

# **GeoTrust Certification Practice Statement**

**Version 1.0**

**Effective Date: January 31, 2008**



**GeoTrust, Inc  
487 E. Middlefield Rd.  
Mountain View, CA 94043 USA  
+1 650.961.7500  
[www.geotrust.com](http://www.geotrust.com)**

**Trademark Notices**

GeoTrust is a registered mark of GeoTrust Inc. The GeoTrust logo, True Credentials, QuickSSL, True Business ID, and Power ServerID, are trademarks and service marks of GeoTrust. Other trademarks and service marks in this document are the property of their respective owners. GeoTrust Inc. is a wholly owned subsidiary of VeriSign, Inc.

Without limiting the rights reserved above, and except as licensed below, no part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without prior written permission of GeoTrust.

Notwithstanding the above, permission is granted to reproduce and distribute this GeoTrust Certification Practice Statement on a nonexclusive, royalty-free basis, provided that (i) the foregoing copyright notice and the beginning paragraphs are prominently displayed at the beginning of each copy, and (ii) this document is accurately reproduced in full, complete with attribution of the document to GeoTrust.

Requests for any other permission to reproduce these VeriSign Certificate Policies (as well as requests for copies from VeriSign) must be addressed to VeriSign, Inc., 487 E. Middlefield Road, Mountain View, CA 94043 USA Attn: Practices Development. Tel: +1 650.961.7500 Fax: +1 650.426.7300 Net: **practices@verisign.com**.

## Table of Contents

<b>1. INTRODUCTION</b> .....	8
<b>1.1 Overview</b> .....	9
<b>1.2 Document Name and Identification</b> .....	9
<b>1.3 PKI Participants</b> .....	9
1.3.1 Certification Authorities .....	9
1.3.2 Registration Authorities .....	9
1.3.3 Subscribers .....	9
1.3.4 Relying Parties .....	9
1.3.5 Other Participants .....	10
<b>1.4 Certificate Usage</b> .....	10
1.4.1 Appropriate Certificate Usages .....	10
1.4.2 Prohibited Certificate Uses .....	10
<b>1.5 Policy Administration</b> .....	10
1.5.1 Organization Administering the Document .....	10
1.5.2 Contact Person .....	11
1.5.3 CPS Approval Procedure .....	11
<b>1.6 Definitions and Acronyms</b> .....	11
<b>2. Publication and Repository Responsibilities</b> .....	11
<b>2.1 Repositories</b> .....	11
<b>Repositories</b> .....	11
<b>2.2 Publication of Certificate Information</b> .....	11
<b>2.3 Time or Frequency of Publication</b> .....	11
<b>2.4 Access Controls on Repository</b> .....	11
<b>3. Identification and Authentication</b> .....	12
<b>3.1 Naming</b> .....	12
3.1.2 Need for Names to be Meaningful .....	12
3.1.3 Anonymity or pseudonymity of Subscribers .....	12
3.1.4 Rules for Interpreting Various Name Forms .....	12
3.1.5 Uniqueness of Names .....	13
3.1.6 Recognition, Authentication, and Role of Trademarks .....	13
<b>3.2 Initial Identity Validation</b> .....	13
3.2.1 Method to Prove Possession of Private Key .....	13
3.2.2 Authentication of Organization Identity .....	13
3.2.3 Authentication of Individual Identity .....	13
3.2.4 Non-Verified Subscriber Information .....	14
3.2.5 Validation of Authority .....	14
3.2.6 Criteria for Interoperation .....	15
<b>3.3 Identification and Authentication for Re-key Requests</b> .....	15
<b>3.4 Identification and Authentication for Revocation Request</b> .....	15
<b>4. Certificate Life-Cycle Operations</b> .....	15
<b>4.1 Certificate Application</b> .....	15
4.1.1 Who Can Submit A Certificate Application? .....	15
4.1.2 Enrollment Process and Responsibilities .....	16
4.1.2.1 End-User Certificate Subscribers .....	16
4.1.2.2 CA and RA Certificates .....	16
<b>4.2 Certificate Application Processing</b> .....	16
4.2.1 Performing Identification and Authentication Functions .....	16
4.2.2 Approval or Rejection of Certificate Applications .....	16
4.2.3 Time to Process Certificate Applications .....	16

<b>4.3 Certificate Issuance</b> .....	17
4.3.1 CA Actions during Certificate Issuance .....	17
4.3.2 Notifications to Subscriber by the CA of Issuance of Certificates .....	17
<b>4.4 Certificate Acceptance</b> .....	17
4.4.1 Conduct Constituting Certificate Acceptance .....	17
4.4.2 Publication of the Certificate by the CA .....	17
4.4.3 Notification of Certificate Issuance by the CA to Other Entities .....	17
<b>4.5 Key Pair and Certificate Usage</b> .....	17
4.5.1 Subscriber Private Key and Usage .....	17
4.5.2 Relying Party Public Key and Certificate Usage .....	18
<b>4.6 Certificate Renewal</b> .....	18
4.6.1 Circumstances for Certificate Renewal .....	18
4.6.2 Who May Request Renewal .....	18
4.6.3 Processing Certificate Renewal Requests .....	18
4.6.4 Notification of New Certificate Issuance to Subscriber .....	18
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate .....	19
4.6.6 Publication of the Renewal Certificate by the CA .....	19
4.6.7 Notification of Certificate Issuance by the CA to Other Entities .....	19
<b>4.7 Certificate Re-Key</b> .....	19
4.7.1 Circumstances for Re-Key .....	19
4.7.2 Who May Request Certification of a New Public Key .....	19
4.7.3 Processing Certificate Re-Keying Requests .....	19
4.7.4 Notification of New Certificate Issuance to Subscriber .....	19
4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate .....	19
4.7.6 Publication of the Re-Keyed Certificate by the CA .....	19
4.7.7 Notification of Certificate Issuance by the CA to Other Entities .....	19
<b>4.8 Certificate Modification</b> .....	19
4.8.1 Circumstances for Certificate Modification .....	19
4.8.2 Who May Request Certificate Modification .....	19
4.8.3 Processing Certificate Modification Requests .....	20
4.8.4 Notification of New Certificate Issuance to Subscriber .....	20
4.8.5 Conduct Constituting Acceptance of Modified Certificate .....	20
4.8.6 Publication of the Modified Certificate by the CA .....	20
4.8.7 Notification of Certificate Issuance by the CA to Other Entities .....	20
<b>4.9 Certificate Revocation and Suspension</b> .....	20
4.9.1 Circumstances for Revocation .....	20
4.9.2 Who Can Request Revocation .....	21
4.9.3 Procedure for Revocation Request .....	21
4.9.3.1 Procedure for Requesting the Revocation of an End-User Subscriber Certificate .....	21
4.9.3.2 Procedure for Requesting the Revocation of a CA or RA Certificate .....	21
4.9.4 Revocation Request Grace Period .....	21
4.9.5 Time within Which CA Must Process the Revocation Request .....	21
4.9.6 Revocation Checking Requirements for Relying Parties .....	21
4.9.7 CRL Issuance Frequency .....	21
4.9.8 Maximum Latency for CRLs .....	21
4.9.9 On-Line Revocation/Status Checking Availability .....	21
4.9.10 On-Line Revocation Checking Requirements .....	21
4.9.11 Other Forms of Revocation Advertisements Available .....	21
4.9.12 Special Requirements regarding Key Compromise .....	22
4.9.13 Circumstances for Suspension .....	22
4.9.14 Who can request Suspension .....	22
4.9.15 Procedure for Suspension Request .....	22
4.9.16 Limits of Suspension Period .....	22

<b>4.10 Certificate Status Services</b> .....	22
4.10.1 Operational Characteristics .....	22
4.10.2 Service Availability .....	22
4.10.3 Optional Features .....	22
<b>4.11 End of Subscription</b> .....	22
<b>4.12 Key Escrow and Recovery</b> .....	22
4.12.1 Key Escrow and Recovery Policy and Practices .....	22
4.12.2 Session Key Encapsulation and Recovery Policy and Practices .....	23
<b>5 Facility, Management, and Operational Controls</b> .....	23
<b>5.1 Physical Controls</b> .....	23
5.1.1 Site Location and Construction .....	23
5.1.2 Physical Access .....	23
5.1.3 Power and Air Conditioning .....	23
5.1.4 Water Exposures .....	24
5.1.5 Fire Prevention and Protection .....	24
5.1.6 Media Storage .....	24
5.1.7 Waste Disposal .....	24
5.1.8 Off-Site Backup .....	24
<b>5.2 Procedural Controls</b> .....	24
5.2.1 Trusted Roles .....	24
5.2.2 Number of Persons Required per Task .....	25
5.2.3 Identification and Authentication for Each Role .....	25
5.2.4 Roles Requiring Separation of Duties .....	25
<b>5.3 Personnel Controls</b> .....	25
5.3.1 Qualifications, Experience, and Clearance Requirements .....	25
5.3.2 Background Check Procedures .....	25
5.3.3 Training Requirements .....	26
5.3.4 Retraining Frequency and Requirements .....	26
5.3.5 Job Rotation Frequency and Sequence .....	26
5.3.6 Sanctions for Unauthorized Actions .....	26
5.3.7 Independent Contractor Requirements .....	27
5.3.8 Documentation Supplied to Personnel .....	27
<b>5.4 Audit Logging Procedures</b> .....	27
5.4.1 Types of Events Recorded .....	27
5.4.2 Frequency of Processing Log .....	27
5.4.3 Retention Period for Audit Log .....	27
5.4.4 Protection of Audit Log .....	27
5.4.5 Audit Log Backup Procedures .....	27
5.4.6 Audit Collection System (Internal vs. External) .....	27
5.4.7 Notification to Event-Causing Subject .....	27
5.4.8 Vulnerability Assessments .....	27
5.4.9 Archive Collection System (Internal or External) .....	28
5.4.10 Procedures to Obtain and Verify Archive Information .....	28
<b>5.5 Records Archival</b> .....	28
5.5.1 Types of Records Archived .....	28
5.5.2 Retention Period for Archive .....	28
5.5.3 Protection of Archive .....	28
5.5.4 Archive Backup Procedures .....	28
5.5.5 Requirements for Time-Stamping of Records .....	28
5.5.6 Archive Collection System (Internal or External) .....	28
5.5.7 Procedures to Obtain and Verify Archive Information .....	28
<b>5.5.8 Key Changeover</b> .....	28
<b>5.7 Compromise and Disaster Recovery</b> .....	29
5.7.1 Incident and Compromise Handling Procedures .....	29

