GeoTrust

Certification Practices Statement

Version 1.1.15

Effective Date: January 15, 2015

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

GeoTrust Certification Practices Statement

Revision date: November 17, 2014

Trademark Notices

Table of Contents

1. INTRODUCTION 1

1.1 OVERVIEW 1
1.2 DOCUMENT NAME AND IDENTIFICATION 1
1.3 PKI PARTICIPANTS 2
1.3.1 Certification Authorities 2
1.3.2 Registration Authorities 2
1.3.3 Subscribers 2
1.3.4 Relying Parties 2
1.3.6 Other Participants 2
1.4 CERTIFICATE USAGE 3
1.4.1 Appropriate Certificate Usages 3
1.4.2 Prohibited Certificate Uses 4
1.5 POLICY ADMINISTRATION 4
1.5.1 Organization Administering the Document 4
1.5.2 Contact Person 4
1.5.3 CPS Approval Procedure 4
1.6 DEFINITIONS AND ACRONYMS 4

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES 5

2.1 REPOSITORIES 5
2.2 PUBLICATION OF CERTIFICATE INFORMATION 5
2.3 TIME OR FREQUENCY OF PUBLICATION 5
2.4 ACCESS CONTROLS ON REPOSITORY 5

3. IDENTIFICATION AND AUTHENTICATION 5

3.1 NAMING 5
3.1.1 Types of Names 5
3.1.2 Need for Names to be Meaningful 6
3.1.3 Anonymity or Pseudonymity of Subscribers 6
3.1.4 Rules for Interpreting Various Name Forms 6
3.1.5 Uniqueness of Names 6
3.1.6 Recognition, Authentication, and Role of Trademarks 6
3.2 INITIAL IDENTITY VALIDATION 7
3.2.1 Method to Prove Possession of Private Key 7
3.2.2 Authentication of Organization Identity 7
3.2.3 Authentication of Domain Name 8
3.2.4 Authentication of individual identity 9
3.2.5 Non-Verified Subscriber Information 9
3.2.6 Validation of Authority 9
3.2.7 Criteria for Interoperation 10
3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS 10
3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST 10

4. CERTIFICATE LIFE-CYCLE OPERATIONS 10

4.1 CERTIFICATE APPLICATION 10
4.1.1 Who Can Submit A Certificate Application? 10
4.1.2 Enrollment Process and Responsibilities 11
4.2 CERTIFICATE APPLICATION PROCESSING 11
4.2.1 Performing Identification and Authentication Functions 11
4.2.2 Approval or Rejection of Certificate Applications 11
4.2.3 Time to Process Certificate Applications 12
4.3 CERTIFICATE ISSUANCE 12
4.3.1 CA Actions during Certificate Issuance 12
4.3.2 Notifications to Subscriber by the CA of Issuance of Certificates 12
4.3.3 CABF Requirement for Certificate Issuance by a Root CA 12
4.4 CERTIFICATE ACCEPTANCE ..... 13~~12~~
4.4.1 Conduct Constituting Certificate Acceptance ..... 13~~12~~
4.4.2 Publication of the Certificate by the CA 13
4.4.3 Notification of Certificate Issuance by the CA to Other Entities 13
4.5 KEY PAIR AND CERTIFICATE USAGE 13
4.5.1 Subscriber Private Key and Usage 13
4.5.2 Relying Party Public Key and Certificate Usage 13
4.6 CERTIFICATE RENEWAL 14
4.6.1 Circumstances for Certificate Renewal 14
4.6.2 Who May Request Renewal 14
4.6.3 Processing Certificate Renewal Requests 14
4.6.4 Notification of New Certificate Issuance to Subscriber 14
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate 14
4.6.6 Publication of the Renewal Certificate by the CA 14
4.6.7 Notification of Certificate Issuance by the CA to Other Entities 14
4.7 CERTIFICATE RE-KEY ..... 15~~14~~
4.7.1 Circumstances for Re-Key ..... 15~~14~~
4.7.2 Who May Request Certification of a New Public Key 15
4.7.3 Processing Certificate Re-Keying Requests 15
4.7.4 Notification of New Certificate Issuance to Subscriber 15
4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate 15
4.7.6 Publication of the Re-Keyed Certificate by the CA 15
4.7.7 Notification of Certificate Issuance by the CA to Other Entities 15
4.8 CERTIFICATE MODIFICATION 15
4.8.1 Circumstances for Certificate Modification 15
4.8.2 Who May Request Certificate Modification 15
4.8.3 Processing Certificate Modification Requests 15
4.8.4 Notification of New Certificate Issuance to Subscriber ..... 16~~15~~
4.8.5 Conduct Constituting Acceptance of Modified Certificate ..... 16~~15~~
4.8.6 Publication of the Modified Certificate by the CA 16
4.8.7 Notification of Certificate Issuance by the CA to Other Entities 16
4.9 CERTIFICATE REVOCATION AND SUSPENSION 16
4.9.1 Circumstances for Revocation 16
4.9.2 Who Can Request Revocation 17
4.9.3 Procedure for Revocation Request 17
4.9.4 Revocation Request Grace Period 17
4.9.5 Time within Which CA Must Process the Revocation Request 17
4.9.6 Revocation Checking Requirements for Relying Parties 17
4.9.7 CRL Issuance Frequency ..... 18~~17~~
4.9.8 Maximum Latency for CRLs 18

