the Applicant has a current valid EV Certificate issued by the CA, a CA MAY:
(1) Rely on its prior authentication and verification of:
(A) The Principal Individual of a Business Entity under Section 11.2.2 (4) if the Principal Individual is the same as the Principal Individual verified by the CA in connection with the previously issued EV Certificate;
(B) The Applicant's Place of Business under Section 11.4.1;
(C) The telephone number of the Applicant's Place of Business required by Section 11.4.2, but still MUST perform the verification required by Section 11.4.2 (2)(A);
(D) The Applicant's Operational Existence under Section 11.5;
(E) The name, title, and authority of the Contract Signer, Certificate Approver, and Certificate Requester under Section 11.7, except where a contract is in place between the CA and the Applicant that specifies a specific term for the authority of the Contract Signer, and/or the Certificate Approver, and/or Certificate Requester in which case, the term specified in such contract will control;
(F) The email address used by the CA for independent confirmation from the Applicant under Section 11.10.4 (1)(B)(ii);
(2) Rely on a prior Verified Legal Opinion or Accountant Letter that established:
(A) The Applicant's exclusive right to use the specified Domain Name under Section 11.6.2 (2)(A)(i) and Section 11.6.2 (2)(B)(i), provided that the CA verifies that either:
(i) The WHOIS record still shows the same registrant as indicated when the CA received the prior Verified Legal Opinion or Verified Accountant Letter, or
(ii) The Applicant establishes domain control via a practical demonstration as detailed in Section 11.6.2(2)(B)(ii).
(B) That the Applicant is aware that it has exclusive control of the Domain Name, under Section 11.6.1 (3).
11.13.4 Validation of Re-issuance Requests
A CA may rely on previously verified information to issue a replacement certificate where:
(1) The expiration date of the replacement certificate is the same as the expiration date of the currently valid EV Certificate that is being replaced, and
(2) The Subject of the Certificate is the same as the Subject in the currently valid EV Certificate that is being replaced.
12 Certificate Issuance by a Root CA
Certificate issuance by the Root CA SHALL require an individual authorized by the CA (i.e. the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation.
Root CA Private Keys MUST NOT be used to sign EV Certificates. 37

13 Certificate Revocation and Status Checking

The requirements in Section 13 of the Baseline Requirements apply equally to EV Certificates. However, CAs MUST ensure that CRLs for an EV Certificate chain can be downloaded in no more than three (3) seconds over an analog telephone line under normal network conditions.

14 Employee and third party issues

14.1 Trustworthiness and Competence

14.1.1 Identity and Background Verification

Prior to the commencement of employment of any person by the CA for engagement in the EV Processes, whether as an employee, agent, or an independent contractor of the CA, the CA MUST:

(1) **Verify the Identity of Such Person:** Verification of identity MUST be performed through:
(A) The personal (physical) presence of such person before trusted 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 drivers licenses);
and
(2) **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 qualification obtained;
(D) Search of criminal records (local, state or provincial, and national) where allowed by the jurisdiction in which the person will be employed;
and
(3) In the case of employees already in the employ of the CA at the time of adoption of these Guidelines whose identity and background has not previously been verified as set forth above, the CA SHALL conduct such verification within three months of the date of adoption of these Guidelines.

14.1.2 Training and Skills Level

The requirements in Section 14.1.2 of the Baseline Requirements apply equally to EV Certificates and these Guidelines. The required internal examination must relate to the EV Certificate validation criteria outlined in these Guidelines.

14.1.3 Separation of Duties

(1) The CA MUST 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 Cross-Correlation and Due Diligence steps, as outlined in Section 11.12, MAY be performed by one of the persons. For example, one Validation Specialist MAY review and verify all the Applicant information and a second Validation Specialist MAY approve issuance of the EV Certificate.
(2) Such controls MUST be auditable. 38

14.2 Delegation of Functions to Registration Authorities and Subcontractors

14.2.1 General

The CA MAY delegate the performance of all or any part of a requirement of these Guidelines to an Affiliate or a Registration Authority (RA) or subcontractor, provided that the process employed by the CA fulfills all of the requirements of Section 11.12. Affiliates and/or RAs must conform with the qualification requirements of Section 14.1 of these Guidelines.

The CA SHALL verify that the Delegated Third Party's personnel involved in the issuance of a Certificate meet the training and skills requirements of Section 14 and the document retention and event logging requirements of Section 15.

14.2.2 Enterprise RAs

The CA MAY contractually authorize the Subject of a specified Valid EV Certificate to perform the RA function and authorize the CA to issue additional EV Certificates at third and higher domain levels that are contained within the domain of the original EV Certificate (also known as an Enterprise EV Certificate). In such case, the Subject SHALL be considered an Enterprise RA, and the following requirements SHALL apply:

(1) An Enterprise RA SHALL NOT authorize the CA to issue an Enterprise EV Certificate at the third or higher domain levels to any Subject other than the Enterprise RA or a business that is owned or directly controlled by the Enterprise RA;

(2) In all cases, the Subject of an Enterprise EV Certificate MUST be an organization verified by the CA in accordance with these Guidelines;

(3) The CA MUST impose these limitations as a contractual requirement with the Enterprise RA and monitor compliance by the Enterprise RA;

(4 The Final Cross-Correlation and Due Diligence requirements of Section 11.12 of these Guidelines MAY be performed by a single person representing the Enterprise RA; and

(5) The audit requirements of Section 17.1 of these Guidelines SHALL apply to the Enterprise RA, except in the case where the CA maintains control over the Root CA Private Key or Subordinate CA Private Key used to issue the Enterprise EV Certificates, in which case, the Enterprise RA MAY be exempted from the audit requirements.

14.2.3 Guidelines Compliance Obligation

In all cases, the CA MUST contractually obligate each Affiliate, RA, subcontractor, and Enterprise RA to comply with all applicable requirements in these Guidelines and to perform them as required of the CA itself. The CA SHALL enforce these obligations and internally audit each Affiliate's, RA's, subcontractor's, and Enterprise RA's compliance with these Requirements on an annual basis.

14.2.4 Allocation of Liability

As specified in Section 14.2.4 of the Baseline Requirements.

15 Data Records

As specified in Section 15 of the Baseline Requirements.

16 Data Security

As specified in Section 16 of the Baseline Requirements. In addition, systems used to process and approve EV Certificate Requests MUST require actions by at least two trusted persons before creating an EV Certificate. 39

17 Audit

17.1 Eligible Audit Schemes

A CA issuing EV Certificates SHALL undergo an audit in accordance with one of the following schemes:

(i) WebTrust Program for CAs audit and WebTrust EV Program audit, or

(ii) ETSI TS 102 042 v2.1.1 audit.

If the CA is a Government Entity, an audit of the CA by the appropriate internal government auditing agency is acceptable in lieu of the audits specified above, provided that such internal government auditing agency publicly certifies in writing that its audit addresses the criteria specified in one of the above audit schemes and certifies that the government CA has successfully passed the audit.

EV audits MUST cover all CA obligations under these Guidelines regardless of whether they are performed directly by the CA or delegated to an RA or subcontractor.

17.2 Audit Period

CAs issuing EV Certificates MUST undergo an annual audit that meets the criteria of Section 17.1.

17.3 Audit Record

CAs SHOULD make its audit report publicly available no later than three months after the end of the audit period. If there is a delay greater than three months and if so requested by an Application Software Supplier, the CA MUST provide an explanatory letter signed by its auditor.

17.4 Pre-Issuance Readiness Audit

(1) If the CA has a currently valid WebTrust Seal of Assurance for CAs, then, before issuing EV Certificates, the CA and its Root CA MUST successfully complete a point-in-time readiness assessment audit against the WebTrust EV Program.

(2) If the CA has a currently valid ETSI 102 042 audit, then, before issuing EV Certificates, the CA and its Root CA MUST successfully complete a point-in-time readiness assessment audit against ETSI TS 102 042 V2.1.1.

(3) If the CA does not have a currently valid WebTrust Seal of Assurance for CAs or an ETSI 102 042 audit, then, before issuing EV Certificates, the CA and its Root CA MUST successfully complete either: (i) a point-in-time readiness assessment audit against the WebTrust for CA Program, or (ii) a point-in-time readiness assessment audit against the WebTrust EV Program, or an ETSI TS 102 042 V2.1.1. audit.

The CA MUST complete any required point-in-time readiness assessment no earlier than twelve (12) months prior to issuing an EV Certificate. The CA MUST undergo a complete audit under such scheme within ninety (90) days of issuing the first EV Certificate.

17.5 Regular Self Audits

During the period in which it issues EV Certificates, the CA MUST strictly control its service quality by performing ongoing self audits against a randomly selected sample of at least three percent of the EV Certificates it has issued in the period beginning immediately after the last sample was taken. For all EV Certificates where the Final Cross-Correlation and Due Diligence requirements of Section 11.12 of these Guidelines is performed by an RA, the CA MUST strictly control its service quality by performing ongoing self audits against a randomly selected sample of at least six percent of the EV Certificates it has issued in the period beginning immediately after the last sample was taken.

17.6 Auditor Qualification

A Qualified Audit (as defined in Section 17.6 of the Baseline Requirements) MUST perform the CA’s audit. 40

17.7 Root CA Key Pair Generation

All requirements in Section 17.7 of the Baseline Requirements apply equally to EV Certificates. However, for Root CA Key Pairs generated after the release of these Guidelines, the Root CA Key Pair generation ceremony MUST be witnessed by the CA's Qualified Auditor in order to observe the process and the controls over the integrity and confidentiality of the Root CA Key Pairs produced. The Qualified Auditor MUST then issue a report opining that the CA, during its Root CA Key Pair and Certificate generation process:

□□□□□Documented its Root CA key generation and protection procedures in its Certificate Policy, and its Certification Practices Statement;

□□□□□Included appropriate detail in its Root Key Generation Script;

□□□□□Maintained effective controls to provide reasonable assurance that the Root CA key pair was generated and protected in conformity with the procedures described in its CP/CPS and with its Root Key Generation Script;

□□□□□Performed, during the Root CA key generation process, all the procedures required by its Root Key Generation Script.

18 Liability and Indemnification

CAs MAY limit their liability as described in Section 18 of the Baseline Requirements except that a CA MAY NOT limit its liability to Subscribers or Relying Parties for legally recognized and provable claims to a monetary amount less than two thousand US dollars per Subscriber or Relying Party per EV Certificate.

