

# **True Credentials® and True Credentials Express™ Certificate Practice Statement**

## **TABLE of CONTENTS**

### **I. INTRODUCTION**

- A. Overview
- B. Definitions
- C. Description and Use of Certificates

### **II. GENERAL PROVISIONS**

- A. Obligations
- B. Fees
- C. Security Audit
- D. Limited Warranty/Disclaimer
- E. Limitation on Liability
- F. Force Majeure
- G. Financial Responsibility
- H. Interpretation & Enforcement
- I. Repository and CRL
- J. Confidentiality Policy
- K. Waiver
- L. Survival
- M. Export

### **III. OPERATIONAL REQUIREMENTS**

- A. Application Requirements
- B. Certificate Information
- C. Procedure for Processing Certificate Applications
- D. Application Issues
- E. Certificate Delivery
- F. Certificate Acceptance
- G. Certificate Renewal and Rekey
- H. Certificate Expiration
- I. Certificate Revocation
- J. Certificate Suspension
- K. Key Management
- L. Subscriber Key Pair Generation
- M. Records Archival
- N. CA Termination

### **IV. PHYSICAL SECURITY CONTROLS**

- A. Site Location and Construction
- B. Physical Access Controls
- C. Power and Air Conditioning
- D. Water Exposures
- E. Fire Prevention and Protection
- F. Media Storage
- G. Waste Disposal
- H. Off-Site Backup

### **V. TECHNICAL SECURITY CONTROLS**

- A. CA Key Pair
- B. Subscriber Key Pairs
- C. Business Continuity Management Controls

D. Event Logging

## **VI. CERTIFICATE AND CRL PROFILE**

- A. Certificate Profile
- B. CRL Profile

## **VII. CPS ADMINISTRATION**

- A. CPS Authority
- B. Contact Person
- C. CPS Change Procedures

## **VIII. DEFINITIONS**

### **I. INTRODUCTION**

#### **A. Overview**

This GeoTrust Certificate Practice Statement (the "CPS") presents the principles and procedures GeoTrust employs in the issuance and life cycle management of GeoTrust True Credentials® and True Credentials Express™ Client Certificates. This CPS and any and all amendments thereto are incorporated by reference into all of the above-listed GeoTrust Certificates.

#### **B. Definitions**

For the purposes of this CPS, all capitalized terms used herein shall have the meaning given to them in Section VIII, Definitions, or elsewhere in this CPS.

#### **C. Description and Use of Certificates**

##### 1a. GeoTrust True Credentials Express Client Certificates

GeoTrust True Credentials Express Client Certificates are X.509 Certificates with S/MIME Extensions issued from GeoTrust's True Credentials CA 2 (which is chained to GeoTrust's Equifax Secure eBusiness CA-1 trusted root) and 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.

##### 1b. GeoTrust True Credentials Client Certificates

GeoTrust True Credentials Client Certificates are X.509 Certificates with S/MIME Extensions that may be off a customer branded private CA or issued from GeoTrust's True Credentials CA 2 (which is chained to GeoTrust's Equifax Secure eBusiness CA-1 trusted root) and 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.

##### 2. Operational Period of Certificates

GeoTrust True Credentials and True Credentials Express Client Certificates have an Operational Period of 379 days from the date of issuance, unless another time period or expiration date is specified on such Certificate, or unless the Certificate is revoked prior to the expiration of the Certificate's Operational Period.

### 3. Installation of Certificates:

Certificates may not be installed on more than a single client at a time.

### 4. Technical Requirements of Certificates

In order to use a Certificate, the appropriate client software must support X.509 v3.

## **II. GENERAL PROVISIONS**

### **A. Obligations**

#### 1. GeoTrust Obligations

GeoTrust will: (i) issue Certificates in accordance with this CPS; (ii) perform limited authentication of Company as described in this CPS; (iii) revoke Certificates issued to Company's Administrator as described in this CPS; and (iv) perform any other functions which are described within this CPS.

#### 2. Company's Obligations

Company will: (i) submit truthful information about itself and its business entity, domain ownership and contacts, as applicable; (ii) appoint an Administrator with authority to perform the RA Functions and to order, manage, and revoke the digital certificates provided under the True Credentials and True Credential Express Service (the "Service") on behalf of Company; (iii) abide by all the terms of this CPS; and (iv) immediately request revocation of its Administrator's Certificate if the related Private Key is Compromised. Company will only use Administrator's Certificate for access to the Service. Company is solely responsible for the protection of its Private Key and for notifying GeoTrust immediately in the event that its Private Key has been Compromised.