4.9.9 On-Line Revocation/Status Checking Availability 18
4.9.10 On-Line Revocation Checking Requirements 18
4.9.11 Other Forms of Revocation Advertisements Available 18
4.9.12 Special Requirements Regarding Key Compromise ... 18
4.9.13 Circumstances for Suspension 18
4.9.14 Who can Request Suspension ..... 19~~18~~
4.9.15 Procedure for Suspension Request ..... 19~~18~~
4.9.16 Limits of Suspension Period 19
4.10 CERTIFICATE STATUS SERVICES 19
4.10.1 Operational Characteristics 19
4.10.2 Service Availability 19
4.10.3 Optional Features 19
4.11 END OF SUBSCRIPTION 19
4.12 KEY ESCROW AND RECOVERY 19
4.12.1 Key Escrow and Recovery Policy and Practices 19
4.12.2 Session Key Encapsulation and Recovery Policy and Practices 20

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 20

5.1 PHYSICAL CONTROLS 20
5.1.1 Site Location and Construction 20
5.1.2 Physical Access 20
5.1.3 Power and Air Conditioning 20
5.1.4 Water Exposures ..... 21~~20~~
5.1.5 Fire Prevention and Protection ..... 21~~20~~
5.1.6 Media Storage 21
5.1.7 Waste Disposal 21
5.1.8 Off-Site Backup 21
5.2 PROCEDURAL CONTROLS 21
5.2.1 Trusted Roles 21
5.2.2 Number of Persons Required per Task ..... 22~~21~~
5.2.3 Identification and Authentication for Each Role 22
5.2.4 Roles Requiring Separation of Duties 22
5.3 PERSONNEL CONTROLS 22
5.3.1 Qualifications, Experience, and Clearance Requirements 22
5.3.2 Background Check Procedures ..... 23~~22~~
5.3.3 Training Requirements 23
5.3.4 Retraining Frequency and Requirements 23
5.3.5 Job Rotation Frequency and Sequence 23
5.3.6 Sanctions for Unauthorized Actions ..... 24~~23~~
5.3.7 Independent Contractor Requirements ..... 24~~23~~
5.3.8 Documentation Supplied to Personnel 24
5.4 AUDIT LOGGING PROCEDURES 24
5.4.1 Types of Events Recorded 24
5.4.2 Frequency of Processing Log 24
5.4.3 Retention Period for Audit Log 24
5.4.4 Protection of Audit Log 24
5.4.5 Audit Log Backup Procedures 24
5.4.6 Audit Collection System (Internal vs. External) ..... 25~~24~~
5.4.7 Notification to Event-Causing Subject ..... 25~~24~~
5.4.8 Vulnerability Assessments 25
5.4.9 Archive Collection System (Internal or External) 25
5.4.10 Procedures to Obtain and Verify Archive Information 25
5.5 RECORDS ARCHIVAL 25
5.5.1 Types of Records Archived 25
5.5.2 Retention Period for Archive 25
5.5.3 Protection of Archive 25
5.5.4 Archive Backup Procedures 25
5.5.5 Requirements for Time-Stamping of Records ..... 26~~25~~
5.5.6 Archive Collection System (Internal or External) ..... 26~~25~~
5.5.7 Procedures to Obtain and Verify Archive Information 26
5.6 KEY CHANGEOVER 26
5.7 COMPROMISE AND DISASTER RECOVERY 27
5.7.1 Incident and Compromise Handling Procedures 27
5.7.2 Computing Resources, Software, and/or Data are Corrupted 27
5.7.3 Entity Private Key Compromise Procedures 27
5.7.4 Business Continuity Capabilities after a Disaster 27
5.8 CA OR RA TERMINATION 28
5.9 DATA SECURITY 28