A CA's indemnification obligations and a Root CA's obligations with respect to subordinate CAs are set forth in the Baseline Requirements. 41

Appendix A - User Agent Verification (Normative)

The CA MUST host test Web pages that allow Application Software Suppliers to test their software with EV Certificates that chain up to each EV Root Certificate. At a minimum, the CA MUST host separate Web pages using certificates that are (i) valid (ii) revoked and (iii) expired.
42

Appendix B - Sample Legal Opinion Confirming Specified Information (Informative)
[Law Firm Letterhead]

[Date] To:	***[Name of Issuing Certification Authority] [Address / fax number of Issuing CA – may be sent by fax or email attachment]***
Re:	**EV Certificate Request No.** ***[CA Reference Number]***
Client:	***[Exact company name of Client – see footnote 1]***
Client Representative:	***[Exact name of Client Representative who signed the Application – see footnote 2]***
Application Date:	***[Insert date of Client's Application to the Issuing CA,]***

Appendix B2: Minimum Cryptographic Algorithm and Key Sizes for EV Certificates

Minimum Cryptographic Algorithm and Key Sizes for EV Certificates

1. Root CA Certificates

	Key Sizes
Digest algorithm	SHA1*, SHA-256, SHA-384 or SHA-512
RSA	2048
ECC	256 or 384

2. Subordinate CA Certificates

	Key Sizes
Digest algorithm	SHA1*, SHA-256, SHA-384 or SHA-512
RSA	2048
ECC	256 or 384

3. Subscriber Certificates

	Key Sizes
Digest algorithm	SHA1*, SHA-256, SHA-384 or SHA-512
RSA	2048
ECC	256 or 384

*SHA-1 shall be used until SHA-256 is supported widely by browsers used by a majority of Relying Parties worldwide.

Appendix B3: EV Certificates Required Certificate Extensions

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.

(c) certificatePolicies
This extension SHOULD NOT be present.

(d) extendedKeyUsage
This extension is not present.

All other fields and extensions are set in accordance to RFC *5280*.

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 EV policy.

certificatePolicies:policyIdentifier (Required)

- the ***anyPolicy*** if subordinate CA is controlled by the GeoTrust Root CA

(b) cRLDistributionPoint
is always present and NOT marked critical. It contains the HTTP URL of the CA's CRL service.

(c) authorityInformationAccess
MUST 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 SHOULD be included for the CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2).

(d) basicConstraints
This extension MUST be present and MUST be marked critical 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 MUST BE set in accordance to RFC *5280.*

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 EV policy.

certificatePolicies:policyIdentifier (Required)
- EV policy OID

certificatePolicies:policyQualifiers:policyQualifierId (Required)
- id-qt 2 [RFC *5280*]

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

(b) cRLDistributionPoint
is always present and NOT marked critical. It contains the HTTP URL of GeoTrust's CRL service.

(c) authorityInformationAccess
is always present and NOT 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).

(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.

(f) extKeyUsage
Either the ***value id-kp-serverAuth*** [RFC5280] or ***id-kp-clientAuth*** [RFC5280] or both values MUST be present. Other values SHOULD NOT be present.

(g) SubjectAltName (optional)
If present is populated in accordance with RFC5280 and criticality is set to FALSE.

All other fields and extensions set in accordance to RFC *5280.*

Appendix B4: Foreign Organization Name Guidelines

Foreign Organization Name Guidelines

NOTE: This appendix is only relevant to EV applications from countries that do not have Latin character organization name registrations. More specific information for particular countries may be added to this appendix in the future.

Where an EV Applicant's organization name is not registered with a QGIS in Latin characters and the applicant's foreign character organization name and registration have been verified with a QGIS in accordance with these Guidelines, GeoTrust MAY include a Latin character organization name in the EV certificate. In such a case, GeoTrust will follow the procedures laid down in this appendix.

Romanized Names
In order to include a transliteration/Romanization of the registered name, the Romanization will be verified by GeoTrust using a system officially recognized by the Government in the Applicant's jurisdiction of incorporation.

If GeoTrust can not rely on a transliteration/Romanization of the registered name using a system officially recognized by the Government in the Applicant's jurisdiction of incorporation, then it MUST rely on one of the options below, in order of preference:

- A system recognized by the International Standards Organization (ISO),
- A system recognized by the United Nations or
- A Lawyers Opinion confirming the Romanization of the registered name.

English Name
In order to include a Latin character name that is not a Romanization of the registered name in the EV certificate, GeoTrust will verify that the Latin character name is:

- Included in the Articles of Incorporation (or equivalent document) filed as part of the organization registration, or
- Recognized by a QGTIS in the Applicant's Jurisdiction of Incorporation as the applicant's recognized name for tax filings, or
- Confirmed with a QIIS to be the name associated with the registered organization, or
- Confirmed by a lawyer's opinion letter to be the trading name associated with the registered organization.

Country Specific Procedures

F-1. Japan
In addition to the procedures set out above:

- The Hepburn method of Romanization is acceptable for Japanese Romanizations.
- GeoTrust MAY verify the Romanized transliteration of Applicant's formal legal name with either a QIIS or a lawyer's opinion letter.
- GeoTrust MAY use the Financial Services Agency to verify an English Name. When used, GeoTrust will verify that the English name is recorded in the audited Financial Statements filed with the Financial Services Agency.

- When relying on Articles of Incorporation to verify an English Name, the Articles of Incorporation MUST be accompanied either: by a document, signed with the original Japanese Corporate Stamp, that proves that the Articles of Incorporation are authentic and current, or by a lawyer's opinion letter. GeoTrust will verify the authenticity of the Corporate Stamp.

Appendix C:

Supplemental Validation Procedures for Extended Validation (EV) Code-Signing Certificates

Reference: *CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation (EV) Code Signing Certificates, www.cabforum.org .*

Table of Contents

1. INTRODUCTION

These procedures for Extended Validation Certificates document 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 Extended Validation Certificates ("EV Certificates") used for EV signatures in code-signing. Such EV code-signing attests to only one level of assurance in code.

Subject Organization information from Valid EV Code Signing Certificates may be displayed in a special manner by certain relying-party software applications in order to provide users with a trustworthy confirmation of the identity of the entity providing the code signing services.

2. PURPOSE

2.1 Purpose of EV Code Signing Certificates

EV Code Signing ("EV CS") Certificates and signatures are intended to be used to verify the identity of the certificate holder (Subscriber) and the integrity of its code. They provide assurance to a user or platform provider that code verified with the certificate has not been modified from its original form and is distributed by the legal entity identified in the EV Code Signing Certificate by name, Place of Business address, Jurisdiction of Incorporation or Registration, and other information. EV Code Signing Certificates may help to establish the legitimacy of signed code, help to maintain the trustworthiness of software platforms, help users to make informed software choices, and limit the spread of malware.

The EV Code Signing Certificate does not identify a particular software object, but only its distributor.

2.1.1 Secondary Purposes

As specified in Section 2.1, Appendix B1, EV SSL Certificates.

2.1.2 Excluded Purposes

EV CS Certificates focus only on assuring the identity of the Subscriber and that the signed code has not been modified from its original form. EV Code Signing Certificates are ***not*** intended to provide any other assurances, representations, or warranties. Specifically, EV Code Signing Certificates do not warrant that code is free from vulnerabilities, malware, bugs, or other problems. EV Code Signing Certificates do not warrant or represent that:

i. The Subject named in the EV Code Signing Certificate is actively engaged in doing business;
ii. The Subject named in the EV Code Signing Certificate complies with applicable laws;
iii. The Subject named in the EV Code Signing Certificate is trustworthy, honest, or reputable in its business dealings; or
iv. It is "safe" to install code distributed by the Subject named in the EV Code Signing Certificate.

3. REFERENCES

Refer to *References* provided in the CA/Browser Forum EV Code-Signing Guidelines located *http://cabforum.org/documents.html*.

4. DEFINITIONS

Refer to *Definitions* provided in the CA/Browser Forum EV Code-Signing Guidelines located at *http://cabforum.org/documents.html*.

5. ABBREVIATIONS AND ACRONYMS

Refer to *Abbreviations and Acronyms* provided in the CA/Browser Forum EV Code-Signing Guidelines located at *http://cabforum.org/documents.html*.

6. CONVENTIONS

No stipulation.

7. CERTIFICATE WARRANTIES AND REPRESENTATIONS

7.1 EV Code Signing Certificate Warranties

When GeoTrust issues an EV Code Signing Certificate, the GeoTrust Issuing and Root CA represents and warrants to the Certificate Beneficiaries listed in Section 7.1.1, Appendix D, Supplemental Baseline Requirements, during the period when the EV Code Signing Certificate is Valid, that GeoTrust has followed the requirements of these Guidelines and its EV Policies in issuing and managing the EV Code Signing Certificate and in verifying the accuracy of the information contained in the EV Code Signing Certificate.

These warranties specifically include, but are not limited to, the following:

(A) **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 Code Signing Object was issued, the Subject of the EV Code Signing Object legally exists as a valid organization or entity in the Jurisdiction of Incorporation or Registration;

(B) **Identity:** GeoTrust has confirmed that, as of the date the EV Code Signing Object was issued, the legal name of the Subject named in the EV Code Signing Object 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;

(C) **Authorization for EV Code Signing Certificate:** GeoTrust has taken all steps reasonably necessary to verify that the Subject of the EV Code Signing Object authorized the issuance of the EV Code Signing Object;

(D) **Accuracy of Information:** GeoTrust has taken all steps reasonably necessary to verify that all of the other information in the EV Code Signing Object is accurate, as of the date

of issuance;

(E) **Subscriber Agreement:** The Subject of the EV Code Signing Object has entered into a legally valid and enforceable Subscriber Agreement with GeoTrust that satisfies the requirements of these Guidelines or, if they are affiliated, the Applicant Representative has acknowledged and accepted the Terms of Use;

(F) **Status:** The Issuer 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 Code Signing Object as Valid or revoked; and

(G) **Revocation:** GeoTrust will follow the requirements of these Guidelines and revoke the EV Code Signing Object for any of the revocation reasons specified in these Guidelines.

7.2 By the Applicant

Applicants make the commitments and warranties set forth in Section 10.3.2 of this Appendix for the benefit of the Issuer and the Certificate Beneficiaries.

8. COMMUNITY AND APPLICABILITY

8.1 Issuance of EV Code Signing Certificates

When issuing EV CS Certificates, GeoTrust shall at all times satisfy the requirements as required by the Guidelines and set forth in this Appendix.