5.7.2 Computing Resources, Software, and/or Data are Corrupted .....	29
5.7.3 Entity Private Key Compromise Procedures .....	29
5.7.4 Business Continuity Capabilities After a Disaster .....	30
<b>5.8 CA or RA Termination .....</b>	<b>30</b>
<b>6 Technical Security Controls .....</b>	<b>30</b>
<b>6.1 Key Pair Generation and Installation .....</b>	<b>30</b>
6.1.1 Key Pair Generation .....	30
6.1.2 Private Key Delivery to Subscriber .....	31
6.1.3 Public Key Delivery to Certificate Issuer .....	31
6.1.4 CA Public Key Delivery to Relying Parties .....	31
6.1.5 Key Sizes .....	31
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
<b>6.2 Private Key Protection and Cryptographic Module Engineering Controls .....</b>	<b>31</b>
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
6.2.4 Private Key Backup .....	32
6.2.5 Private Key Archival .....	32
6.2.6 Private Key Transfer Into of 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
<b>6.3 Other Aspects of Key Pair Management .....</b>	<b>33</b>
6.3.1 Public Key Archival .....	33
6.3.2 Certificate Operational Periods and Key Pair Usage Periods .....	33
<b>6.4 Activation Data .....</b>	<b>33</b>
6.4.1 Activation Data Generation and Installation .....	33
6.4.2 Activation Data Protection .....	33
6.4.3 Other Aspects of Activation Data .....	33
6.4.3.1 Activation Data Transmission .....	33
6.4.3.2 Activation Data Destruction .....	33
<b>6.5 Computer Security Controls .....</b>	<b>34</b>
6.5.1 Specific Computer Security Technical Requirements .....	34
6.5.2 Computer Security Rating .....	34
<b>6.6 Life Cycle Technical Controls .....</b>	<b>34</b>
6.6.1 System Development Controls .....	34
6.6.2 Security Management Controls .....	34
6.6.3 Life Cycle Security Controls .....	34
<b>6.7 Network Security Controls .....</b>	<b>34</b>
<b>6.8 Time Stamping .....</b>	<b>34</b>
<b>7. Certificate, CRL, and OCSP Profiles .....</b>	<b>34</b>
<b>7.1 Certificate Profile .....</b>	<b>34</b>
7.1.1 Version Number(s) .....	35
7.1.2.1 Key Usage .....	35
7.1.2.2 Certificate Policies Extension .....	35
7.1.2.3 Subject Alternative Names .....	35
7.1.2.4 Basic Constraints .....	35
7.1.2.5 Extended Key Usage .....	35

7.1.2.6 CRL Distribution Points .....	35
7.1.2.7 Authority Key Identifier .....	35
7.1.2.8 Subject Key Identifier .....	35
7.1.3 Algorithm Object Identifiers .....	35
7.1.4 Name Forms .....	35
7.1.5 Name Constraints .....	35
7.1.6 Certificate Policy Object Identifier .....	36
7.1.7 Usage of Policy Constraints Extension .....	36
7.1.8 Policy Qualifiers Syntax and Semantics .....	36
7.1.9 Processing Semantics for the Critical Certificate Policies Extension .....	36
<b>7.2 CRL Profile</b> .....	<b>36</b>
7.2.1 Version Number(s) .....	36
7.2.2 CRL and CRL Entry Extensions .....	36
<b>7.3 OCSP Profile</b> .....	<b>36</b>
7.3.1 Version Number(s) .....	36
7.3.2 OCSP Extensions .....	36
<b>8. Compliance Audit and Other Assessments</b> .....	<b>36</b>
<b>8.1 Frequency and Circumstances of Assessment</b> .....	<b>36</b>
<b>8.2 Identity/Qualifications of Assessor</b> .....	<b>36</b>
<b>8.3 Assessors Relationship to Assessed Entity</b> .....	<b>37</b>
<b>8.4 Topics Covered by Assessment</b> .....	<b>37</b>
<b>8.5 Actions Taken as a Result of Deficiency</b> .....	<b>37</b>
<b>8.6 Communications of Results</b> .....	<b>37</b>
<b>9. Other Business and Legal Matters</b> .....	<b>37</b>
<b>9.1 Fees</b> .....	<b>37</b>
9.1.1 Certificate Issuance or Renewal Fees .....	37
9.1.2 Certificate Access Fees .....	37
9.1.3 Revocation or Status Information Access Fees .....	37
9.1.4 Fees for Other Services .....	38
9.1.5 Refund Policy .....	38
<b>9.2 Financial Responsibility</b> .....	<b>38</b>
9.2.1 Insurance Coverage .....	38
9.2.2 Other Assets .....	38
9.2.3 Warranty Coverage .....	38
<b>9.3 Confidentiality of Business Information</b> .....	<b>38</b>
9.3.1 Scope of Confidential Information .....	38
9.3.2 Information Not Within the Scope of Confidential Information .....	39
9.3.3 Responsibility to Protect Confidential Information .....	39
<b>9.4 Privacy of Personal Information</b> .....	<b>39</b>
<b>9.4.1 Privacy Plan</b> .....	<b>39</b>
9.4.2 Information Treated as Private .....	39
9.4.3 Information Not Deemed Private .....	39
9.4.4 Responsibility to Protect Private Information .....	39
9.4.5 Notice and Consent to Use Private Information .....	39
9.4.6 Disclosure Pursuant to Judicial or Administrative Process .....	39
9.4.7 Other Information Disclosure Circumstances .....	40
<b>9.5 Intellectual Property Rights</b> .....	<b>40</b>
9.5.1 Property Rights in Certificates and Revocation Information .....	40
9.5.2 Property Rights in the CPS .....	40
9.5.3 Property Rights in Names .....	40
9.5.4 Property Rights in Keys and Key Material .....	40
<b>9.6 Representations and Warranties</b> .....	<b>40</b>

9.6.1 CA Representations and Warranties .....	40
9.6.2 RA Representations and Warranties .....	40
9.6.3 Subscriber Representations and Warranties.....	41
9.6.4 Relying Party Representations and Warranties .....	41
9.6.5 Representations and Warranties of Other Participants.....	41
<b>9.7 Disclaimer of Warranties .....</b>	<b>41</b>
<b>9.8 Limitation of Liability .....</b>	<b>41</b>
<b>9.9 Indemnities .....</b>	<b>42</b>
9.9.1 Indemnification by Relying Parties.....	42
<b>9.10 Term and Termination.....</b>	<b>42</b>
9.10.1 Term .....	42
9.10.2 Termination .....	42
9.10.3 Effect of Termination and Survival .....	42
<b>9.11 Individual Notices and Communications with Participants.....</b>	<b>42</b>
<b>9.12 Amendments.....</b>	<b>43</b>
9.12.1 Procedure for Amendment .....	43
9.12.2 Notification Mechanism and Period.....	43
9.12.2.1 Comment Period.....	43
9.12.2.2 Mechanism to Handle Comments .....	43
9.12.3 Circumstances Under Which OID Must be Changed .....	43
<b>9.13 Dispute Resolution Provisions .....</b>	<b>43</b>
9.13.1 Disputes Among GeoTrust, Affiliates, and Customers.....	43
9.13.2 Disputes with End-User Subscribers or Relying Parties.....	43
<b>9.14 Governing Law .....</b>	<b>43</b>
<b>9.15 Compliance with Applicable Law.....</b>	<b>43</b>
<b>9.16 Miscellaneous Provisions.....</b>	<b>44</b>
9.16.1 Entire Agreement.....	44
9.16.2 Assignment .....	44
9.16.3 Severability.....	44
9.16.4 Enforcement (Attorney’s Fees and Waiver of Rights) .....	44
9.16.5 Force Majeure.....	44
<b>9.17 Other Provisions .....</b>	<b>44</b>
Appendix A. Table of Acronyms and Definitions .....	44
Table of Acronyms .....	44
Definitions.....	45

## 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 GeoTrust employs 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.

### **1.2 Document Name and Identification**

This document is the GeoTrust Certification Practice Statement.