6 TECHNICAL SECURITY CONTROLS ..... 29~~28~~

6.1 KEY PAIR GENERATION AND INSTALLATION ..... 29~~28~~
6.1.1 Key Pair Generation ..... 29~~28~~
6.1.2 Private Key Delivery to Subscriber 29
6.1.3 Public Key Delivery to Certificate Issuer 29
6.1.4 CA Public Key Delivery to Relying Parties 29
6.1.5 Key Sizes 29
6.1.6 Public Key Parameters Generation and Quality Checking 31
6.1.7 Key Usage Purposes (as per x.509 v3 Key Usage Field) 31
6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS 31
6.2.1 Cryptographic Module Standards and Controls 31
6.2.2 Private Key (m of n) Multi-Person Control 31
6.2.3 Private Key Escrow ..... 32~~31~~
6.2.4 Private Key Backup ..... 32~~31~~
6.2.5 Private Key Archival ..... 32~~31~~
6.2.6 Private Key Transfer Into or From Cryptographic Module 32
6.2.7 Private Key Storage on Cryptographic Module 32
6.2.8 Method of Activating Private Key 32
6.2.9 Method of Deactivating Private Key 32
6.2.10 Method of Destroying Private Key 32
6.2.11 Cryptographic Module Rating 32
6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT ..... 33~~32~~
6.3.1 Public Key Archival ..... 33~~32~~
6.3.2 Certificate Operational Periods and Key Pair Usage Periods ..... 33~~32~~
6.4 ACTIVATION DATA 33
6.4.1 Activation Data Generation and Installation 33
6.4.2 Activation Data Protection 33
6.4.3 Other Aspects of Activation Data ..... 34~~33~~
6.5 COMPUTER SECURITY CONTROLS 34
6.5.1 Specific Computer Security Technical Requirements ... 34
6.5.2 Computer Security Rating 34
6.6 LIFE CYCLE TECHNICAL CONTROLS 34
6.6.1 System Development Controls 34
6.6.2 Security Management Controls 34
6.6.3 Life Cycle Security Controls 34
6.7 NETWORK SECURITY CONTROLS ..... 35~~34~~

6.8 TIME STAMPING 3534

7. CERTIFICATE, CRL, AND OCSP PROFILES 3534

7.1 CERTIFICATE PROFILE 3534
7.1.1 Version Number(s) 35
7.1.3 Algorithm Object Identifiers 36
7.1.6 Certificate Policy Object Identifier 3736
7.1.7 Usage of Policy Constraints Extension 3736
7.1.8 Policy Qualifiers Syntax and Semantics 3736
7.1.9 Processing Semantics for the Critical Certificate Policies Extension 37
7.2 CRL PROFILE 37
7.2.1 Version Number(s) 37
7.2.2 CRL and CRL Entry Extensions 37
7.3 OCSP PROFILE 37
7.3.1 Version Number(s) 3837
7.3.2 OCSP Extensions 3837

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS 3837

8.1 FREQUENCY AND CIRCUMSTANCES OF ASSESSMENT 3837
8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR 38
8.3 ASSESSORS RELATIONSHIP TO ASSESSED ENTITY 38
8.4 TOPICS COVERED BY ASSESSMENT 38
8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY 3938
8.6 COMMUNICATIONS OF RESULTS 3938