GeoTrust shall at all times conform with all laws applicable to its business and the certificates it issues in each jurisdiction where it operates. GeoTrust shall notify the CA / Browser Forum of any occasions whereby a court or government body with jurisdiction over the activities (operations or certificate issuances) that are covered by the Guidelines determines that the performance of any mandatory requirement is deemed illegal subject to the laws of that jurisdiction..

8.2 EV Code Signing Policies

8.2.1 Implementation

The GeoTrust CPS, together with this Supplemental Appendix C to the GeoTrust CPS:

- Implements the requirements of the Guidelines as they are revised from time-to-time;
- Implements 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;
- Specifies GeoTrust'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 *www.geotrust.com/ev*

8.2.2 Disclosure

GeoTrust publicly discloses its EV Policies through this CPS that is available on a 24x7 basis from the GeoTrust online repository. The GeoTrust CPS is structured according to the RFC 3647 format.

GeoTrust publicly discloses its CA business practices through an annual WebTrust for CAs Audit in accordance with section 8 of this CPS.

8.3 Commitment to Conform with Recommendations

GeoTrust conforms to the current version of the CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Code Signing Certificates published at *www.cabforum.org*. In the event of any inconsistency between this document and those Guidelines, those Guidelines take precedence over this document.

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

8.4 Insurance

GeoTrust maintains insurance as specified in Section 8.4, Appendix B1, EV SSL Certificates.

8.5 Obtaining EV Code Signing Certificates

GeoTrust only issues EV Code Signing Certificates to Applicants that meet the requirements specified in Section 8.5, Appendix B1, EV SSL Certificates.

9. EV CERTIFICATE CONTENT AND PROFILE

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

9.1 Issuer Information

An EV Code Signing Certificate MUST include Issuer information as specified by Baseline Requirements for publicly trusted Certificates and set forth in Section 9.1, Issuer Information, Appendix D, Supplemental Baseline Requirements.

9.2 Subject Information

EV Code Signing Objects issued to Subscribers MUST include the following information about the Subject organization in the fields listed:

9.2.1 Subject Organization Name Field

As specified in Section 9.2.1, Appendix B1, EV SSL Certificates.

9.2.2 Subject Alternative Name Extension

This field should not be included in the EV Code Signing Objects.

9.2.3 Subject Common Name Field

Certificate field: subject:*commonName* (OID: 2.5.4.3)

Required/Optional: Deprecated (Discouraged, but not prohibited)
Contents: If present, this field MUST NOT contain a Domain Name.

9.2.4 Subject Business Category Field

As specified in Section 9.2.4, Appendix B1, EV SSL Certificates.

9.2.5 Subject Jurisdiction of Incorporation or Registration Field

As specified in Section 9.2.5, Appendix B1, EV SSL Certificates.

9.2.6 Subject Registration Number Field

As specified in Section 9.2.6, Appendix B1, EV SSL Certificates.

9.2.7 Subject Physical Address of Place of Business Field

As specified in Section 9.2.7, Appendix B1, EV SSL Certificates.

9.2.8 Other Subject Attributes

All other optional attributes, when present within the subject field, MUST contain information that has been verified by GeoTrust. Optional subfields within the Subject field MUST either contain information verified by the Issuer or MUST be left empty. Metadata such as '.', '-', and ' ' characters, and/or any other indication that the field is empty, absent or incomplete, MUST not be used.

9.3 Certificate Policy Identification

As specified in Section 9.3, Appendix B1, EV SSL Certificates.

9.4 Maximum Validity Period For EV Code Signing Certificate

The validity period for an EV Code Signing Certificate issued to a Subscriber MUST NOT exceed thirty-nine (39) months.

9.5 Subscriber Public Key

GeoTrust Certificates meet the requirements for algorithm type and key size as set forth in section 6.1.5 of this CPS. Minimum key algorithms and sizes for EV Certificates are set forth in Appendix B2.

9.6 Certificate Serial Number

GeoTrust CAs generate non-sequential certificate serial numbers that exhibit at least 20 bits of entropy.

9.7 Additional Technical Requirements for EV Code Signing Certificates

As specified in Section 9.7, Appendix B1, EV SSL Certificates, with the following exceptions:

(A) the Domain Name as required for EV SSL Certificates SHALL be omitted;

(B) the Certificate MUST include a *SubjectAltName*:*permanentIdentifier* which MUST contain the following:

1) The ISO 3166-2 country code corresponding Subject's Jurisdiction of Incorporation or Registration (CC), as specified in the *subject*:*jurisdictionOfIncorporationCountryName* field;

2) If applicable, the state, province, or locality of the Subject's Jurisdiction of Incorporation in uppercase characters as specified in the *subjectjurisdictionOfIncorporationLocalityName* or subject:*jurisdictionofIncorporationStateorProvinceName* field, expressed in an unabbreviated format (STATE);

3) The first one of the following that applies:
   a. The Registration Number as included in the *Subject*:*serialNumber* field (REG), or
   b. A date of Incorporation or Registration in YYYY-MM-DD format (DATE) and the Subject's Organization Name as included in the *organizationName* field (ORG), or
   c. A verifiable date of creation in YYYY-MM-DD format (DATE) and the Subject's Organization Name as included in the *organizationName* field (ORG), or
   d. the Subject's Organization Name as included in the *organizationName* field (O).

GeoTrust formats data in the *SubjectAltName*:*permanentIdentifier* extension using Unicode as follows: CC-STATE (if applicable)- REG or DATE (if available)-ORG (if REG is not present). Characters representing the organization name MUST be uppercase Unicode. Any included "-" characters MUST be Unicode 002D and any included spaces in REG, STATE, or ORG MUST be Unicode 0020.

GeoTrust MAY truncate or abbreviate an organization name included in this field to ensure that the combination does not exceed 64 characters provided that GeoTrust has checked this field in accordance with Section 11, Appendix B1, EV SSL Certificates such that a Relying Party will not be misled into thinking that they are dealing with a different organization. If this is not possible, GeoTrust MUST NOT issue the EV Code Signing Certificate.

(C) the *keyUsage* extension MUST be set as follows:
This extension MUST be present and MUST be marked critical. The bit position for *digitalSignature* MUST be set. All other bit positions SHOULD NOT be set; AND

(D) the extended keyUsage extension MUST be set as follows:
This extension MUST be present, and the value *id-kp-codeSigning* MUST be present. Other values SHOULD NOT be present.

10. EV CODE SIGNING CERTIFICATE REQUEST REQUIREMENTS

10.1 General Requirements

As specified in Section 10.1of Appendix B1, EV SSL Certificates.

10.2 EV Code Signing Certificate Request Requirements

As specified in Section 10.2 of Appendix B1, EV SSL Certificates.

10.3 Requirements for Subscriber Agreement and Terms of Use

10.3.1 General

Prior to issuing an EV Code Signing Certificate, GeoTrust obtains, for the express benefit of the Issuer and the Certificate Beneficiaries, either:

1. The Applicant's agreement to the Subscriber Agreement with the Issuer, or
2. The Applicant's agreement to the Terms of Use agreement.

Prior to the issuance of the EV Code Signing 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 Code Signing Certificate to be issued pursuant to the Certificate Request. A separate Subscriber Agreement may be used for each Certificate Request, or a single Subscriber Agreement may be used to cover multiple future Certificate Requests and resulting Certificates.

10.3.2 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:

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

2. **Protection of Private Key**: An obligation and warranty by the Applicant to take all reasonable measures 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 Certificate(s) (and any associated activation data or device, e.g. password or token);

3. **Acceptance of Certificate**: An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy;

4. **Use of the Certificate**: An obligation and warranty to not knowingly sign software that contains Suspect Code and use the EV Code Signing Certificate as follows:

    a. only to sign code that complies with the requirements set forth in these Guidelines;
    b. solely in compliance with all applicable laws;
    c. solely for authorized company business; and
    d. solely in accordance with the Subscriber Agreement;

5. **Reporting and Revocation**: An obligation and warranty to promptly cease using a Certificate and its associated Private Key, and promptly request GeoTrust to revoke the Certificate, in the event that:

   a. there is evidence that the certificate was used to sign suspect code;
   b. any information in the Certificate is, or becomes, incorrect or inaccurate; or
   c. there is any actual or suspected misuse or compromise of either the key activation data or the Subscriber's Private Key associated with the Public Key included in the Certificate;

6. **Termination of Use of Certificate**: An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise.

7. **Responsiveness**: An obligation to respond to GeoTrust's instructions concerning Key Compromise or Certificate misuse within a specified time period.

8. **Acknowledgment and Acceptance**: An acknowledgment and acceptance that GeoTrust is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber or Terms of Use Forum Guideline Agreement or if GeoTrust discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware.

11. VERIFICATION REQUIREMENTS

11.1 General Overview

This section sets forth Verification Requirements and Acceptable Methods of Verification for each such Requirement and the procedures used by GeoTrust to satisfy the requirements**.** Before issuing an EV Code Signing Certificate, GeoTrust ensures that all Subject organization information included in the EV Code Signing Certificate conforms to the requirements of, and has been verified in accordance with the EV Guidelines and matches the information confirmed and documented by GeoTrust pursuant to its verification processes set forth in sub-sections 11.2 through 11.13 following.

11.2 Verification of Applicant's Legal Existence and Identity

As specified in Section 11.2 of Appendix B1, EV SSL Certificates.

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

As specified in Section 11.3 of Appendix B1, EV SSL Certificates.

11.4 Verification of Applicant's Physical Existence

As specified in Section 11.4 of Appendix B1, EV SSL Certificates.

11.5 Verification of Applicant's Operational Existence

As specified in Section 11.5 of Appendix B1, EV SSL Certificates.

11.6 Verification of Applicant's Domain Name

Code Signing Certificates SHALL NOT include a Domain Name.

11.7 Verification of Name, Title and Authority of Contract Signer and Certificate Approver

As specified in Section 11.7 of Appendix B1, EV SSL Certificates.

11.8 Verification of Signature on Subscriber Agreement and EV Code Signing Certificate Requests

As specified in Section 11.8 of Appendix B1, EV SSL Certificates.

11.9 Verification of Approval of EV Code Signing Certificate Request

As specified in Section 11.9 of Appendix B1, EV SSL Certificates.