### **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.

#### **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.

### **1.3.5 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.

#### **1.4.2 Prohibited Certificate Uses**

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 VeriSign, inc.. Inquiries should be addressed as follows:

VeriSign, Inc  
487 E. Middlefield Rd.  
Mountain View, CA 94043 USA  
+1 (650) 961-7500 (voice)  
+1 (650) 961-7300 (fax)  
practices@verisign.com

### **1.5.2 Contact Person**

Address inquiries about the CPS to [practices@verisign.com](mailto:practices@verisign.com) or to the following address:

VeriSign, Inc. Practices  
487 E Middlefield Rd.  
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 <http://www.geotrust.com/resources/repository/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 Table 5 below.

<b>Attribute</b>	<b>Value</b>
Country (C) =	2 letter ISO country code or not used.
Organization (O) =	The Organization attribute is used as follows: <ul style="list-style-type: none"> <li>• Subscriber organizational name for web server Certificates and individual Certificates that have an organization affiliation, or</li> <li>• 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</li> <li>• When applicable, wording to the effect that the organization has not been authenticated.</li> </ul>
Organizational Unit (OU) =	GeoTrust Certificates may contain multiple OU attributes. Such attributes may contain one or more of the following: <ul style="list-style-type: none"> <li>• Subscriber organizational unit (for organizational Certificates and individual Certificates that have an organization affiliation)</li> <li>• Text to describe the type of Certificate.</li> <li>• Text to describe the entity that performed the verification</li> <li>• “Domain Control Validated”, where appropriate</li> <li>• The address of the customer</li> </ul>
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: <ul style="list-style-type: none"> <li>• Domain name (for web server Certificates)</li> <li>• Organization name (for code/object signing Certificates)</li> <li>• Name of individual (for certificates issued to individuals).</li> <li>• IP Address (TrueBusiness ID)</li> </ul>
E-Mail Address (E) =	When used, the e-mail address associated with the certificate

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

##### 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 pregenerated 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 (a) verify the validity of the registration through the authority that issued it, or (b) verify the validity of the registration through a reputable third party database or other resource, or (c) verify the validity of the Organization through a trusted third party, or (d) 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).

### **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 IDs and Enterprise SSL and Enterprise SSL Premium Certificates.

True Business ID Certificates may contain an IP address in the CommonName field. GeoTrust Verifies the Organization's ownership of the IP address in these circumstances.

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 enrollment 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 conducted by GeoTrust, to another e-mail address containing the domain name that is listed as the Common Name in the enrollment form. 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.

<b>Product Name</b>
GeoTrust Power Server ID Certificates
GeoTrust QuickSSL Certificates
GeoTrust QuickSSL Premium 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 as specified below. 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 enrollment 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.

**3.2.4 Non-Verified Subscriber Information**

Non-verified subscriber information for all products includes:

- Organization Unit (OU)
- Any other information designated as non-verified in the certificate.

Non-verified subscriber information for, Power Server ID, and Quick SSL Certificates, also includes Country Code

**3.2.5 Validation of Authority**

GeoTrust will take reasonable steps to establish that a Certificate request made on behalf of that Organization is legitimate and properly authorized. To prove that a Certificate is duly authorized by the Organization, GeoTrust will typically request the name of a contact person who is employed by or is an officer of the Organization. GeoTrust will also typically require a form of

authorization from the Organization confirming its intent to obtain a Certificate and will usually document the Organization's contact person. GeoTrust normally confirms the contents of this authorization with the listed contact person

### **3.2.6 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.

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.

### **4.1.2.2 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.

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

### **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
- The Subscriber fails to respond to notices within a specified time, or
- Payment has not been received, or
- they believe that issuing a certificate to the Subscriber may bring the GeoTrust PKI into disrepute

### **4.2.3 Time to Process Certificate Applications**

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



A certificate application remains active until rejected or issued.

### **4.3 Certificate Issuance**

#### **4.3.1 CA Actions during Certificate Issuance**

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

#### **4.3.2 Notifications to Subscriber by the CA of Issuance of Certificates**

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

### **4.4 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.

#### **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 enduser 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.

#### **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:

- o whenever any of the information on the Certificate changes or becomes obsolete; or
- o whenever the Private Key, or the media holding the Private Key, associated with the Certificate is Compromised; or
- o 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:

- o upon request of a Subscriber as described above;
- o in the event of Compromise of GeoTrust's Private Key used to sign a Certificate;
- o upon the Subscriber's breach of either this CPS or Subscriber Agreement;
- o if GeoTrust determines that the Certificate was not properly issued; or
- o in the event the SSL Certificate is installed on more than a single server at a time without permission of GeoTrust.
- o If customer or subscriber has failed to meet its material obligations under the subscriber and /or Enrollment agreement
- o If an RA reasonably determines that Publisher Certificate is being used in a manner that compromises the trust status of relying parties.
- o 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.

#### **4.9.2 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 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. GeoTrust will then revoke the Certificate. 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/resources/crls/index.asp](http://www.geotrust.com/resources/crls/index.asp)

#### **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.

#### **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: <http://www.geotrust.com/resources/crls/index.asp>

#### **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.

#### **4.10.2 Service Availability**

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

#### **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 participant 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.

#### **4.12.2 Session Key Encapsulation and Recovery Policy and Practices**

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 enrollment 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.

## **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-30 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**

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

GeoTrust will maintain records of such training and ensure that personnel entrusted with Validation Specialist duties meet a minimum skills requirement that enable them to perform such duties satisfactorily. Validation Specialists engaged in EV Certificate issuance must maintain adequate skill levels in order to have issuance privilege, consistent with GeoTrust's training and performance programs.

GeoTrust will ensure that its Validation Specialists qualify for each skill level required by the corresponding validation task before granting privilege to perform said task. GeoTrust will require all Validation Specialists to pass an internal examination on the EV Certificate validation criteria outlined in the Guidelines.

### **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

### **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, but 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 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

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](http://www.geotrust.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.

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.

#### **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,
- Provisions needed for the transition of the CA's services to a successor CA, and
- The identity of the custodian of GeoTrust's CA and RA archival records. Unless a different custodian is indicated through notice to Subscribers and Relying Parties, the Registered Agent for GeoTrust, Inc., a Delaware corporation, shall be the custodian.

### **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.

#### **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 Resource Web site at <http://www.geotrust.com/resources>.

#### **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 recommends that Registration Authorities and end-user Subscribers generate 1024 bit RSA key pairs. Key sizes for True BusinessID and True Business ID with Extended validation can be found in Appendix A2 of the corresponding CPS.

#### **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. Subscribers are required by contract to take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of private keys.

#### **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.

### **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 of 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.

### **6.4 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**

### **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 3280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002 ("RFC 3280"). Certificate extensions and their criticality, as well as cryptographic algorithm object identifiers, are populated according to the IETF RFC3280 standards and recommendations. The name forms for Subscribers are enforced through GeoTrust's internal policies and the authentication steps described elsewhere in this CPS. Name constraint enforcement is not through the name constraint extension, but through the authentication steps followed and contractual limitations with each Subscriber. GeoTrust does not apply any specific Certificate Policy Object Identifier(s), but instead refers to the applicable CPS version and URL address. The policy constraints extensions and policy qualifiers syntax and semantics, when used, conform to the RFC 3280 standards.

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

### **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 3280: Internet X.509 Public Key Infrastructure Certificate.

#### **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 A3 to this CPS.

#### **7.1.2.3 Subject Alternative Names**

The subjectAltName extension of X.509 Version 3 Certificates, when used, is populated in accordance with RFC 3280.

#### **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 3280.

### **7.1.3 Algorithm Object Identifiers**

Cryptographic algorithm object identifiers, are populated according to the IETF RFC3280 standards and recommendations.

### **7.1.4 Name Forms**

GeoTrust populates Certificates in accordance with Section 3.1.1.

### **7.1.5 Name Constraints**

No stipulation

#### **7.1.6 Certificate Policy Object Identifier**

Only applicable to EV certificates in accordance with Appendix A3 to this CPS.

#### **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**

No stipulation

#### **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.

#### **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.

### **8.2 Identity/Qualifications of Assessor**

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

- Demonstrates proficiency in public key infrastructure technology, information security tools and techniques, security auditing, and the third-party attestation function, and
- 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.

### **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 (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**

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 site at <http://www.geotrust.com/resources>. If a Subscriber has paid the fees for the Certificate to another party such as a reseller, the Subscriber should request the refund from that party.

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. VeriSign's financial resources are set forth in disclosures appearing at: <http://investor.verisign.com/financials-income.cfm>

#### **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 [http://www.geotrust.com/resources/cps/pdfs/GeoSure\\_Plan\\_v3.0.pdf](http://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 enrollment forms for Certificates will be kept confidential by GeoTrust (such as contact information for individuals and credit card information) and GeoTrust shall not release such information without the prior consent of the Subscriber. Notwithstanding the foregoing, GeoTrust may make such information available (a) to courts, law enforcement agencies or other third parties (including release in response to civil

discovery) upon receipt of a court order or subpoena or upon the advice of GeoTrust's legal counsel, (b) to law enforcement officials and others for the purpose of investigating suspected fraud, misrepresentation, unauthorized access, or potential illegal activity by the Subscriber in the opinion of GeoTrust.