9. OTHER BUSINESS AND LEGAL MATTERS 39

9.1 FEES 39
9.1.1 Certificate Issuance or Renewal Fees 39
9.1.2 Certificate Access Fees 39
9.1.3 Revocation or Status Information Access Fees 39
9.1.4 Fees for Other Services 39
9.1.5 Refund Policy 4039
9.2 FINANCIAL RESPONSIBILITY 4039
9.2.1 Insurance Coverage 4039
9.2.2 Other Assets 40
9.2.3 Extended Warranty Coverage 40
9.3 CONFIDENTIALITY OF BUSINESS INFORMATION 40
9.3.1 Scope of Confidential Information 40
9.3.2 Information Not Within the Scope of Confidential Information 4140
9.3.3 Responsibility to Protect Confidential Information . 4140
9.4 PRIVACY OF PERSONAL INFORMATION 4140
9.4.1 Privacy Plan 4140
9.4.2 Information Treated as Private 41
9.4.3 Information Not Deemed Private 41
9.4.4 Responsibility to Protect Private Information 41
9.4.5 Notice and Consent to Use Private Information 41
9.4.6 Disclosure Pursuant to Judicial or Administrative Process 41
9.4.7 Other Information Disclosure Circumstances 4241
9.5 INTELLECTUAL PROPERTY RIGHTS 4241
9.5.1 Property Rights in Certificates and Revocation Information 4241
9.5.2 Property Rights in the CPS 42
9.5.3 Property Rights in Names 42
9.5.4 Property Rights in Keys and Key Material 42
9.6 REPRESENTATIONS AND WARRANTIES 42
9.6.1 CA Representations and Warranties 42
9.6.2 RA Representations and Warranties 4342
9.6.3 Subscriber Representations and Warranties 43
9.6.4 Relying Party Representations and Warranties 43
9.6.5 Representations and Warranties of Other Participants 4443
9.7 DISCLAIMER OF WARRANTIES 4443
9.8 LIMITATION OF LIABILITY 4443
9.9 INDEMNITIES 44
9.9.1 Indemnification by Subscribers 44
9.9.2 Indemnification by Relying Parties 44
9.9.3 Indemnification of Application Software Suppliers .. 4544
9.10 TERM AND TERMINATION 45
9.10.1 Term 45
9.10.2 Termination 45
9.10.3 Effect of Termination and Survival 45
9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS 45
9.12 AMENDMENTS 45
9.12.1 Procedure for Amendment 45
9.12.2 Notification Mechanism and Period 4645
9.12.3 Circumstances under Which OID must be Changed 4645
9.13 DISPUTE RESOLUTION PROVISIONS 46
9.13.1 Disputes among GeoTrust, Affiliates and Customers . 46
9.13.2 Disputes with End-User Subscribers or Relying Parties 46
9.14 GOVERNING LAW 46
9.15 COMPLIANCE WITH APPLICABLE LAW 4746
9.16 MISCELLANEOUS PROVISIONS 4746
9.16.1 Entire Agreement 4746
9.16.2 Assignment 4746
9.16.3 Severability 47
9.16.4 Enforcement (Attorney's Fees and Waiver of Rights) . 47
9.16.5 Force Majeure 47
9.17 OTHER PROVISIONS 47

APPENDICES 48

APPENDIX A: TABLE OF ACRONYMS AND DEFINITIONS 48
APPENDIX B1: SUPPLEMENTAL VALIDATION PROCEDURES FOR EXTENDED VALIDATION (EV) SSL CERTIFICATES 56
APPENDIX B2: MINIMUM CRYPTOGRAPHIC ALGORITHM AND KEY SIZES FOR EV CERTIFICATES 56
APPENDIX B3: EV CERTIFICATES REQUIRED CERTIFICATE EXTENSIONS 57
APPENDIX B4: FOREIGN ORGANIZATION NAME GUIDELINES 59
APPENDIX C: SUPPLEMENTAL VALIDATION PROCEDURES FOR EXTENDED VALIDATION (EV) CODE-SIGNING CERTIFICATES 61
APPENDIX D: SUPPLEMENTAL BASELINE REQUIREMENTS FOR ISSUANCE AND MANAGEMENT OF PUBLICLY-TRUSTED CERTIFICATES 62
APPENDIX E: HISTORY OF CHANGES 63

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.
Note that the use of Certificates with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Name has been deprecated by the CA / Browser Forum and will be eliminated by October 2016. Any such certificate issued prior to October 2016 must have an expiry date of 1 November 2015 or earlier. Previously issued certificates with expiry dates after 1 November 2015 will be revoked effective 1 October 2016.