11.10 Verification of Certain Information Sources

As specified in Section 11.10 of Appendix B1, EV SSL Certificates.

11.11 Other Verification Requirements

As specified in Section 11.11 of Appendix B1, EV SSL Certificates.

11.12 Final Cross-Correlation and Due Diligence

As specified in Section 11.12 of Appendix B1, EV SSL Certificates.

11.13 Requirements for Re-use of Existing Documentation

As specified in Sections 9.7 and 11.13 of Appendix B1, EV SSL Certificates.

12. CERTIFICATE ISSUANCE BY A ROOT CA

GeoTrust enforces multi-person controls for certificate issuance by the Root CA. The Root CA Private Keys are not used to sign EV Code Signing Certificates[2].

13. CERTIFICATE REVOCATION AND STATUS CHECKING

As specified in Section 13 of Appendix B1, EV SSL Certificates, and additionally:

(A) Revocation Reasons: Subscribers are expected to not intentionally include Suspect Code in their signed software. Intentionally signing Suspect Code is a violation of the terms of the Subscriber Agreement, and will likely result in revocation of the EV Code Signing Object.

[2] Individual exceptions may be approved by GeoTrust for issuance of a Subscriber certificate by a GeoTrust Root CA.

(B) Revocation Status Information: GeoTrust provides accurate and up-to-date revocation status information for at least one year following the expiration of the associated certificate, and, upon request, for a period not less than one year beyond expiry of the EV Code Signing Certificate.

(C) Revocation Processing: Whenever practical, platforms should check the revocation status of the certificates that they rely upon. However, this is not always practical, for instance, when signed code has to be loaded earlier in the boot sequence than the network communication stack.

In the timestamp model, the platform should deviate from the RFC 5280 certification path validation algorithm and check the revocation status, not only of the timestamp certificate, but also of the Subscriber's EV Code Signing Certificate at the time of reliance rather than at the time the time-stamp was applied.

In addition to checking revocation status, where practical, platforms should consult blacklists of suspect software.

(D) Revocation Consequences: A certificate may have a one-to-one relationship with the software object that it verifies. In such cases, revocation of the certificate only invalidates the signature on the code that is suspect. If, on the other hand, a certificate has a one-to-many relationship with the software objects that it verifies, then revocation of the certificate invalidates the signatures on all those software objects, some of which may be perfectly sound.

(E) Responsiveness. GeoTrust responds to all plausible notices of Suspect Code in a signed software object that verifies with a certificate that GeoTrust has issued, by setting the revocation status of that certificate to 'revoked'.

14. EMPLOYEE AND THIRD PARTY ISSUES

14.1 Trustworthiness and Competence

As specified in Section 14.1 of Appendix B1, EV SSL Certificates.

14.2 Delegation of Functions to Registration Authorities and Subcontractors

GeoTrust shall not delegate the RA functions for EV Code Signing Certificates.

15. DATA RECORDS

GeoTrust records events in accordance with Section 15, Appendix D, Supplemental Baseline Requirements.

16. DATA SECURITY

GeoTrust implements a comprehensive security program in accordance with Section 16, Appendix D, Supplemental Baseline Requirements. In addition, GeoTrust requires actions by at least two trusted persons before creating an EV Code Signing Certificate.

In addition:

(1) not applicable.

(2) not applicable.

(3) GeoTrust CAs protect private keys in a FIPS 140-2 level 3 (or equivalent) crypto module as set forth in section 6.2.1 of this CPS.

(4) GeoTrust ensures that the Subscriber's private key is generated, stored and used in a crypto module that meets or exceeds the requirements of FIPS 140-2 level 2. GeoTrust ships the FIPS 140-2 level 2 crypto module along with necessary drivers to the Subscriber. The Subscriber installs the driver and visits the GeoTrust web page that generates keys only on a FIPS 140-2 level 2 device.

17. AUDIT

17.1 Eligible Audit Schemes

GeoTrust performs an annual WebTrust for Certification Authorities v2.0, or later, audit as set forth in section 8 of this CPS.

Such audits will cover all CA obligations under the CA/Browser Forum Guidelines regardless of whether they are performed directly by GeoTrust or delegated to an RA or subcontractor.

17.2 Audit Period

See Section 17.1.

17.3 Audit Record

See Section 17.1.

17.4 Pre-Issuance Readiness Audit

Not applicable.

17.5 Regular Self-Audits

GeoTrust and Affiliates undergo self-audits to monitor adherence to its Certificate Policy and CPS requirements and strictly control its service quality on at least a quarterly basis against a randomly selected sample of the greater of one Certificate or at least 3% of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

For all EV Code Signing Certificates where the Final Cross-Correlation and Due Diligence requirements of Section 11.12 of this Appendix is performed by an RA, GeoTrust strictly controls its service quality by performing ongoing self audits against a randomly selected sample of at least 6% of the EV Code Signing Certificates it has issued in the period beginning immediately after the last sample was taken.

17.6 Auditor Qualification

A Qualified Auditor (as defined in Section 8.2 of this CPS) performs GeoTrust's annual audit.

17.7 Root CA Key Pair Generation

As specified in Section 17.7 of Appendix B1, EV SSL Certificates.

18. LIABILITY AND INDEMNIFICATION

GeoTrust is subject to the liability and indemnification obligations as set forth in Section 16 of Appendix B1, EV SSL Certificates.

Appendix D

Supplemental Baseline Requirements for Issuance and Management of Publicly-Trusted Certificates

Reference: *CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, www.cabforum.org .*

Table of Contents

1. INTRODUCTION

This Appendix articulates supplemental procedures to the GeoTrust CPS for issuing Organization Validated (OV) Certificates and Domain Validated (DV) Certificates in conformance with the Baseline Requirement for Publicly Trusted Certificates ("Baseline Requirements"). Additionally, certain sections in this Appendix are referenced from GeoTrust's Supplemental Procedures for the issuance of EV SSL Certificates (Appendix B1) and EV Code-Signing Certificates (Appendix C). Baseline Requirements are published by the CA Browser Forum at *www.cabforum.org*, to describe certain of the minimum requirements that a Certificate Authority (CA) must meet in order to issue Publicly Trusted Certificates.

GeoTrust's OV and DV Certificates issued under the Supplemental Procedures in this Appendix are used for authenticating servers accessible through the Internet.

2. PURPOSE

As specified in section 2 of the CA/Browser Forum Baseline Requirements.

3. REFERENCES

As specified in section 3 of the CA/Browser Forum Baseline Requirements.

4. DEFINITIONS

As specified in section 4 of the CA/Browser Forum Baseline Requirements.

5. ABBREVIATIONS AND ACRONYMS

As specified in section 5 of the CA/Browser Forum Baseline Requirements.

6. CONVENTIONS

As specified in section 6 of the CA/Browser Forum Baseline Requirements.

7. CERTIFICATE WARRANTIES AND REPRESENTATION

7.1 By the CA

By issuing a Certificate, GeoTrust makes Certificate Warranties (as listed in section 7.1.2) to the Certificate Beneficiaries (as described in 7.1.1).

7.1.1 Certificate Beneficiaries

Certificate Beneficiaries of GeoTrust CAs include, but are not limited to:

- The Subscriber that is a party to the Subscriber Agreement for the Certificate;
- All Application Software Suppliers with whom the Root CA has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier; and

- All Relying Parties who reasonably rely on a Valid Certificate.

7.1.2 Certificate Warranties

The CA represents and warrants to the Certificate Beneficiaries that, during the period when the Certificate is valid, the CA has complied with these Requirements and its Certificate Policy and/or Certification Practice Statement in issuing and managing the Certificate. The Certificate Warranties specifically include, but are not limited to, the following:

1. Right to Use Domain Name or IP Address: That, at the time of issuance, the CA (i) implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Domain Name(s) and IP address(es) listed in the Certificate's subject field and *subjectAltName* extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;
2. Authorization for Certificate: That, at the time of issuance, the CA (i) implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;
3. Accuracy of Information: That, at the time of issuance, the CA (i) implemented a procedure for verifying the accuracy of all of the information contained in the Certificate (with the exception of the *subject*:*organizationalUnitName* attribute); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;
4. No Misleading Information: That, at the time of issuance, the CA (i) implemented a procedure for reducing the likelihood that the information contained in the Certificate's *subject*:*organizationalUnitName* attribute would be misleading; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;
5. Identity of Applicant: That, if the Certificate contains Subject Identity Information, the CA (i) implemented a procedure to verify the identity of the Applicant in accordance with Sections 3.1.1.1 and 3.2.2.1; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;
6. Subscriber Agreement: That, if the CA and Subscriber are not Affiliated, the Subscriber and CA are parties to a legally valid and enforceable Subscriber Agreement that satisfies these Requirements, or, if the CA and Subscriber are Affiliated, the Applicant Representative acknowledged and accepted the Terms of Use;
7. Status: That the CA maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates; and
8. Revocation: That the CA will revoke the Certificate for any of the reasons specified in these Requirements.

7.2 By the Applicant

GeoTrust requires that the Applicant makes the commitments and warranties set forth in section 10.3.2 of this Appendix for the benefit of the CA and the Certificate Beneficiaries.

8. COMMUNITY AND APPLICABILITY

8.1 Compliance

The GeoTrust CA complies with the requirements set forth in this Appendix. GeoTrust issues Certificates and operates its PKI in accordance with applicable law as set forth in section 9.15 of this CPS.

If a court of government body with jurisdiction over the activities covered by these Baseline Requirements determines that the performance of any mandatory requirement is illegal, then such requirement is considered reformed to the minimum extent necessary to make the requirement valid and legal. This applies only to operations or certificate issuances that are subject to the laws of that jurisdiction. The parties involved SHALL notify the CA / Browser Forum of the facts, circumstances and law(s) involved so that the CA/Browser Forum may revise the Baseline Requirements accordingly.

8.2 Certificate Policies

8.2.1 Implementation

GeoTrust develops. Implements, enforces and annually updates a Certificate Policy and Certificate Practice Statement that describes in detail how GeoTrust implements the latest version of the CA/Browser Forum Baseline Requirements.

8.2.2 Disclosure

GeoTrust publicly discloses Certificate Information via an online repository as set forth in section 2.2 that is readily available on a 24x7 basis. Such CA business practices are provided in accordance with RFC 3647 and the WebTrust for CAs Audit Scheme.