Company agrees that the Administrator shall have authority to submit Subscriber Certificate signing requests and to approve the issuance and revocation of Certificates for the Subscribers in accordance with this CPS. Company may change its designated Certificate Administrator by providing written notice to GeoTrust. GeoTrust will provide the Administrator with a unique Personal Identification Number (PIN) and URL and a client certificate for the purpose of managing the Certificates. All communications concerning the approval and revocation of Certificates to be issued to Company will be made by and through the designated Administrator. The Administrator will be responsible for verifying all the information in all Certificate orders submitted to GeoTrust on behalf of Company, and GeoTrust shall have no responsibility for verifying the accuracy or legitimacy of these orders. The Administrator must notify GeoTrust via the secure web-based administrator pages provided by GeoTrust immediately in the event he or she becomes aware of a Certificate that should be revoked for any reason.

#### 3. Subscriber Obligations

Subscriber will submit truthful information about himself or herself and his or her related business entity, e-mail, and contact information, as applicable. Subscribers will at all times abide by this CPS and a Subscriber will immediately request revocation of a Certificate if the related Private Key is Compromised. The Subscriber will only use the GeoTrust True Credentials and True Credential Express Client Certificate for SSL Client Authentication, VPN and S/MIME purposes authorized by Company. The Subscriber is solely responsible for the protection of its Private Key and for notifying Company immediately in the event that its Private Key has been Compromised.

#### 4. Relying Party Obligations

With regard to GeoTrust True Credentials and True Credential Express Client Certificates, Relying Parties must verify that the Certificate is valid by examining the Certificate Revocation List before initiating a transaction involving such Certificate. GeoTrust does not accept responsibility for reliance on a fraudulently obtained Certificate or a Certificate that is on the CRL.

#### **B. Fees**

##### 1. Issuance, Management, and Renewal Fees

GeoTrust is entitled to charge Company for the issuance, management, and renewal of Certificates. The fees charged will be as stated on GeoTrust's Web site or in any applicable contract at the time the Certificate is issued or renewed, and may change from time to time without prior notice.

##### 2. Certificate Access Fees

GeoTrust does not charge a fee as a condition of making a Certificate available in a repository or otherwise making Certificates available to Relying Parties.

##### 3. Revocation or Status Information Fees

GeoTrust does not charge a fee as a condition of making the CRL required by CPS Section II.I available in a repository or otherwise available to Relying Parties. GeoTrust may, however, charge a fee for providing customized CRLs, OCSP services, or other value-added revocation and status information services. GeoTrust does not permit access to revocation information, Certificate status information, or time stamping in its repository by third parties that provide products or services that utilize such Certificate status information without GeoTrust's prior express written consent.

##### 4. Fees for Other Services Such as Policy Information

GeoTrust does not charge a fee for access to this CPS.

##### 5. Refund Policy

GeoTrust's refund policy is available for review on the GeoTrust web site at <http://www.geotrust.com/resources>. If Company has paid the fees for the Certificate to another party such as a reseller, Company should request the refund from that party.

#### **C. Security Audit**

GeoTrust performs periodic internal security audits performed by trained and qualified security personnel according to GeoTrust's security policies and procedures. Results of the periodic audits are presented to GeoTrust's PKI Policy Authority with a description of any deficiencies noted and corrective actions taken.

#### **D. Limited Warranty/Disclaimer**

GeoTrust provides the following limited warranty at the time of Certificate issuance: (i) it issued the Certificate substantially in compliance with this CPS; and (ii) the information contained within the Certificate accurately reflects the information provided to GeoTrust by the Applicant in all material respects. The nature of the steps GeoTrust takes to verify the information contained in a Certificate is set forth in Section III of this CPS.

EXCEPT FOR THE LIMITED WARRANTY DESCRIBED ABOVE, GEOTRUST EXPRESSLY DISCLAIMS AND MAKES NO REPRESENTATION, WARRANTY OR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, WITH RESPECT TO THIS CPS OR ANY CERTIFICATE ISSUED HEREUNDER, INCLUDING WITHOUT LIMITATION, ALL WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE OR USE OF A CERTIFICATE OR ANY SERVICE (INCLUDING, WITHOUT LIMITATION, ANY SUPPORT SERVICES) PROVIDED BY GEOTRUST AS DESCRIBED HEREIN, AND ALL WARRANTIES, REPRESENTATIONS, CONDITIONS, UNDERTAKINGS, TERMS AND OBLIGATIONS IMPLIED BY STATUTE OR COMMON LAW, TRADE USAGE, COURSE OF DEALING OR OTHERWISE ARE HEREBY EXCLUDED TO THE FULLEST EXTENT PERMITTED BY LAW. EXCEPT FOR THE LIMITED WARRANTY DESCRIBED ABOVE, GEOTRUST FURTHER DISCLAIMS AND MAKES NO REPRESENTATION, WARRANTY OR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, TO ANY APPLICANT, COMPANY, SUBSCRIBER OR ANY RELYING PARTY THAT (A) THE SUBSCRIBER TO WHICH IT OR COMPANY HAS ISSUED A CERTIFICATE IS IN THE FACT THE PERSON, ENTITY OR ORGANIZATION IT CLAIMS TO HAVE BEEN (B) A SUBSCRIBER IS IN FACT THE PERSON, ENTITY OR ORGANIZATION LISTED IN THE CERTIFICATE, OR (C) THAT THE INFORMATION CONTAINED IN THE CERTIFICATES OR IN ANY CERTIFICATE STATUS MECHANISM COMPILED, PUBLISHED OR OTHERWISE DISSEMINATED BY GEOTRUST, OR THE RESULTS OF ANY CRYPTOGRAPHIC METHOD IMPLEMENTED IN CONNECTION WITH THE CERTIFICATES IS ACCURATE, AUTHENTIC, COMPLETE OR RELIABLE.