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) * The use of Certificates with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Name has been deprecated by the CA / Browser Forum and will be eliminated by October 2016. Any such certificate issued prior to October 2016 must have an expiry date of 1 November 2015 or earlier. Previously issued certificates with expiry dates after 1 November 2015 will be revoked effective 1 October 2016.
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, 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, 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.
Note that the use of Certificates with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Name has been deprecated by the CA / Browser Forum and will be eliminated by October 2016. Any such certificate issued prior to October 2016 must have an expiry date of 1 November 2015 or earlier. Previously issued certificates with expiry dates after 1 November 2015 will be revoked effective 1 October 2016.

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.

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

3.2.7 Criteria for Interoperation

No Stipulation

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, 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.

4.2.4 Certificate Authority Authorization

As of October 1, 2015, GeoTrust will check Certificate Authority Authorization (CAA) records as part of its public SSL certificate authentication and verification processes. Prior to this date GeoTrust may not check CAA records for all public SSL certificate orders. 'Public SSL Certificates' are those that chain up to our publicly available root certificates and which meet CA/Browser Forum Baseline or Extended Validation Requirements.

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, 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, 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, Appendix B1, Appendix C and 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, Appendix B1, Appendix C, and 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, Appendix B1, Appendix C, and 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, Appendix B1, Appendix C and 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, 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 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 Appendix B1, Appendix C and 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, 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, 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	2048	2048

(bits)		
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, 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, 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, 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, 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, Appendix B1, Appendix C, 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, Appendix B1, Appendix C, and 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 Statement, 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 Statement 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, Appendix B1, Appendix C, and 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 the 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

The current version of the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation (EV) SSL Certificates can be accessed at https://cabforum.org/extended validation/
o submit, the EV Certificate

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

The current version of the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation (EV) Code Signing Certificates can be accessed at https://cabforum.org/ev-code-signing-certificate-guidelines/

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

The current version of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates can be accessed at https://cabforum.org/baseline-requirements-documents/

Appendix E:
History of Changes

History of changes: version 1.1.15 (effective Jan 2015)

Description	Section & Changes made
Added language to specifically include Certificate Authority Authorization (CA)	4.2.4 Certificate Authority Authorization (CAA) As of October 1, 2015, GeoTrust will check Certificate Authority Authorization (CAA) records as part of its public SSL certificate authentication and verification processes. Prior to this date GeoTrust may not check CAA records for all public SSL certificate orders. 'Public SSL Certificates' are those that chain up to our publicly available root certificates and which meet CA/Browser Forum Baseline or Extended Validation Requirements.

History of changes: version 1.1.14 (effective November 2014)

Section	Section & Changes made
1.4.1 Appropriate Certificate Use	Added reference that the use of Certificates with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Name has been deprecated by the CA / Browser Forum including dates.
3.1.1 Types of Names, Table 1	Added footnote that the use of Certificates with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Name has been deprecated by the CA / Browser Forum including dates.
3.2.3 Authentication of Domain Name	Added reference that the use of Certificates with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Name has been deprecated by the CA / Browser Forum including dates.
9.4.1 Privacy Plan	Replaced 'privacy policy' with 'Privacy Statement'
9.4.5 Notice and Consent to Use Private Information	Replaced 'privacy policy' with 'Privacy Statement'
Appendix B1	Appendix B1 Replaced text with reference to URL on external website "The current version of the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation (EV) Certificates can be accessed at https://cabforum.org/extended-validation/"
Appendix C	Appendix C Replaced text with reference to URL on external website "The current version of the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation (EV) Code Signing Certificates can be accessed at https://cabforum.org/ev-code-signing-certificate-guidelines/"
Appendix D	Appendix D Replaced text with reference to URL on external website "The current version of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates can be accessed at https://cabforum.org/baseline-requirements-documents/"

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

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 Non-Commercial Entity Subjects
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.