8.3 Commitment to Conform

CAs within the GeoTrust Trust Network hierarchy conform to the current version of the CA/Browser Forum (CABF) Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at *www.cabforum.org*. In the event of any inconsistency between this document and those Requirement, those Requirements take precedence over this document.

8.4 Trust Model

GeoTrust discloses all Cross-Certificates that identify a GeoTrust CA as the Subject. Such disclosures are provided in section 1 (Cross-Certification) of this CPS.

9. CERTIFICATE CONTENT AND PROFILE

9.1 Issuer Information

The following naming attributes shall be used to populate the Issuer Name in Certificates issued under this CPS:

9.1.1 Issuer Common Name Field (optional)

If the Issuer *commonName* (CN=) field is present, it must contain a name that accurately identifies the Issuing CA.

9.1.2 Issuer Domain Component Field

No stipulation.

9.1.3 Issuer Organization Name Field (required)

The *organizationName* (O=) field is required and contains the Issuer organization name (or abbreviation thereof), trademark, or other meaningful identifier for GeoTrust, that accurately identifies GeoTrust. The field must not contain a generic designation such as “Root” or “CA1”.

9.1.4 Issuer Country Name Field (required)

The *countryName* (C=) component is required and contains the two-letter ISO 3166-1 country code for the country in which the issuer’s place of business is located.

9.2 Subject Information

The following naming attributes shall be used to populate the Subject in Certificates issued under this CPS:

9.2.1 Subject Alternative Name Extensions (required)

The *subjectAlternativeName* extension is required and contains at least one entry. Each entry is either a *dNSName* containing the Fully-Qualified Domain Name or an *iPAddress* containing the IP address of a server. The GeoTrust CA confirms that the Applicant controls the Fully-Qualified Domain Name (FQDN) or IP address or has been granted the right to use it by the Domain Name Registrant or IP address assignee, as appropriate. Wildcard FQDNs are permitted.

Prior to the issuance of a Certificate with a *subjectAlternativeName* extension or Subject *commonName* field containing a Reserved IP Address or Internal Server Name, the GeoTrust CA notifies the Applicant that the use of such Certificates has been deprecated by the CA / Browser Forum and that the practice will be eliminated by October 2016. Also, as of July 1 2012, the GeoTrust CA shall not issue a certificate with an Expiry Date later than 1 November 2015 with a *subjectAlternativeName* extension or Subject *commonName* field containing a Reserved IP Address or Internal Server Name. Effective 1 October 2016, GeoTrust CAs shall revoke all unexpired Certificates whose *subjectAlternativeName* extension or Subject *commonName* field contains a Reserved IP Address or Internal Server Name.

9.2.2 Subject Common Name Field (optional)

The *commonName* (CN=) component is deprecated (discouraged, but not prohibited). If present, *commonName* contains a single IP address or Fully-Qualified Domain Name that is also one of the values contained in the Certificate’s *subjectAlternativeName* extension.

9.2.3 Subject Domain Component Field (optional)

The *domainComponent* (dc=) component is optional. If present, *domainComponent* contains all components of the subject's Registered Domain Name in ordered sequence, with the most significant component, closest to the root of the namespace, written last.

9.2.4 Subject Organization Name Field (optional)

If the *organizationName* (O=) field is present, the field contains the Subject's name or DBA and the required address fields contain a location of the Subject as verified in accordance with section 11.2.

If the Subject is a natural person, because Subject name attributes for individuals (e.g. *givenName* and surname) are not broadly supported by application software, the CA may use the *organizationName* field to convey the Subject's name or DBA (see 11.2 *Verification of Subject Identity Information*).

If the fields include discrepancies that the CA considers minor, such as common variations and abbreviations, then the CA shall document the discrepancy and shall use locally accepted abbreviations when abbreviating the organization name (e.g., if the official record shows "Company Name Incorporated", the CA may include "Company Name, Inc."). The *organizationName* field may include a verified DBA or tradename of the Subject.

If *organizationName* is present, then *localityName*, *stateOrProvinceName* (where applicable), and *countryName* shall also be required and *countryName* shall also be required and *streetAddress* and *postalCode* are optional. If *organizationName* is absent, then the Certificate shall not contain a *streetAddress*, *localityName*, *stateOrProvinceName*, or *postalCode* attribute. The CA may include the Subject's *countryName* field without including other Subject Identity Information pursuant to *countryName* requirements above.

9.2.5 Subject Country Name Field (optional)

If present, the *countryName* (C=) component shall be the two-letter ISO 3166-1 country code. If present, GeoTrust CAs shall verify the country associated with the Subject in accordance with section 11.2.5.

9.2.6 Other Subject Attributes

Optional attributes, when present in the subject field, must contain information that has been verified by the CA. Metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable, shall not be used.

GeoTrust shall not include Fully-Qualified Domain Names in Subject attributes except as specified for *subjectAlternativeName* and *CommonName* above.

***OrganizationalUnitName* (optional)**
The *OrganizationalUnitName* (OU=) component, when present, may contain information that has not been verified by the CA. Metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable, shall not be used.

GeoTrust implements a process that prevents an OU attribute from including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless GeoTrust has verified this information in accordance with section 11.2 and

the Certificate also contains subject:*organizationName*, subject:*localityName*, and subject:*countryName* attributes, also verified in accordance with section 11.2.5.

When an OU value is submitted in a Request, the value is subjected to a search of various high risk lists as per section 11.5, *High Risk Requests*. If a match is found, the value is reviewed by the RA to ensure that the value is accurate and not misleading. If the OU value identifies the name of a legal entity, the value is verified in accordance with section 11.2.

9.3 Certificate Policy Identification

9.3.1 Reserved Certificate Policy Identifiers

No stipulation.

9.3.2 Root CA Certificates

GeoTrust Root CA certificates shall not contain the *certificatePolices* extension.

9.3.3 Subordinate CA Certificates

GeoTrust Certificates contain the corresponding policy identifier specified in section 1.2 of the GeoTrust CPS that indicates the Certificate is issued and managed in compliance with the CA/Browser Forum Requirements.

The effective date ("Effective Date") of the CA/Browser Forum Baseline requirements is July 1, 2012.

After the Effective Date, a Certificate issued to a Subordinate CA that is not an Affiliate of the Issuing CA:

- must include the corresponding policy identifier identified in section 1.2 of the GeoTrust CPS that indicates the Subordinate CA's adherence to and compliance with these CA/Browser Forum Requirements, and
- must not contain the "*anyPolicy*" identifier (2.5.29.32.0).

After the Effective Date, a Certificate issued to a Subordinate CA that is an Affiliate of the Issuing CA:

- may include the corresponding policy identifier identified in section 1.2 of the GeoTrust CPS that indicates the Subordinate CA's adherence to and compliance with these CA/Browser Forum Requirements, and
- may contain the "*anyPolicy*" identifier (2.5.29.32.0) in place of the explicit policy identifier.

9.3.4 Subscriber Certificates

GeoTrust has assigned a reserved OID value, in section 1.2 of the GeoTrust CPS, for asserting conformance with the current version of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates. This OID value is reserved for use by any brand of GeoTrust CA as a means of asserting compliance with these CA/Browser Forum Requirements and as such does not distinguish a particular brand or class of Certificate.

GeoTrust's domain validated and organization validated SSL Certificates contain the corresponding OID value in section 1.2 of the GeoTrust CPS that indicates adherence to and compliance with the CA / Browser Forum Baseline Requirements.

9.4 Validity Period

GeoTrust's domain validated and organization validated SSL Certificates issued after the Effective Date[3] must have a Validity Period no greater than 48 months (4 years).

Except as provided for below, Certificates issued after 1 April 2015 must have a Validity Period no greater than 36 months (3 years). Beyond 1 April 2015, CAs may continue to issue Certificates with a Validity Period greater than 36 months but not greater than 48 months provided that the CA documents that the Certificate is for a system or software that:

a) was in use prior to the Effective Date;
b) is currently in use by either the Applicant or a substantial number of Relying Parties;
c) fails to operate if the Validity Period is shorter than 48 months;
d) does not contain known security risks to Relying Parties; and
e) is difficult to patch or replace without substantial economic outlay.

9.5 Subscriber Public Key

GeoTrust Certificates meet the requirements for algorithm type and key size as set forth in section 6.1.5 of this CPS. Minimum key algorithms and sizes for EV Certificates are set forth in Appendix B2.

9.6 Certificate Serial Number

GeoTrust generates a unique serial number value per Issuer DN that exhibits at least 20 bits of entropy.

9.7 Additional Technical Information

See Appendix B2 and Appendix B3.

10. CERTIFICATE APPLICATION

10.1 Documentation Requirements

Prior to the issuance of a Certificate, GeoTrust obtains the following documentation from the Applicant:

1. A certificate request, which may be electronic; and
2. An executed Subscriber Agreement, which may be electronic.

GeoTrust obtains any additional documentation necessary to meet these Requirements.

[3] The Effective Date of the CA Browser Forum requirements for OV and DV certificates is July 1, 2012.

10.2 Certificate Request

10.2.1 General

Prior to the issuance of a Certificate, GeoTrust obtains from the Applicant a certificate request in a form prescribed by GeoTrust that complies with these Requirements. One certificate request may suffice for multiple Certificates to be issued to the same Applicant, subject to the aging and updating requirement in Section 11.3, *Age of Certificate Data*, provided that each Certificate is supported by a valid, current certificate request signed by the appropriate Applicant Representative on behalf of the Applicant. The certificate request may be made, submitted and/or signed electronically.

10.2.2 Request and Certification

The certificate request must contain a request from, or on behalf of, the Applicant for the issuance of a Certificate, and a certification by, or on behalf of, the Applicant that all of the information contained therein is correct.

10.2.3 Information Requirements

The certificate request may include all factual information about the Applicant to be included in the Certificate, and such additional information as is necessary for GeoTrust to obtain from the Applicant in order to comply with these Requirements and GeoTrust's Certificate Policy and/or Certification Practice Statement. In cases where the certificate request does not contain all the necessary information about the Applicant, GeoTrust obtains the remaining information from the Applicant or, having obtained it from a reliable, independent, third-party data source, confirm it with the Applicant.

Applicant information must include, but not be limited to, at least one Fully-Qualified Domain Name or IP address to be included in the Certificate's *SubjectAltName* extension.

10.2.4 Subscriber Private Key

Parties other than the Subscriber shall not archive the Subscriber Private Key.

If GeoTrust or any of its designated RAs become aware that a Subscriber's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subscriber, then GeoTrust shall revoke all certificates that include the Public Key corresponding to the communicated Private Key.