### **9.3.2 Information Not Within the Scope of Confidential Information**

Information appearing on Certificates, information relating to Certificate revocation, or to information regarding Subscribers that is already in the possession of or separately acquired by GeoTrust is not within the scope of confidential information.

GeoTrust may disclose Subscriber information on an aggregate basis, and the Subscriber hereby grants to GeoTrust a license to do so, including the right to modify the aggregated Subscriber information and to permit third parties to perform such functions on its behalf.

### **9.3.3 Responsibility to Protect Confidential Information**

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

## **9.4 Privacy of Personal Information**

### **9.4.1 Privacy Plan**

GeoTrust has implemented a privacy policy, which is located at: <http://www.geotrust.com/resources/legal/privacy.asp>.

### **9.4.2 Information Treated as Private**

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

### **9.4.3 Information Not Deemed Private**

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

### **9.4.4 Responsibility to Protect Private Information**

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

### **9.4.5 Notice and Consent to Use Private Information**

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

### **9.4.6 Disclosure Pursuant to Judicial or Administrative Process**

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

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

This section is subject to applicable privacy laws.

#### **9.4.7 Other Information Disclosure Circumstances**

No Stipulation

### ***9.5 Intellectual Property Rights***

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

#### **9.5.1 Property Rights in Certificates and Revocation Information**

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

#### **9.5.2 Property Rights in the CPS**

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

#### **9.5.3 Property Rights in Names**

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

#### **9.5.4 Property Rights in Keys and Key Material**

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

### ***9.6 Representations and Warranties***

#### **9.6.1 CA Representations and Warranties**

GeoTrust provides the following limited warranty at the time of Certificate issuance: (i) it issued the Certificate substantially in compliance with this CPS; (ii) the information contained within the Certificate accurately reflects the information provided to GeoTrust by the Applicant in all material respects; and (iii) it has taken reasonable steps to verify that the information within the Certificate is accurate (with the exception of True Credentials and True Credential Express Client Certificates). The nature of the steps GeoTrust takes to verify the information contained in a Certificate is set forth in this CPS.

#### **9.6.2 RA Representations and Warranties**



RAs warrant that:

- There are no material misrepresentations of fact in the Certificate known originating from the entities approving the Certificate Application or issuing Certificate,
- There are no errors in the information in the Certificate that were introduced 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 conform 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,
- 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.

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.

## **9.10 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 <http://www.geotrust.com/resources>. Amendments to this CPS will be evidenced by a new version number and date, except where the amendments are purely clerical.

### **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 Fairfax County, Virginia, 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 Fairfax County, Virginia, 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.

**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

**Appendix A. Table of Acronyms and Definitions**

**Table of Acronyms**

Term	Definition
<b>ANSI</b>	The American National Standards Institute.
<b>ACS</b>	Authenticated Content Signing
<b>BIS</b>	The United States Bureau of Industry and Science of the United States Department of Commerce
<b>CA</b>	Certificate Authority
<b>CP</b>	Certificate Policy
<b>CPS</b>	Certificate Practice Statement
<b>CRL</b>	Certificate Revocation List
<b>EAL</b>	Evaluation Assurance Level
<b>EV</b>	Extended Validation

<b>FIPS</b>	United State Federal Information Processing Standards.
<b>ICC</b>	International Chamber of Commerce.
<b>KRB</b>	Key Recovery Block.
<b>LSVA</b>	Logical security vulnerability assessment.
<b>OCSP</b>	Online Certificate Status Protocol.
<b>PCA</b>	Primary Certification Authority.
<b>PIN</b>	Personal identification number.
<b>PKCS</b>	Public-Key Cryptography Standard.
<b>PKI</b>	Public Key Infrastructure.
<b>PMA</b>	Policy Management Authority.
<b>QGIS</b>	Qualified Government Information Source
<b>QIIS</b>	Qualified Independent Information Source
<b>RA</b>	Registration Authority.
<b>RFC</b>	Request for comment.
<b>SAS</b>	Statement on Auditing Standards (promulgated by the American Institute of Certified Public Accountants)
<b>S/MIME</b>	Secure multipurpose Internet mail extensions.
<b>SSL</b>	Secure Sockets Layer.

## Definitions

Term	Definition
<b>Administrator</b>	A Trusted Person within the organization that performs validation and other CA or RA Functions.
<b>Administrator Certificate</b>	A Certificate issued to an Administrator that may only be used to perform CA or RA functions.
<b>Affiliate</b>	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.
<b>Applicant</b>	The Private Organization or Government Entity that applies for (or seeks renewal of) an EV Certificate naming it as the Subject.
<b>Applicant Representative</b>	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.
<b>Application Software Vendor</b>	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.
<b>Certificate</b>	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.
<b>Certificate Applicant</b>	An individual or organization that requests the issuance of a Certificate by a CA.
<b>Certificate Application</b>	A request from a Certificate Applicant (or authorized agent of the Certificate Applicant) to a CA for the issuance of a Certificate.

<b>Certificate Approver</b>	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.
<b>Certificate Chain</b>	An ordered list of Certificates containing an end-user Subscriber Certificate and CA Certificates, which terminates in a root Certificate.
<b>Certificate Management Control Objectives</b>	Criteria that an entity must meet in order to satisfy a Compliance Audit.
<b>Certificate Requester</b>	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.
<b>Certificate Revocation List (CRL)</b>	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.
<b>Certificate Signing Request</b>	A message conveying a request to have a Certificate issued.
<b>Certification Authority (CA)</b>	An entity authorized to issue, manage, revoke, and renew Certificates.
<b>Certificate Practices Statement (CPS)</b>	A statement of the practices that GeoTrust or an Affiliate employs in approving or rejecting Certificate Applications and issuing, managing, and revoking Certificates.
<b>Challenge Phrase</b>	A secret phrase chosen by a Certificate Applicant during enrollment 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.
<b>Class</b>	A specified level of assurances as defined within the CP. See CP § 1.1.1.
<b>Code Confirmation Certificate</b>	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.
<b>Compromise</b>	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.
<b>Confidential/Private Information</b>	Information required to be kept confidential and private pursuant to CP § 2.8.1.
<b>Contract Signer</b>	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.

<b><i>CRL Usage Agreement</i></b>	An agreement setting forth the terms and conditions under which a CRL or the information in it can be used.
<b><i>Demand Deposit Account</i></b>	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.
<b><i>EV Certificate:</i></b>	A digital certificate that contains information specified in the EV Guidelines and that has been validated in accordance with the Guidelines.
<b><i>EV OID</i></b>	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.
<b><i>Exigent Audit/Investigation</i></b>	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.
<b><i>Extended Validation</i></b>	Validation Procedures defined by the Guidelines for Extended Validation Certificates published by a forum consisting of major certification authorities and browser vendors.
<b><i>Intellectual Property Rights</i></b>	Rights under one or more of the following: any copyright, patent, trade secret, trademark, and any other intellectual property rights.
<b><i>Intermediate Certification Authority (Intermediate CA)</i></b>	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.
<b><i>Key Generation Ceremony</i></b>	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.
<b><i>Nonverified Subscriber Information</i></b>	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.
<b><i>Non-repudiation</i></b>	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.

<b>Offline CA</b>	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.
<b>Online CA</b>	CAs that sign end user Subscriber Certificates are maintained online so as to provide continuous signing services.
<b>Online Certificate Status Protocol (OCSP)</b>	A protocol for providing Relying Parties with real-time Certificate status information.
<b>Operational Period</b>	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.
<b>PKCS #10</b>	Public-Key Cryptography Standard #10, developed by RSA Security Inc., which defines a structure for a Certificate Signing Request.
<b>PKCS #12</b>	Public-Key Cryptography Standard #12, developed by RSA Security Inc., which defines a secure means for the transfer of private keys.
<b>Primary Certification Authority (PCA)</b>	A CA that acts as a root CA for a specific Class of Certificates, and issues Certificates to CAs subordinate to it.
<b>Principal Individual(s)</b>	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.
<b>Public Key Infrastructure</b>	The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based public key cryptographic system.
<b>Registration Agency</b>	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).
<b>Registration Authority (RA)</b>	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.
<b>Regulated Financial Institution</b>	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.
<b>Relying Party</b>	An individual or organization that acts in reliance on a certificate and/or a digital signature.
<b>Relying Party Agreement</b>	An agreement used by a CA setting forth the terms and conditions under which an individual or organization acts as a Relying Party.
<b>Reseller</b>	An entity marketing services on behalf of GeoTrust or an Affiliate to specific markets.



<b>RSA</b>	A public key cryptographic system invented by Rivest, Shamir, and Adelman.
<b>RSA Secure Server Certification Authority (RSA Secure Server CA)</b>	The Certification Authority that issues Secure Server IDs.
<b>RSA Secure Server Hierarchy</b>	The PKI hierarchy comprised of the RSA Secure Server Certification Authority.
<b>Secret Share</b>	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.
<b>Secret Sharing</b>	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.
<b>Secure Server ID</b>	A Class 3 organizational Certificate used to support SSL sessions between web browsers and web servers.
<b>Secure Sockets Layer (SSL)</b>	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.
<b>Subject</b>	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.
<b>Subscriber</b>	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.
<b>Subscriber Agreement</b>	An agreement used by a CA or RA setting forth the terms and conditions under which an individual or organization acts as a Subscriber.
<b>Subsidiary Company</b>	A subsidiary company is defined, for EV, as a company that is wholly owned by Applicant as verified by referencing a QIIS or from financial statement supplied by a registered Chartered Professional Accountant (CPA) or equivalent outside of the USA
<b>Trusted Person</b>	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.
<b>Trusted Position</b>	The positions within GeoTrust that must be held by a Trusted Person.
<b>Trustworthy System</b>	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.