10.3 Subscriber Agreement

10.3.1 General

Prior to the issuance of a 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 for a Certificate to be issued pursuant to a Certificate Request.

GeoTrust implements a process to ensure that each Subscriber Agreement is legally enforceable against the Applicant. In either case, the Agreement must apply to the Certificate to be issued pursuant to the certificate request.

GeoTrust uses an electronic or "click-through" Agreement; such agreements are legally enforceable. A separate Agreement may be used for each certificate request, or a single Agreement may be used to cover multiple future certificate requests and the resulting Certificates, so long as each Certificate that GeoTrust issues to the Applicant is clearly covered by that Subscriber Agreement.

10.3.2 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 Certificate Request and as otherwise requested by GeoTrust in connection with the issuance of the 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 Certificate(s) (and any associated access information or device – e.g., password or token);
- Acceptance of 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 Certificate;
- Use of Certificate: An obligation and warranty to install the Certificate only on the server accessible at the domain name listed on the Certificate, and to use the 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 a Certificate and its associated Private Key, and promptly request GeoTrust to revoke the 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 Certificate;
- Termination of Use of Certificate. An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key listed in a Certificate upon expiration or revocation of that Certificate.
- Responsiveness: An obligation to respond to GeoTrust's instructions concerning Key Compromise or Certificate misuse within a specified time period.
- Acknowledgment and Acceptance: An acknowledgment and acceptance that GeoTrust is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber or Terms of Use Agreement or if GeoTrust discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware.

11. VERIFICATION PRACTICES

11.1 Authorization of Domain Name Registrant

GeoTrust confirms that, as of the date the Certificate was issued, the Applicant either had the right to use, or had control of, the Fully-Qualified Domain Name(s) and IP address(es) listed in the Certificate, or was authorized by a person having such right or control (e.g. under a Principal-Agent or Licensor-Licensee relationship) to obtain a Certificate containing the Fully-Qualified Domain Name(s) and IP address(es).

When relying on a confirmation of the right to use or control the Registered Domain Name(s) from a Domain Name Registrar, and the top-level Domain is a two-letter country code (ccTLD), GeoTrust obtains the confirmation directly from the Domain Name Registrar for the Domain Name level to which the rules of the ccTLD apply. For example, if the requested FQDN is www.mysite.users.example.co.uk, then GeoTrust obtains confirmation from the Domain Name Registrant of the Domain Name example.co.uk, because applications for Domain Names immediately subordinate to .co.uk are governed by the rules of the .uk registry.

When using the Internet mail system to confirm that the Applicant has authorization from the Domain Name Registrant to obtain a Certificate for the requested Fully-Qualified Domain Name, GeoTrust uses a mail system address formed in one of the following ways:

1. Supplied by the Domain Name Registrar;
2. Taken from the Domain Name Registrant's "registrant", "technical", or "administrative" contact information, as it appears in the Domain's WHOIS record; or;
3. By pre-pending a local part to a Domain Name as follows:
    a. Local part - One of the following: 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster'; and
    b. Domain Name – Formed by pruning zero or more components from the Registered Domain Name or the requested Fully-Qualified Domain Name.

If the Domain Name Registrant has used a private, anonymous, or proxy registration service, and GeoTrust relies upon a Domain Authorization as an alternative to the foregoing, the Domain Authorization must be received directly from the private, anonymous, or proxy registration service identified in the WHOIS record for the Registered Domain Name. The document must contain the letterhead of the private, anonymous, or proxy registration service, the signature of the General Manager, or equivalent, or an authorized representative of such officer, dated on or after the certificate request date, and the Fully-Qualified Domain Name(s) to be included in the Certificate.

If the WHOIS record identifies the private, anonymous, or proxy registration service as the Domain Name Registrant, then the Domain Authorization must contain a statement granting the Applicant the right to use the Fully-Qualified Domain Name in a Certificate. GeoTrust contacts the private, anonymous, or proxy registration service directly, using contact information obtained from a reliable, independent, third-party data source, and obtain confirmation from the Domain Name Registrant that the Domain Authorization is authentic.

11.2 Verification of Subject Identity Information

If the Applicant requests a Certificate that will contain Subject identity Information comprised only of the *countryName* field, then GeoTrust will verify the country associated with the Subject in accordance with section 11.2.5.

If the Applicant requests a Certificate that will contain the *countryName* field and other Subject Identity Information, then GeoTrust verifies the identity of the Applicant, and the authenticity of the Applicant Representative's certificate request using a verification process meeting the following sets of requirements. GeoTrust inspects any document relied upon under this Section for alteration or falsification.

11.2.1 Identity

If the Subject Identity Information is to include the name or address of an organization, GeoTrust verifies the identity and address of the organization and that the address is the Applicant's address of existence or operation. GeoTrust verifies the identity and address of the Applicant using documentation provided by, or through communication with, at least one of the following:

1) A government agency (e.g, Secretary of State) in the jurisdiction of the Applicant's legal creation, existence, or recognition;
2). An external third party database (e.g. Dun and Bradstreet database) that is periodically updated, which GeoTrust has evaluated in accordance with Data Source Accuracy (below);
3). A site visit by the GeoTrust CA or a third party who is acting as an agent for the CA; or
4) An Attestation Letter.

GeoTrust may use the same documentation or communication described in 1 through 4 above to verify both the Applicant's identity and address.

Alternatively, GeoTrust may verify the address of the Applicant (but not the identity of the Applicant) using a utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that meets the requirements of Data Source Accuracy in section 11.6.

11.2.2 DBA/Tradename

If the Subject Identity Information includes a DBA or tradename, GeoTrust verifies the Applicant's right to use the DBA/tradename using at least one of the following:

1. Documentation provided by, or communication with, a government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
2. Documentation or communication provided by a third party source that meets the requirements of Data Source Accuracy in section 11.6;
3. Communication with a government agency responsible for the management of such DBAs or tradenames;
4. An Attestation Letter accompanied by documentary support that meets the requirements of Data Source Accuracy (below); or
5. A utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that meets the requirements of Data Source Accuracy in section 11.6.

11.2.3 Authenticity of Certificate Request (Reliable Method of Communication)

If the Applicant for a Certificate containing Subject Identity Information is an organization, GeoTrust uses a Reliable Method of Communication to verify the authenticity of the Applicant Representative's certificate request including: email, postal services and telephone.

GeoTrust uses the sources listed in section 11.2.1 to verify the Reliable Method of Communication. Using a Reliable Method of Communication, GeoTrust establishes the authenticity of the certificate request directly with the Applicant Representative or with an authoritative source within the Applicant's organization, such as the Applicant's main business offices, corporate offices, human resource offices, information technology offices, or other department that the CA deems appropriate.

In addition, GeoTrust has a process that allows an Applicant to specify the individuals who may request Certificates. If an Applicant specifies, in writing, the individuals who may request a Certificate, then GeoTrust shall not accept any certificate requests that are outside this specification. Upon the Applicant's verified written request GeoTrust will provide a list of the Applicant's authorized certificate requesters.

11.2.4 Verification of Individual Applicant

If an Applicant is a natural person then GeoTrust verifies the Applicant's name, Applicant's address, and the authenticity of the certificate request (also see 9.2.4 *OrganizationName*)..

GeoTrust verifies the Applicant's name using a legible copy, which discernibly shows the Applicant's face, of at least one currently valid government-issued photo ID (passport, driver's license, military ID, national ID, or equivalent document type). GeoTrust inspects the copy for any indication of alteration or falsification.

GeoTrust verifies the Applicant's address using a form of identification that meets "*Data Source Accuracy*" requirements, such as a government ID, utility bill, or bank or credit card statement. GeoTrust may rely on the same government-issued ID that was used to verify the Applicant's name.

GeoTrust verifies the certificate request with the Applicant using a Reliable Method of Communication.

11.2.5 Verification of Country (Subject Identity comprised of only country Name)

If the Applicant requests a Certificate that will contain Subject Identity Information comprised only of the *countryName* field, then GeoTrust verifies the country associated with the Subject using one of the following:

a) the IP Address range assignment by country for either
   (i) the web site's IP address, as indicated by the DNS record for the web site or
   (ii) the Applicant's IP address;
b) the two-letter country code (ccTLD) of the requested Domain Name;
c) information provided by the Domain Name Registrar; or
d) a method identified in the *"Verification of Subject Identity comprised of Country Name and other Identity Information"* section.

GeoTrust implements a process to screen proxy servers in order to prevent reliance upon IP addresses assigned in countries other than where the Applicant is actually located.

11.3 Age of Certificate Data

GeoTrust shall not use any data or document to validate a certificate request if the data or document was obtained more than thirty-nine (39) months prior to the Certificates' issuance.

11.4 Denied List

GeoTrust maintains an internal database of all previously revoked Certificates and previously rejected certificate requests due to suspected phishing or other fraudulent usage or concerns, for at least seven (7) years in accordance with documentation retention requirements (section 5.5.2 of this CPS).

GeoTrust uses this information to identify subsequent suspicious certificate requests.

11.5 High Risk Status

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

GeoTrust maintains an internal database that includes previously revoked Certificates, including Certificates and previously rejected Certificate Requests, due to suspected phishing or other fraudulent usage. This information is used to flag suspicious new Certificate Requests for future scrutiny before issuance.

GeoTrust uses information identified by GeoTrust's high-risk criteria to flag suspicious certificate requests. GeoTrust follows a documented procedure for performing additional verification of any certificate request flagged as suspicious or high risk. 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 organization.

11.6 Data Source Accuracy

Before relying on a data source to verify Subject Identity Information, GeoTrust evaluates the data source's accuracy and reliability. To verify Subject Identity Information, GeoTrust uses only those data sources that GeoTrust has evaluated to be reasonably accurate or reliable.

12. CERTIFICATE ISSUANCE BY A ROOT CA

GeoTrust's Root CA Private Keys shall not be used to sign Subscriber Certificates. GeoTrust's Root CA Private Keys shall be used to sign Certificates[4] under only the following cases:

[4] Individual exceptions may be approved by GeoTrust for issuance of a Subscriber certificate by a GeoTrust Root CA.

1. Self-signed Certificates to represent the Root CA itself;
2. Certificates for Subordinate CAs and Cross Certificates;
3. Certificates for infrastructure purposes (e.g. administrative role certificates, internal CA operational device certificates, and OCSP Response verification Certificates).