<b>VeriSign</b>	Means, with respect to each pertinent portion of this CPS, VeriSign, Inc. and/or any wholly owned VeriSign subsidiary responsible for the specific operations at issue.
-----------------	---

**Appendix A1  
Supplemental Validation Procedures for  
Extended Validation SSL Certificates**

**TABLE OF CONTENTS**

	<b><u>Page</u></b>
<b>A. INTRODUCTION .....</b>	
1. Introduction .....	
<b>B. BASIC CONCEPT OF THE EV CERTIFICATE .....</b>	
2. Purpose of EV Certificates .....	
(a) Primary Purposes .....	
(b) Secondary Purposes .....	
(c) Excluded Purposes .....	
3. EV Certificate Warranties and Representations .....	
(a) By GeoTrust .....	
(b) By the Subscriber .....	
<b>C. COMMUNITY AND APPLICABILITY .....</b>	
4. Issuance of EV Certificates .....	
(a) Compliance .....	
(b) EV Policies .....	
(c) Insurance .....	
5. Obtaining EV Certificates .....	
(a) Private Organization Subjects .....	
(b) Government Entity Subjects .....	
(c) Excluded Subjects .....	
<b>D. EV CERTIFICATE CONTENT AND PROFILE .....</b>	
6. EV Certificate Content Requirements .....	
(a) Subject Organization Information .....	
7. EV Certificate Policy Identification Requirements .....	
(a) EV Subscriber Certificates .....	
(b) EV Subordinate CA Certificates .....	
(c) Root CA Certificates .....	
8. Maximum Validity Period .....	
(a) For EV Certificate .....	
(b) For Validated Data .....	
9. Other Technical Requirements for EV Certificates .....	
<b>E. EV CERTIFICATE REQUEST REQUIREMENTS .....</b>	
10. General Requirements .....	
(a) Documentation Requirements .....	
(b) Role Requirements .....	
11. EV Certificate Request Requirements .....	
(a) General .....	
(b) Request and Certification .....	
(c) Information Requirements .....	

	12.	Subscriber Agreement Requirements .....
	(a)	General .....
	(b)	Agreement Requirements .....
<b>F.</b>		<b>INFORMATION VERIFICATION REQUIREMENTS .....</b>
	13.	General Overview .....
	14.	Verification of Applicant's Legal Existence and Identity .....
	15.	Verification of Applicant's Legal Existence and Identity – Assumed Name .....
	16.	Verification of Applicant's Physical Existence .....
	(a)	Address of Applicant's Place of Business .....
	(b)	Telephone Number for Applicant's Place of Business .....
	17.	Verification of Applicant's Operational Existence .....
	18.	Verification of Applicant's Domain Name .....
		.....Verification of Name, Title and Authority of Contract Signer & Certificate Approver
	20.	Verification of Signature on Subscriber Agreement and EV Certificate Requests .....
	(a)	Verification Requirements .....
	21.	Verification of Approval of EV Certificate Request .....
	22.	Verification of Certain Information Sources .....
	(a)	Verified Legal Opinion .....
	(b)	Verified Accountant Letter .....
	(c)	Independent Confirmation From Applicant .....
	(d)	Qualified Independent Information Sources (QIIS) .....
	(e)	Qualified Government Information Sources (QGIS) .....
	23.	Other Verification Requirements .....
	(a)	High Risk Status .....
	(b)	Denied Lists and Other Legal Black Lists .....
	24.	Final Cross-Correlation and Due Diligence .....
	25.	Certificate Renewal Verification Requirements .....
<b>G.</b>		<b>CERTIFICATE STATUS CHECKING AND REVOCATION ISSUES .....</b>
	26.	EV Certificate Status Checking .....
	27.	EV Certificate Revocation .....
	28.	EV Certificate Problem Reporting and Response Capability .....
<b>H.</b>		<b>EMPLOYEE AND THIRD PARTY ISSUES.....</b>
	29.	Trustworthiness and Competence.....
	30.	Delegation of Functions to Registration Authorities and Subcontractors .....
<b>I.</b>		<b>DATA AND RECORD ISSUES .....</b>
	31.	Documentation and Audit Trail Requirements.....
	32.	Document Retention.....
	(a)	Audit Log Retention .....
	(b)	Retention of Documentation .....
	33.	Reuse and Updating Information and Documentation .....
	(a)	Use of Documentation to Support Multiple EV Certificates.....
	(b)	Use of Pre-Existing Information or Documentation.....
	34.	Data Security.....
<b>J.</b>		<b>COMPLIANCE.....</b>
	35.	Audit Requirements.....
	(a)	Pre-Issuance Readiness Audit.....
	(b)	Regular Self Audits .....
	(c)	Annual Independent Audit.....
	(d)	Auditor Qualifications .....
	(e)	Root Key Generation .....
<b>K.</b>		<b>OTHER CONTRACTUAL COMPLIANCE .....</b>
	36.	Privacy Issues .....
	37.	Limitations on EV Certificate Liability .....
	(a)	CA Liability .....
<b>L.</b>		<b>DEFINITIONS.....</b>

## A. INTRODUCTION

### 1. Introduction

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

## B. BASIC CONCEPT OF THE EV CERTIFICATE

### 2. Purpose of EV Certificates.

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

#### (a) Primary Purposes

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

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

#### (b) Secondary purposes

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

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

#### (c) Excluded Purposes

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

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

### **3. EV Certificate Warranties and Representations**

#### **(a) By GeoTrust**

Beneficiaries of EV Certificates may be:

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

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

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

- Status: GeoTrust will follow the requirements of these Guidelines and maintain a 24 x 7 online-accessible Repository with current information regarding the status of the EV Certificate as Valid or revoked; and
- Revocation: GeoTrust will follow the requirements of the Guidelines and promptly revoke the EV Certificate upon the occurrence of any revocation event as specified in the Guidelines and this Appendix.

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

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

**(b) By the Subscriber**

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

**C. COMMUNITY AND APPLICABILITY**

**4. Issuance of EV Certificates**

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

**(a) Compliance**

GeoTrust shall at all times:

- (1) Comply with all laws applicable to its business and the certificates it issues in each jurisdiction where it operates;
- (2) Comply with the requirements of the EV Guidelines;
- (3) Comply with the requirements of (i) the then-current WebTrust Program for CAs, and (ii) the then-current WebTrust EV Program, or an equivalent for both (i) and (ii) as approved by the CA/Browser Forum; and
- (4) Be licensed as a CA in each jurisdiction where it operates if licensing is required by the law of such jurisdiction for the issuance of EV Certificates.

## **(b) EV Policies**

### **(1) Implementation**

The GeoTrust CPS together with this Appendix A to the GeoTrust CPS:

- (A) Implement the requirements of the Guidelines as they are revised from time-to-time;
- (B) Implement the requirements of (i) the then current WebTrust Program for CAs, and (ii) the then-current WebTrust EV Program, or an equivalent for both (i) and (ii) as approved by the CA/Browser Forum;
- (C) Specify the CA's and its Root CA's entire root certificate hierarchy including all roots that its EV Certificates depend on for proof of those EV Certificates' authenticity. GeoTrust's root hierarchy structure is available at <http://www.geotrust.com/ev>

### **(2) Disclosure**

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

### **(3) Commitment to Comply with Guidelines**

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

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

## **(c) Insurance**

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

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

## **5. Obtaining EV Certificates**

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

### **(a) Private Organization Subjects**

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

- (1) The organization **MUST** be a legally recognized entity whose existence was created by a filing with (or an act of) the Incorporating or Registration Agency, or Governing Body in its Jurisdiction of Incorporation or Registration (e.g., by issuance of a certificate of incorporation), or is an entity that is chartered by a state or federal regulatory agency;
- (2) The organization **MUST** have designated with the Incorporating or Registration Agency, or Governing Body a Registered Agent, Registered Office (as required under the laws of the Jurisdiction of Incorporation or Registration) or an equivalent facility;
- (3) The organization **MUST** not be designated on the records of the Incorporating or Registration Agency, or Governing Body by labels such as "inactive," "invalid," "not current," or the equivalent;
- (4) The Private organization **MUST** have a verifiable physical existence and business presence
- (5) The organization's Jurisdiction of Incorporation or Registration and/or its Place of Business **MUST NOT** be in any country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and
- (6) The organization **MUST NOT** be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.

### **(b) Government Entity Subjects**

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

- (1) The legal existence of the Government Entity is established by the political subdivision in which such Government Entity operates; I;
- (2) The Government Entity **MUST NOT** be in any country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and
- (3) The Government Entity **MUST NOT** be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.

### **(c) Business Entities**

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

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



- (3) At least one Principal Individual associated with the Business Entity MUST be identified and validated. ;
- (4) The identified Principal Individual MUST attest to the representations made in the Subscriber Agreement;

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

## **D. EV CERTIFICATE CONTENT AND PROFILE**

### **6. EV Certificate Content Requirements**

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

#### **(a) Subject Organization Information**

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

##### **(1) Organization name**

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

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

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

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

##### **(2) Domain name**

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

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

### (3) Business Category:

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

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

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

**Table 1 Business category field content**

### (4) Jurisdiction of Incorporation or Registration

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

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

**Table 2. Jurisdiction of Incorporation or Registration Certificate Fields**

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

### **(5) Registration Number**

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

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

### **(6) Physical Address of Place of Business**

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

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

**Table 3. Physical address of Place of Business Certificate Fields**

## **7. EV Certificate Policy Identification Requirements**

### **(a) EV Subscriber Certificates**

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

### **(b) EV On-line Subordinate CA Certificate**

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

### **(c) EV Off-line Subordinate CA Certificate**

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

### **(d) Root CA Certificates**

There are two GeoTrust EV Root certificates.

1 – The off-line GeoTrust Extended Validation SSL CA will be signed by the Equifax Secure Certification Authority Root certificate. This Root CA does not contain the certificatePolicies or extendedKeyUsage fields.

2 – The On-line Extended Validation SSL CA certificate is signed by the EV off-line Subordinate CA, And it is also signed by the GeoTrust Primary Certificate Authority. The EV-Offline subordinate CA and the GeoTrust EV Root CA both have the same subject DN and use the same key which allows individuals validating the chain to chain to either of these CA certificates.

## **8. Maximum Validity Period**

### **(a) For EV Certificate**

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

### **(b) For Validated Data**

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

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

## **9. Other Technical Requirements for EV Certificates**

See Appendix A2 and Appendix A3 attached.

## **E. EV CERTIFICATE REQUEST REQUIREMENTS**

### **10. General Requirements**

#### **(a) Documentation Requirements**

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

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

#### **(b) Role Requirements**

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

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

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

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

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

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

## **11. EV Certificate Request Requirements**

### **(a) General**

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

### **(b) Request and Certification**

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

### **(c) Information Requirements**

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

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

- Organization Name: Applicant's formal legal organization name to be included in EV Certificate, as recorded with the Incorporating Agency in Applicant's Jurisdiction of Incorporation or Registration (for Private Organizations), or as specified in the law of the political subdivision in which the Government Entity operates (for Government Entities), or as registered with the government business Registration Agency (for Business Entities);
- ;
- Assumed Name (Optional): Applicant's assumed name (e.g., d/b/a name) to be included in the EV Certificate, as recorded in the jurisdiction of Applicant's Place of Business, if applicable;
- Domain Name: Applicant's fully qualified domain name to be included in the EV Certificate;

- Jurisdiction of Incorporation or Registration: Applicant's Jurisdiction of Incorporation or Registration to be included in EV Certificate, and consisting of:
  - (a) City or town (if any),
  - (b) State or province (if any), and
  - (c) Country.
- Incorporating or Registration Agency: The name of the Applicant's Incorporating or Registration Agency;
- Registration Number: The unique registration number assigned to Applicant by the Incorporating or Registration Agency in Applicant's Jurisdiction of Incorporation or Registration and to be included in EV Certificate (for Private Organization Applicants only).
- Applicant Address: The address of Applicant's Place of Business, including –
  - (a) Building number and street,
  - (b) City or town,
  - (c) State or province (if any),
  - (d) Country,
  - (e) Postal code (zip code), and
  - (f) Main telephone number.
- Certificate Approver: Name and contact information of the Certificate Approver submitting and signing, or that has authorized the Certificate Requester to submit and sign, the EV Certificate Application on behalf of the Applicant; and
- Certificate Requester: Name and contact information of the Certificate Requester submitting the EV Certificate Request on behalf of the Applicant, if other than the Certificate Approver.

## **12. Subscriber Agreement Requirements**

### **(a) General**

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

### **(b) Agreement Requirements**

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

- Accuracy of Information: An obligation and warranty to provide accurate and complete information at all times to GeoTrust, both in the EV Certificate Request and as otherwise requested by GeoTrust in connection with the issuance of the EV Certificate(s) to be supplied by GeoTrust;
- Protection of Private Key: An obligation and warranty by the subscriber or a subcontractor (e.g. hosting provider) to take all reasonable measures necessary to maintain sole control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested EV

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

- Acceptance of EV Certificate: An obligation and warranty that it will not install and use the EV Certificate(s) until it has reviewed and verified the accuracy of the data in each EV Certificate;
- Use of EV Certificate: An obligation and warranty to install the EV Certificate only on the server accessible at the domain name listed on the EV Certificate, and to use the EV Certificate solely in compliance with all applicable laws, solely for authorized company business, and solely in accordance with the Subscriber Agreement;
- Reporting and Revocation Upon Compromise: An obligation and warranty to promptly cease using an EV Certificate and its associated Private Key, and promptly request GeoTrust to revoke the EV Certificate, in the event that: (a) any information in the EV Certificate is or becomes incorrect or inaccurate, or (b) there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key listed in the EV Certificate;
- Termination of Use of EV Certificate. An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key listed in an EV Certificate upon expiration or revocation of that EV Certificate.

## **F. INFORMATION VERIFICATION REQUIREMENTS**

### ***13. General Overview***

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

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

### ***14. Verification of Applicant's Legal Existence and Identity***

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

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

GeoTrust obtains and records the specific unique Registration Number assigned to Applicant by the Incorporating or Registration Agency in the Applicant's Jurisdiction of Incorporation or Registration.

GeoTrust will also obtain and record the identity and address of the Applicant's Registered Agent or Registered Office (as applicable) in the Applicant's Jurisdiction of Incorporation or Registration.

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

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

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

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

### **16. Verification of Applicant's Physical Existence**

#### **(a) Address of Applicant's Place of Business**

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

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

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

- (1) For Applicants listed at the same Place of Business address in the current version of at least one (1) QIIS, or a Qualified Governmental Tax Information Source (QGTIS), GeoTrust confirms that the Applicant's address as listed in the EV Certificate Request is a valid business address for Applicant by reference to such QIIS or QGTIS, and may rely on Applicant's representation that such address is its Place of Business;
- (2) For Applicants who are not listed at the same Place of Business address in the current version of at least one (1) QIIS, or QGTIS, GeoTrust may confirm that the



address provided by the Applicant in the EV Certificate Request is in fact Applicant's business address by obtaining documentation of a site visit to the business address. When used, the site visit will be performed by a reliable individual or firm. The documentation of the site visit will:

- (a) Verify that the Applicant's business is located at the exact address stated in the EV Certificate Request (e.g., via permanent signage, employee confirmation, etc.);
  - (b) Identify the type of facility (e.g., office in a commercial building, private residence, storefront, etc.) and whether it appears to be a permanent business location;
  - (c) Indicate whether there is a permanent sign (that cannot be moved) that identifies the Applicant;
  - (d) Indicate whether there is evidence that Applicant is conducting ongoing business activities at the site (e.g., that it is not just a mail drop, P.O. box, etc.), and
  - (e) Include one or more photos of (i) the exterior of the site (showing signage indicating the Applicant's name, if present, and showing the street address if possible), and (ii) the interior reception area or workspace.
- (B) For Applicants whose Place of Business is not in the same country as the Applicant's Jurisdiction of Incorporation or Registration, GeoTrust requires a Verified Legal Opinion that indicates the address of Applicant's Place of Business and that business operations are conducted there.

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

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

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

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

- (A) Confirming the telephone number is listed as the Applicant's telephone number for the verified address of its Place of Business in records provided by the applicable phone company or alternatively in at least one (1) QIIS, or QGTIS; *or*
- (B) During a site visit, the person who is conducting the site visit MUST confirm the Applicant's, or a Parent/Subsidiary Company's, main telephone number by calling it and obtaining an affirmative response sufficient to enable a reasonable person to conclude that the Applicant is reachable by telephone at the number dialed.

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

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

## **17. Verification of Applicant's Operational Existence**

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

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

## **18. Verification of Applicant's Domain Name**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- (1) Name, Title and Agency. GeoTrust verifies the name and title of the Contract Signer and the Certificate Approver, as applicable, as well as the fact that they are agents representing the Applicant.
- (2) Authorization of Contract Signer. GeoTrust verifies, through a source other than the Contract Signer, that the Contract Signer is expressly authorized by the Applicant to enter into the Subscriber Agreement (and any other relevant contractual obligations) on behalf of the Applicant, including a contract that designates one or more Certificate Approvers on behalf of Applicant ("Signing Authority").
- (3) Authorization of Certificate Approver. GeoTrust verifies, through a source other than the Certificate Approver, that the Certificate Approver is expressly authorized by the Applicant to do the following, as of the date of the EV Certificate Request ("EV Authority"):
  - (a) Submit, and if applicable authorize a Certificate Requester to submit, the EV Certificate Request on behalf of the Applicant; and
  - (b) Provide, and if applicable, authorize a Certificate Requester to provide, the information requested from the Applicant by the CA for issuance of the EV Certificate; and
  - (c) Approve EV Certificate Requests submitted by a Certificate Requester