Certificate issuance by the Root CA requires an individual authorized by the CA (i.e. the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation. Additional controls for Certificate issuance by the Root CA are described in section 5.6, Key Changeover and section 6.1, Key Pair Generation.

13. CERTIFICATE REVOCATION AND STATUS CHECKING

13.1 Revocation.

13.1.1 Revocation Request

GeoTrust provides Subscribers with an online form to request revocation of their own certificates as set forth in section 4.9 of this CPS. GeoTrust maintains a continuous 24x7 ability to accept and respond to revocation requests and related inquiries.

13.1.2 Certificate Problem Reporting

GeoTrust provides Subscribers, Relying Parties, Application Software Vendors, and other third parties with an online form to report complaints or suspected Private Key compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates ("Certificate Problem Reports") at: www.geotrust.com/about/contact/extended-validation-support/

13.1.3 Investigation

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

1. The nature of the alleged problem;
2. Number of Certificate Problem Reports received about a particular Certificate or website;
3. 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
4. Relevant legislation in force.

13.1.4 Response

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 Certificate that is the subject of such a complaint.

13.1.5 Reasons for Revocation

In addition to any revocation circumstances listed in section 4.9.1 of this CPS, GeoTrust will revoke an Certificate within 24 hours if one or more of the following events occurs:

1. The Subscriber requests in writing that the CA revoke its Certificate;
2. The Subscriber notifies GeoTrust that the original 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 Certificate) has been compromised, or that the Certificate has otherwise been misused (eg, Private key has been archived);
4. GeoTrust receives notice or otherwise becomes aware that a Subscriber violates any of its material obligations under the Subscriber Agreement;
5. GeoTrust receives notice or otherwise becomes aware that the Fully-Qualified Domain Name or IP address listed in the Certificate is no longer permitted (e.g, a court or arbitrator has revoked a Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or that the Domain Name Registrant has failed to renew its Domain Name);
6. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
7. GeoTrust receives notice or otherwise becomes aware of a material change in the information contained in the Certificate;
8. A determination, in GeoTrust's sole discretion, that the Certificate was not issued in accordance with the terms and conditions of GeoTrust's CPS;
9. If GeoTrust determines that any of the information appearing in the Certificate is inaccurate or misleading.
10. GeoTrust ceases operations for any reason and has not arranged for another CA to provide revocation support for the Certificate;
11. GeoTrust's right to issue Certificates under this CPS expires or is revoked or terminated, unless GeoTrust makes arrangements to continue maintaining the CRL/OCSP Repository;
12. GeoTrust's Private Key for its 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.
14. Revocation is otherwise required by the GeoTrust CPS, or
15. The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. as determined by the CA/Browser Forum).

13.2 Certificate Status Checking

13.2.1 Mechanisms

GeoTrust makes revocation information available as stipulated in Appendix B3, Required Certificate Extensions.

13.2.2 Repository

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

For Subscriber Certificates:

1. 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 beyond the value of the *thisUpdate* field; or
2. OCSP. 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.

For GeoTrust's Subordinate CA Certificate:

1. CRLs. Are updated and reissued at least (i) every twelve (12) months and (ii) within 24 hours after revoking a Subordinate CA Certificate, with the value of the *nextUpdate* field not more than twelve (12) months beyond the value of the *thisUpdate* field; or
2. OCSP. If used, GeoTrust's OCSP for CA Certificates will be updated at least (i) every twelve (12) months, and (ii) within 24 hours after revoking a Subordinate CA Certificate.

GeoTrust operates and maintains 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 Certificates issued by it.

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

Effective 1 January 2013, the CA shall support an OCSP capability using the GET method for Certificates issued in accordance with these Requirements.

13.2.3 Response Time

GeoTrust's CRL and OCSP capability shall provide a response time of ten (10) seconds or less under normal operating conditions.

13.2.4 Deletion of Entries

See section 4.9.7 of this CPS.

13.2.5 OCSP Signing

OCSP Responses shall conform to RFC5019 and either be:

- Signed by the CA that issued the Certificates whose revocation status is being checked, or
- Signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked. Such OCSP Responder signing Certificate shall contain the extension *id-pkix-ocsp-nocheck* as defined by RFC2560.

14 EMPLOYEES AND THIRD PARTIES

14.1 Trustworthiness and Competence

14.1.1 Identity and Background Verification

As specified in section 5.3.2 of this CPS.

14.1.2 Training and Skill Level

GeoTrust provides all personnel performing information verification duties with skills-training that covers basic Public Key Infrastructure knowledge, authentication and vetting policies and procedures (including this CPS), common threats to the information verification process (including phishing and other social engineering tactics), and the pertinent CABF Requirements.

GeoTrust maintains records of such training and ensures that personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily. Validation Specialists engaged in Certificate Issuance shall maintain skill levels consistent with the CA's training and performance programs.

GeoTrust documents that each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task. GeoTrust requires all Validation Specialists to pass an examination provided by the CA on the information verification requirements outlined in the CABF Requirements.

14.2 Delegation of Functions

14.2.1 General

Should GeoTrust delegate the performance of all or part of Section 11 of this Appendix to a Delegated Third Party, GeoTrust shall enforce the requirements as set forth in section 14.2.1 of the CA/Browser Forum Baseline Requirements.

14.2.2 Compliance Obligation

Should GeoTrust delegate the performance of all or part of Section 11 of this Appendix to a Delegated Third Party, GeoTrust shall enforce the requirements as set forth in section 14.2.2 of the CA/Browser Forum Baseline Requirements.

14.2.3 Allocation of Liability

Should GeoTrust delegate the performance of all or part of Section 11 of this Appendix to a Delegated Third Party, GeoTrust shall remain fully responsible as if the tasks had not been delegated as set forth in section 14.2.3 of the CA/Browser Forum Baseline Requirements.

14.2.4 Enterprise RAs

Should GeoTrust delegate the performance of all or part of Section 11 of this Appendix to a Delegated Third Party, GeoTrust shall enforce the requirements as set forth in section 14.2.4 of the CA/Browser Forum Baseline Requirements.

15 DATA RECORDS

15.1 Documentation and Event Logging

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 GeoTrust's practices. This also applies to all delegated third parties, including registration agents (RAs) and subcontractors as well.

15.2 Events and Actions

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

1. CA key lifecycle management events, including:
   a. Key generation, backup, storage, recovery, archival, and destruction; and
   b. Cryptographic device lifecycle management events

2. 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

3. 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

4. Log entries MUST include the following elements:
   a. Date and time of entry;
   b. Identity of the persona and entity making the journal entry; and
   c. Description of entry

15.3 Document Retention

15.3.1 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.

15.3.2 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) year(s) 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. Such information is flagged suspicious EV Certificate Requests.

16. DATA SECURITY

16.1 Objectives

GeoTrust develops, implements, and maintains a comprehensive security program designed to:

1. Protect the confidentiality, integrity, and availability (CIA) of Certificate Data and Certificate Management Processes;
2. Protect against anticipated threats or hazards to the confidentiality, integrity, and availability of the Certificate Data and Certificate Management Processes;
3. Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any Certificate Data or Certificate Management Processes;
4. Protect against accidental loss or destruction of, or damage to, any Certificate Data or Certificate Management Processes; and
5. Comply with all other security requirements applicable to the CA by law.

16.2 Risk Assessment

GeoTrust performs an annual Risk Assessment that:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;
2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

16.3 Security Plan

Based on results of the annual Risk Assessment, GeoTrust develops, implements, and maintains a Security Plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the Certificate Data and Certificate Management Processes.

The Security Plan includes administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the Certificate Data and Certificate Management Processes. The Security Plan takes into account then-available technology and the cost of implementing the specific measures, and implements a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

16.4 Business Continuity

GeoTrust maintains a Disaster Recovery Plan (DRP) to maintain or restore GeoTrust's business operations in a timely manner following the interruption to or failure of critical business processes.

GeoTrust's DRP defines the procedures for the teams to reconstitute GeoTrust CA operations using backup data and backup copies of the GeoTrust keys. The DRP defines emergency procedures, fallback procedures and resumption procedures, the conditions for activating the plan and what constitutes an acceptable system outage and recovery time objective (RTO).

GeoTrust's DRP identifies administrative requirements including:

- maintenance schedule for the plan;
- Awareness and education requirements;
- Responsibilities of the individuals; and
- Regular testing of contingency plans.

Additionally, GeoTrust's DRP includes:

- Requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location,
- Frequency for taking backup copies of essential business information and software,
- Separation distance of the Disaster recovery site to the CA's main site,
- Procedures for securing the Disaster facility during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site,

16.5 System Security

GeoTrust includes system security controls for the Certificate Management Process as follows:

1. Physical security and environmental controls (see section 5.1 of this CPS),
2. System integrity controls including configuration management, integrity maintenance of trusted code and malware detection/prevention (see section 6.6.2 of this CPS),
3. Network security and firewall management, including port restrictions and IP address filtering (see section 6.7 of this CPS),
4. User management, separate trusted-role assignments, education, awareness and training (see section 5.2 of this CPS), and,
5. Logical access controls, activity logging and inactivity time-outs to provide individual accountability (see sections 5.2.3 and 5.4.1 of this CPS).

GeoTrust enforces multi-factor authentication for all accounts capable of directly causing certificate issuance.

16.6 Private Key Protection

GeoTrust's private key protection is described in sections 5.1.2 (Physical Access), 5.2.3 (Identification and Authentication for Each Role), 6.2.9 (Method of Deactivating Private Key) and 6.6.1 (System Development Controls) of this CPS.

17. AUDIT

17.1 Eligible Audit Schemes

GeoTrust performs an annual WebTrust for Certification Authorities v2.0, or later, audit as set forth in section 8 of this CPS.

Such audits will cover all CA obligations under the CA/Browser Forum Guidelines regardless of whether they are performed directly by GeoTrust or delegated to an RA or subcontractor.

17.2 Audit Period

GeoTrust conducts annual compliance audits as set forth in section 8.1 of this CPS.

17.3 Audit Report

GeoTrust makes its annual Audit Report publicly available as set forth in section 8.6 of this CPS.

17.4 Pre-Issuance Readiness Audit

No stipulation.

17.5 Audit of Delegated Functions

No stipulation.

17.6 Auditor Qualifications

GeoTrust engages a qualified auditor as set forth in section 8.2 of this CPS.