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

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

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

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

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

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

- (1) **Corporate Resolution:** The Signing Authority of the Contract Signer, and/or the EV Authority of the Certificate Approver, may be verified by reliance on a properly authenticated corporate resolution that confirms that the person has been granted such Signing Authority, provided that such resolution is (1) certified by the appropriate corporate officer (e.g., secretary), and (2) GeoTrust can reliably verify that the certification was validly signed by such person, and that such person does have the requisite authority to provide such certification.
- (2) **Independent Confirmation from Applicant:** The Signing Authority of the Contract Signer, and/or the EV Authority of the Certificate Approver, may be verified by obtaining an Independent Confirmation from Applicant.
- (3) **Contract between CA and Applicant:** The EV Authority of the Certificate Approver may be verified by reliance on a contract between GeoTrust and the Applicant that designates the Certificate Approver with such EV Authority, provided the contract is signed by the Contract Signer and provided that the agency and Signing Authority of the Contract Signer has been verified.
- (4) **Pre-Authorized Certificate Approver.** Where GeoTrust and the Applicant contemplate the submission of multiple future EV Certificate Requests and GeoTrust has:
  - o Verified the name and title of the Contract Signer and that he/she is an employee or agent of the Applicant, and
  - o Verified the Signing Authority of such Contract Signer in accordance with one of the procedures in this Section 19;

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

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

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

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

### **(a) Verification Requirements**

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

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

- (1) A letter mailed to the Applicant's or Registered Agent's address as verified through independent means in accordance with the Guidelines, c/o of the Certificate Requester or Contract Signer, as applicable, followed by a phone or mail response from someone who identifies themselves as such person confirming that he/she did sign the applicable document on behalf of the Applicant.
- (2) Use of a signature process that establishes the name and title of the signer in a secure manner, such as through use of an appropriately secure login process that identifies the signer before signing, or through use of a digital signature made with reference to an appropriately verified certificate.
- (3) Notarization by a notary, provided that GeoTrust independently verifies that such notary is a legally qualified notary in the jurisdiction of the Certificate Requester or Contract Signer;

## **21. Verification of Approval of EV Certificate Request**

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

## **22. Verification of Certain Information Sources**

### **(a) Verified Legal Opinion**

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

- (A) Status of Author. GeoTrust verifies that the legal opinion is authored by a legal practitioner retained by and representing the Applicant (or an in-house legal practitioner employed by the Applicant) (“Legal Practitioner”) who is either:
- (i) A lawyer (or solicitor, barrister, advocate, or equivalent) licensed to practice law in the Applicant’s Jurisdiction of Incorporation or Registration or any jurisdiction where the Applicant maintains an office or physical facility. GeoTrust verifies the professional status of the author of the legal opinion by directly contacting the authority responsible for registering or licensing such Legal Practitioner(s) in the applicable jurisdiction; or
  - (ii) A notary that is a member of the International Union of Latin Notaries, and is licensed to practice in the country of Applicant’s Jurisdiction of Incorporation or Registration or any jurisdiction where the Applicant maintains an office or physical facility (and that such jurisdiction recognizes the role of the Latin Notary).
- (B) Basis of Opinion. GeoTrust verifies that the Legal Practitioner is acting on behalf of the Applicant and that the conclusions of the Verified Legal Opinion are based on the Legal Practitioner’s stated familiarity with the relevant facts and the exercise of the Legal Practitioner’s professional judgment and expertise.
- (C) Authenticity. GeoTrust confirms the authenticity of the Verified Legal Opinion by calling or sending a copy of the legal opinion back to the Legal Practitioner at the address, phone number, facsimile, or (if available) e-mail address for the Legal Practitioner listed with the authority responsible for registering or licensing such Legal Practitioner and obtain confirmation from the Legal Practitioner or the Legal Practitioner’s assistant that the legal opinion is authentic. In circumstances where the opinion is digitally signed, in a manner that confirms the authenticity of the document and the identity of the signer, as verified by GeoTrust in Section 22(b)(2)(A), no further verification of authenticity is required.

## **(b) Verified Accountant Opinion Letter**

- (1) Verification Requirements. Before relying on any accountant letter submitted GeoTrust verifies that such accountant letter meets the following requirements (“Verified Accountant Letter”):
- (A) Status of Author. GeoTrust shall by directly contact the authority responsible for registering or licensing such Accounting Practitioner(s) in the applicable jurisdiction to establish that the accountant letter is authored by an independent professional accountant retained by and representing the Applicant (or an in-house professional accountant employed by the Applicant) (“Accounting Practitioner”) who is a certified public accountant, chartered accountant, or equivalent licensed by a full member of the International Federation of Accountants (IFAC) to practice accounting in the country of the Applicant’s Jurisdiction of Incorporation or Registration or any jurisdiction where the Applicant maintains an office or physical facility;
- (B) Basis of Opinion. The Accounting Practitioner is acting on behalf of the Applicant and that the conclusions of the Verified Accountant Letter are based on the Accounting Practitioner’s stated familiarity with the relevant facts and the exercise of the Accounting Practitioner’s professional judgment and expertise.
- (C) Authenticity. To confirm the authenticity of the accountant’s opinion, GeoTrust will call or send a copy of the accountant letter back to the Accounting Practitioner at the address, phone number, facsimile, or (if available) e-mail address for the Accounting Practitioner listed with the authority responsible for registering or licensing such Accounting Practitioner and obtain confirmation from the Accounting Practitioner or the Accounting Practitioner’s assistant that the

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

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

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

- (A) Qualification of Third-Party Validator. GeoTrust independently verifies that the Third-Party Validator is a legally-qualified Latin Notary or Notary (or legal equivalent in Applicant's jurisdiction), Lawyer, or Accountant in the jurisdiction of the individual's residency, by directly contacting the authority responsible for registering or licensing such Third-Party Validators in the applicable jurisdiction.
  
- (B) Document chain of custody. GeoTrust verifies that that the Third-Party Validator viewed the Vetting Documents in a face-to-face meeting with the individual being validated. The Third party validator must attest that they obtained the Vetting Documents submitted to the CA for the individual during a face-to-face meeting with the individual.
  
- (C) If the Third-Party Validator is not a Latin Notary, then GeoTrust confirms the authenticity of the attestation and vetting documents, by making a telephone call to the Third-Party Validator and obtaining confirmation from them or their assistant that they performed the face-to-face validation. GeoTrust may rely upon self-reported information obtained from the Third-Party Validator for the sole purpose of performing this verification process. In circumstances where the attestation is digitally signed, in a manner that confirms the authenticity of the documents, and the identity of the signer as verified by GeoTrust in Section 22(c)(2)(A), no further verification of authenticity is required.

### **(d) Independent Confirmation from Applicant**

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

- (i) Received by GeoTrust from a person employed by the Applicant (other than the person who is the subject of the inquiry) that has the appropriate authority to confirm such a fact ("Confirming Person"), and who represents that he/she has confirmed such fact;
- (ii) Received by GeoTrust in a manner that authenticates and verifies the source of the confirmation; and
- (iii) Binding on the Applicant.

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

- (1) Confirmation Request: GeoTrust will initiate an appropriate out-of-band communication requesting verification or confirmation of the particular fact in issue ("Confirmation Request") as follows:
  - (A) Addressee: The Confirmation Request MUST be directed to:
    - (i) A position within Applicant's organization that qualifies as a Confirming Person (e.g., Secretary, President, CEO, CFO, COO, CIO, CSO, Director,

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

- (ii) Applicant's Registered Agent or Registered Office in the Jurisdiction of Incorporation or Registration as listed in the official records of the Incorporating or Registration Agency, with instructions that it be forwarded to an appropriate Confirming Person.
  - (iii) A named individual verified to be in the direct line of management above the Contract Signer or Certificate Approver by contacting Applicant's Human Resources Department by phone or mail (at the verified phone number or address for Applicant's Place of Business)
- (B) Means of Communication: The Confirmation Request MUST be directed to the Confirming Person in a manner reasonably likely to reach such person. The following options are acceptable:
- (i) By paper mail, addressed to the Confirming Person at:
    - (a) The address of Applicant's Place of Business as verified by GeoTrust in accordance with these procedures; or
    - (b) The business address for such Confirming Person specified in a current government-operated Qualified Government Information Source (e.g., an SEC filing), a QIIS, a Qualified Government Tax Information Source, a Verified Legal Opinion, or a Verified Accountant Letter; or
    - (c) The address of Applicant's Registered Agent or Registered Office listed in the official records of the Jurisdiction of Incorporation or Registration; or
  - (ii) By e-mail addressed to the Confirming Person at the business e-mail address for such person listed in a current Qualified Government Information Source or a QIIS, a Verified Legal Opinion, or a Verified Accountant Letter; or
  - (iii) By telephone call to the Confirming Person, where such person is contacted by calling the main phone number of Applicant's Place of Business (verified in accordance with the Guidelines) and asking to speak to such person, and a person taking the call identifies himself as such person; or
  - (iv) By facsimile to the Confirming Person at the Place of Business. The facsimile number must be listed in a current Qualified Government Information Source or a QIIS, a Verified Legal Opinion, or a Verified Accountant Letter. The cover page must be clearly addressed to the Confirming Person.
- (2) Confirmation Response: GeoTrust must receive a response to the Confirmation Request from a Confirming Person that confirms the particular fact in issue. Such response may be provided by telephone, by e-mail, or by paper mail, so long as GeoTrust can reliably verify that it was provided by a Confirming Person in response to the Confirmation Request.

### **(e) Qualified Independent Information Sources (QIIS)**

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

### **(f) Qualified Government Information Source (QGIS)**

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



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

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

### ***23. Other Verification Requirements***

#### **(a) High Risk Status**

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

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

#### **(b) Denied Lists and Other Legal Black Lists**

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

- (a) Identified on any government denied list, list of prohibited persons, or other list that prohibits doing business with such organization or person under the laws of the country of GeoTrust’s jurisdiction(s) of operation; and
- (b) Has its Jurisdiction of Incorporation or Registration or Place of Business in any country with which the laws of GeoTrust’s jurisdiction prohibit doing business

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

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

### ***24. Final Cross-Correlation and Due Diligence***

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

### ***25. Certificate Renewal Verification Requirements.***

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

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

## **G. CERTIFICATE STATUS CHECKING AND REVOCATION ISSUES**

### **26. EV Certificate Status Checking.**

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

- (1) For EV Certificates:
  - (A) CRLs are updated and reissued at least every seven (7) days, and the nextUpdate field value SHALL NOT be more than ten (10) days; or
  - (B) OCSP. If used, GeoTrust's Online Certificate Status Protocol (OCSP) is updated at least every four (4) days, and with a maximum expiration time of ten (10) days.
- (2) For GeoTrust's subordinate CA Certificate for EV:
  - (A) CRLs. Are updated and reissued at least every twelve (12) months, and with a maximum expiration time of twelve (12) months; or
  - (B) OCSP. If used, GeoTrust's OCSP for CA Certificates for EV will be updated at least every twelve (12) months, and with a maximum expiration time of twelve (12) months.

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

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

### **27. EV Certificate Revocation.**

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

- (1) The Subscriber requests revocation of its EV Certificate;
- (2) The Subscriber indicates that the original EV Certificate Request was not authorized and does not retroactively grant authorization;
- (3) GeoTrust obtains reasonable evidence that the Subscriber's Private Key (corresponding to the Public Key in the EV Certificate) has been compromised, or that the EV Certificate has otherwise been misused;
- (4) GeoTrust receives notice or otherwise become aware that a Subscriber violates any of its material obligations under the Subscriber Agreement;
- (5) GeoTrust receives notice or otherwise become aware that a court or arbitrator has revoked a Subscriber's right to use the domain name listed in the EV Certificate, or that the Subscriber has failed to renew it domain name;
- (6) The CA receives notice or otherwise become aware of a material change in the information contained in the EV Certificate;

- (7) A determination, in GeoTrust's sole discretion, that the EV Certificate was not issued in accordance with the terms and conditions of these Guidelines or the CA's EV policies;
- (8) If GeoTrust determines that any of the information appearing in the EV Certificate is not accurate.
- (9) GeoTrust ceases operations for any reason and has not arranged for another EV CA to provide revocation support for the EV Certificate;
- (10) GeoTrust's right to issue EV Certificates under the Guidelines expires or is revoked or terminated [*unless GeoTrust makes arrangements to continue maintaining the CRL/OCSP Repository*];
- (11) GeoTrust's Private Key for its EV issuing CA Certificate has been compromised;
- (13) GeoTrust receives notice or otherwise become aware that a Subscriber has been added as a denied party or prohibited person to a blacklist, or is operating from a prohibited destination under the laws of GeoTrust's jurisdiction of operation.

## **28. EV Certificate Problem Reporting and Response Capability.**

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

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

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

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

## **H. EMPLOYEE AND THIRD PARTY ISSUES**

### **29. Trustworthiness and Competence**

#### **(a) Identity and Background Verification.**

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

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

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

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

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

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

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

**(b) Training and Skills Level.**

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

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

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

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

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

**(c) Separation of Duties.**

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

Such controls will be auditable.

***30. Delegation of Functions to Registration Authorities and Subcontractors***

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

## I. DATA AND RECORD ISSUES

### ***31. Documentation and Audit Trail Requirements***

- (a) GeoTrust records every action taken to process an EV Certificate Request and to issue an EV Certificate, including all information generated or received in connection with an EV Certificate Request, and every action taken to process the Request, including time, date, and personnel involved in the action. These records are available as auditable proof of the CA's practices. This also applies to all registration agents (RAs) and subcontractors as well.
- (b) The foregoing record requirements include, but are not limited to, an obligation to record the following events:
  - (i) CA key lifecycle management events, including:
    - (a) Key generation, backup, storage, recovery, archival, and destruction; and
    - (b) Cryptographic device lifecycle management events
  - (ii) CA and Subscriber EV Certificate lifecycle management events, including:
    - (a) EV Certificate Requests, renewal and re-key requests, and revocation;
    - (b) All verification activities required by these Guidelines
    - (c) Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
    - (d) Acceptance and rejection of EV Certificate Requests;
    - (e) Issuance of EV Certificates; and
    - (f) Generation of EV Certificate revocation lists (CRLs); and OCSP entries
  - (iii) Security events, including:
    - (a) Successful and unsuccessful PKI system access attempts;
    - (b) PKI and security system actions performed;
    - (c) Security profile changes;
    - (d) System crashes, hardware failures, and other anomalies;
    - (e) Firewall and router activities; and
    - (f) Entries to and exits from CA facility
  - (iv) Log entries will include the following elements:
    - (a) Date and time of entry;
    - (b) Identity of the persona and entity making the journal entry; and
    - (c) Description of entry

### ***32. Document Retention***

#### **(a) Audit Log Retention**

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

#### **(b) Retention of Documentation**

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

### **33. Reuse and Updating Information and Documentation**

#### **(a) Use of Documentation to Support Multiple EV Certificates**

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

#### **(b) Use of Pre-Existing Information or Documentation**

- (1) Each EV Certificate issued by GeoTrust will be supported by a valid current EV Certificate Request and a Subscriber Agreement signed by the Applicant Representative on behalf of the Applicant.
- (2) The age of information used by GeoTrust to verify such an EV Certificate Request will not exceed the Maximum Validity Period for such information set forth in these procedures and the Guidelines, based on the earlier of the date the information was obtained (e.g., the date of a confirmation phone call) or the date the information was last updated by the source (e.g., if an online database was accessed by GeoTrust on July 1, but contained data last updated by the vendor on February 1, then the date of information would be considered to be February 1).
- (3) In the case of outdated information, GeoTrust repeats the verification processes required in the Guidelines.

### **34. Data Security**

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

## **J. COMPLIANCE**

### **35. Audit Requirements**

#### **(a) Pre-Issuance Readiness Audit**

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

#### **(b) Regular Self Audits**

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

#### **(c) Annual Independent Audit**

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

The audit report is made publicly available by GeoTrust.

#### **(d) Auditor Qualifications**

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

- (1) Be an independent public accounting firm that has proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function and be currently licensed to perform WebTrust for CA audits and WebTrust EV Program audits, or to perform such alternate equivalent audits approved by the CA/Browser Forum as will be performed; and
- (2) Be a member of the American Institute of Certified Public Accountants (AICPA), or by a non-US equivalent that requires that audits be completed under defined standards that include the possession of certain skill sets, quality assurance measures such as peer review, competency testing, standards with respect to proper assignment of staff to engagements, and requirements for continuing professional education; and
- (3) Maintain Professional Liability/Errors & Omissions insurance, with policy limits of at least \$1 million in coverage

#### **(e) Root Key Generation**

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

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

### **K. OTHER CONTRACTUAL COMPLIANCE**

#### ***36. Privacy/Confidentiality Issues***

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

#### ***37. Limitations on EV Certificate Liability***

##### **(a) CA Liability**

- (1) Subscribers and Relying Parties

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

(2) Indemnification of Application Software Vendors

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

## L. DEFINITIONS

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

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

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

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

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## Appendix A2

### Minimum Cryptographic Algorithm and Key Sizes for EV Certificates

#### 1. Root CA Certificates

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

#### 2. Subordinate CA Certificates

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

#### 3. Subscriber Certificates

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

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

## Appendix A3

### EV Certificates Required Certificate Extensions

#### 1. Root CA Certificate

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

##### (a) basicConstraints

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

##### (b) keyUsage

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

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

#### 2. Subordinate CA Certificate

##### (a) certificatePolicies

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

certificatePolicies:policyIdentifier (Required)

- o anyPolicy if subordinate CA is controlled by Root CA
- o explicit EV policy OID(s) if subordinate CA is not controlled by Root CA

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

certificatePolicies:policyQualifiers:policyQualifierId

- o id-qt 2 [RFC 3280]

certificatePolicies:policyQualifiers:qualifier

- o URI to the Certificate Practice Statement

##### (b) cRLDistributionPoint

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

##### (c) authorityInformationAccess

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

**(d) basicConstraints**

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

**(e) keyUsage**

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

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

**3. Subscriber Certificate**

**(a) certificate Policies**

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

certificatePolicies:policyIdentifier (Required)

- o EV policy OID

certificatePolicies:policyQualifiers:policyQualifierId (Required)

- o id-qt 2 [RFC 3280]

certificatePolicies:policyQualifiers:qualifier (Required)

- o URI to the Certificate Practice Statement

**(b) cRLDistributionPoint**

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

**(c) authorityInformationAccess**

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

**(d) basicConstraints (optional)**

If present, the CA field **MUST** be set false.

**(e) keyUsage (optional)**

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

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

## **Appendix A4**

### **Country Specific Organization Name Guidelines**

#### **E-1. Japan**

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

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

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