17.7 Key Generation Ceremony

GeoTrust conducts key generation ceremonies as set forth in section 6.1.1 of this CPS and additionally in GeoTrust's confidential security policies.

17.8 Regular Quality Assessment Self Audits

GeoTrust and Affiliates shall undergo self-audits to monitor adherence to its Certificate Policy and CPS requirements and strictly control its service quality on at least a quarterly basis against a randomly selected sample of the greater of one Certificate or at least 3% of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

18. LIABILITY AND INDEMNIFICATION

18.1 Liability to Subscribers and Relying Parties

To the extent GeoTrust has issued and managed the Certificate(s) at issue in compliance with CA/Browser Forum requirements and its CPS, GeoTrust shall have no liability to the Subscriber, any Relying Parties or any other third parties for any damages or losses suffered as a result of use or reliance on such Certificate.

In cases where GeoTrust has not issued or managed the Certificate(s) in complete compliance with CA/Browser Forum requirements and its 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 Certificate shall be the greater of (a) the damages recoverable under the Netsure Protection plan or (b) $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 Certificate shall not exceed $2,000.

18.2 Indemnification of Application Software Suppliers

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 the GeoTrust Root CA do not assume any obligation or potential liability of GeoTrust under these Guidelines or that otherwise might exist because of the issuance or maintenance of Certificates or reliance thereon by Relying Parties or others.

GeoTrust shall defend, indemnify, and hold harmless each Application Software Supplier for any and all claims, damages, and losses suffered by such Application Software Supplier related to a 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 Supplier related to a Certificate issued by GeoTrust where such claim, damage, or loss was directly caused by such Application Software Supplier's software displaying as not trustworthy a Certificate that is still valid, or displaying as trustworthy: (1) a Certificate that has expired, or (2) a Certificate that has been revoked (but only in cases where the revocation status is currently available from GeoTrust online, and the browser/application software either failed to check such status or ignored an indication of revoked status).

18.3 Root CA Obligations

The Root CA shall be responsible for the performance and warranties of the Subordinate CA, for the Subordinate CA's compliance with these Requirements, and for all liabilities and indemnification obligations of the Subordinate CA under these Requirements, as if the Root CA were the Subordinate CA issuing the Certificates.

History of Changes

History of changes: version 1.1.13 (effective November 2013)

Section	Section & Changes made
Section 1 Introduction	Identified conformity to CABF Baseline Requirements
6.1.5 Key sizes	Added clarity regarding subscriber certificates under 2048bit will have EKU without server auth flag and designated OID
7.1 Certificate Profile	Added clarity regarding subscriber certificates under 2048bit will have EKU without server auth flag and designated OID
7.1.2.1 Key Usage	Authorization of certificates 2048bit and less in length to be used within closed eco systems
Appendix B1	Updated Extended Validation Guidelines to version 1.4.3
Appendix D	Updated Baseline Requirements to version 1.1.6

History of changes: version 1.1.12 (effective Feb 2013)

Description	Section & Changes made
Addition of new Roots	Section 5.6 – Added G4 PCAs
Addition of Mozilla IDN Verification requirements	Section 3.2.2.2 – Added procedure for verification of IDNs to detect cases of homographic spoofing of IDNs.

History of changes: version 1.1.11 (effective Jan 2013)

Description	Section & Changes made
Re-alignment with CABF EV v1.4 Guidelines	• Updated Appendix B1 all sections to match re-structured CABF Guidelines. • Updated Appendix C (EV CodeSigning) for cross-references to & from Appendix B1. • Created Appendix D (Baseline for OV & DV Certs) for cross-references to & from Appendix B1. • CPS updated throughout with references to Appx B1, C & D as required for CABF procedures.

History of changes: version 1.1.10 (Effective date October 2012)

Section	Description
6.1.5 Key Sizes	Addition of 2048 DSA CA hierarchies

History of changes: Version 1.1.9 (Effective date August 2012)

Section	Description
All updates reflecting compliance with **CABF Requirements for EV Code Signing Certificates**, v1.4.	Appendix C. Section 1.4.1.2, Table 2 – added CS certificates to Class 3 EV Certificates category Section 3.2.2, Table 6 – added additional procedures for EV-CS certificates & H/W protected EV-CS Certificates
Routine maintenance	Section 1, page 1, added footnote clarifying/defining "organizational certificates" Section 1, page 1, added footnote clarifying/defining "organizational certificates" Changed to affirmative language: "GeoTrust confirms" instead of "CA shall confirm" – in sections 3.2.2.1, 4.1.2.2, 4.9.3.2, 4.9.7.1, 4.9.9.1, 6.1.5.1, 6.3.2.1, 6.5.1.1, 7.1.2.2.1,

History of changes: Version 1.1.8 (Effective date June 2012)

Section	Description
Section 1.2	Identified GeoTrust non-EV OIDs
Throughout document	All updates reflecting compliance with CABF Requirements for DV and OV certificates, Effective July 1, 2012. (See PWG Approval Mapping Matrix for GeoTrust CPS)

History of changes: Version 1.1.7 (Effective date April 3, 2012)

Section	Description

Sections 1.3.1 & 1.4.2 - Compliance with the Mozilla Root program	Section 1.3.1 The term Certification Authority (CA) is a trusted third-party entity that issues Certificates and performs all of the functions associated with issuing such Certificates under this CPS. The GeoTrust CA also issues certificates to subordinate CAs, including CAs owned by third parties. All such subordinate CAs are required to operate in conformance with this CPS.. Section 1.4.2 The GeoTrust CA and CAs subordinate to the GeoTrust CA shall not issue any certificate that can be used for man-in-the-middle (MITM) or traffic management of domain names or IPs that the certificate holder does not legitimately own or control. Such certificate usage is expressly prohibited.

History of changes: Version 1.1.6 (Effective date September 28, 2011)

Section	Description
1.4.1, 3.2.3, 3.2.6, 4.9.6, 4.9.9, 4.10.1, 6.1.4, 9.1.5, 9.4.1, 9.12.1	Added FreeSSL Server certificates throughout.
3.2.3	Removed authentication of the ownership of IP address.

History of changes: Version 1.1.5 (Effective date May 5, 2011)

Section	Description
1.4, 3.1.1, 3.2.3, 3.2.5, 4.1.2.1, 4.9.3.2	Added RapidSSL, RapidSSL Wildcard & RapidSSL Enterprise certificates throughout.
3.3 (I&A for Re-Key)	New certificate information provided for renewal certificates are subject to the same I&A as initial certificate requests.
4.5.1 (Subscriber Usage)	Certificate shall not be installed on more than a single server unless agreed at enrolment & fees have been paid.
5.8	Removed description of GeoTrust as "a Delaware corporation".
9.6.3 (Subscriber Representation)	Subscriber shall immediately request revocation if the private key is compromised.
Appx A1, D-6	Clean up of business categories
Appx A2 (EV Key Sizes)	Removed the 2010 deadline for 2048 migration as the migration is now completed.

History of changes: Version 1.1.4 (Effective date September 22, 2010)

Section	Description
9.13 Governing Law	Changed from Virginia to California
9.2.2 Assets	Changed from VeriSign to Symantec.

History of changes: Version 1.1.3 (Effective date March 30, 2010)

Section	Description
6.1.5 Key Sizes	Key pairs shall be of sufficient length to prevent others from determining the key pair's private key using cryptanalysis during the period of expected utilization of such key pairs. The current GeoTrust Standard for minimum key sizes is the use of key pairs equivalent in strength to 1024 bit RSA or higher for its roots and CAs. GeoTrust CAs that have 1024 bit RSA key pairs shall transition to 2048 bit RSA no later than December 31, 2010. GeoTrust Universal Root CAs have 4096 bit RSA. GeoTrust recommends that Registration Authorities and end-user Subscribers generate ~~1024~~2048 bit RSA key pairs. GeoTrust will continue to approve end entity certificates generated with a key pair size of less than 2048 bit RSA but will phase out all 1024-bit RSA by December 31, 2013. Key sizes for GeoTrust EV certificates are identified in Appendix A2 of this CPS. ~~Key sizes for True BusinessID and True Business ID with Extended validation can be found in Appendix A2 of the corresponding CPS.~~
Appendix A2	Updates to key sizes: • All EEC Certificates – 256 & 384 bit
Section 5.1.6	"TL-30 rated safes" changed to "TL-15 rated safes"
Appendix A3	Explicitly added SAN to list of extensions for Subscriber certs. SubjectAltName: If present is populated in accordance with RFC5280 and criticality is set to FALSE

History of changes: Version 1.1.2 (Effective date November 6, 2009)

Section	Description
3.2.3	Changed: "or (c) using a manual process conducted by GeoTrust, to an~~other~~ e-mail address identified as the registered owner of the domain per the *whois* ~~databasecontaining the domain name that is listed as the Common Name in the enrolment form~~. Optionally, a verification phone call may be substituted to the domain owner phone number listed in the *whois*."

History of changes: Version 1.1.1 (Effective date February, 2009)

Section	Description
Appendix A1	Section 8 - Updated maximum validity period from one year to thirteen months
Appendix A1	Section 22(d)(3) - Created section 22(d)(3)
Appendix A1 Section 25	Deleted: "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." Replaced this paragraph with content consistent with published errata to the EV Guidelines. Also included a definition of renewal consistent with the Guidelines.
Appendix A3	Section 3 - Added: "(f) extKeyUsage"
Appendix A1-	A4 and throughout document - Replaced all references to RFC *3280* with RFC 5280

History of changes: Version 1.1 (Effective date April 1, 2008)

Section	Description
Section 5.6	Added: "Root 15 – GeoTrust Primary Certification Authority - G2: Expires January 18, 2038" Added: "GeoTrust Primary Certification Authority – G3: Expires December 1, 2037"
Appendix A1 Section 16 (a)	updated to allow for verification of address of a or a Parent/Subsidiary Company
Appendix A1 Section 5	Added <u>Non-Commercial Entity Subjects</u>
Appendix A1 Section 6(a)3 – table 1	Added: Non-Commercial Entities: V1.0, Clause 5.(3)
Appendix A1 Section 14	Added: Government Entities and Non-Commercial Entities
Appendix A1 Section 19	Added Prior Equivalent Authority
Appendix A4	Updated Appendix A4 in line with published errata to the EV Guidelines
Definitions	Added: "Country": "Sovereign State": "International Organization": "Parent Company" Updated "Subsidiary Company" to be a majority owned and not a wholly owned company.