IT IS AGREED AND ACKNOWLEDGED THAT APPLICANTS, COMPANY, AND SUBSCRIBERS ARE LIABLE FOR ANY MISREPRESENTATIONS MADE TO GEOTRUST AND RELIED UPON BY A RELYING PARTY. GEOTRUST DOES NOT WARRANT OR GUARANTEE UNDER ANY CIRCUMSTANCES THE "NON-REPUDIATION" BY A SUBSCRIBER AND/OR RELYING PARTY OF ANY TRANSACTION ENTERED INTO BY THE COMPANY, SUBSCRIBER AND/OR RELYING PARTY INVOLVING THE USE OF OR RELIANCE UPON A CERTIFICATE.

IT IS UNDERSTOOD AND AGREED UPON BY COMPANY, SUBSCRIBERS, AND RELYING PARTIES THAT IN USING AND/OR RELYING UPON A CERTIFICATE THEY ARE SOLELY RESPONSIBLE FOR THEIR RELIANCE UPON THAT CERTIFICATE AND THAT SUCH PARTIES MUST CONSIDER THE FACTS, CIRCUMSTANCES AND CONTEXT SURROUNDING THE TRANSACTION IN WHICH THE CERTIFICATE IS USED IN DETERMINING SUCH RELIANCE.

THE COMPANY, SUBSCRIBERS, AND RELYING PARTIES AGREE AND ACKNOWLEDGE THAT CERTIFICATES HAVE A LIMITED OPERATIONAL PERIOD AND MAY BE REVOKED AT ANY TIME. COMPANY, SUBSCRIBERS, AND RELYING PARTIES ARE UNDER AN OBLIGATION TO VERIFY WHETHER A CERTIFICATE IS EXPIRED OR HAS BEEN REVOKED. GEOTRUST HEREBY DISCLAIMS ANY AND ALL LIABILITY TO COMPANY, SUBSCRIBERS, AND RELYING PARTIES WHO DO NOT FOLLOW SUCH PROCEDURES. MORE INFORMATION ABOUT THE SITUATIONS IN WHICH A CERTIFICATE MAY BE REVOKED CAN BE FOUND IN SECTION III(I) OF THIS CPS.

GeoTrust provides no warranties with respect to another party's software, hardware or telecommunications or networking equipment utilized in connection with the use, issuance, revocation or management of Certificates or providing other services (including, without limitation, any support services) with respect to this CPS. Applicants, Company, Subscribers, and Relying Parties agree and acknowledge that GeoTrust is not responsible or liable for any misrepresentations or incomplete representations of Certificates or any information contained therein caused by another party's application software or graphical user interfaces. The cryptographic key-generation technology used by Applicants, Company, Subscribers and Relying Parties in conjunction with the Certificates may or may not be subject to the intellectual property rights of third-parties. It is the responsibility of Applicants, Company, Subscribers and Relying

Parties to ensure that they are using technology which is properly licensed or to otherwise obtain the right to use such technology

#### **E. Limitation on Liability**

EXCEPT TO THE EXTENT CAUSED BY GEOTRUST'S WILLFUL MISCONDUCT, IN NO EVENT SHALL THE CUMULATIVE LIABILITY OF GEOTRUST TO APPLICANTS, COMPANY, SUBSCRIBER AND/OR ANY RELYING PARTY FOR ALL CLAIMS RELATED TO THE INSTALLATION OF, USE OF OR RELIANCE UPON A CERTIFICATE OR FOR THE SERVICES PROVIDED HEREUNDER INCLUDING WITHOUT LIMITATION ANY CAUSE OF ACTION SOUNDING IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, FOR BREACH OF A STATUTORY DUTY OR IN ANY OTHER WAY EXCEED FIFTY U.S. DOLLARS (\$50.00).

GEOTRUST SHALL NOT BE LIABLE IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, FOR BREACH OF A STATUTORY DUTY OR IN ANY OTHER WAY (EVEN IF GEOTRUST HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) FOR:

(I) ANY ECONOMIC LOSS (INCLUDING, WITHOUT LIMITATION, LOSS OF REVENUES, PROFITS, CONTRACTS, BUSINESS OR ANTICIPATED SAVINGS);

(II) TO THE EXTENT ALLOWED BY APPLICABLE LAW, ANY LOSS OR DAMAGE RESULTING FROM DEATH OR INJURY OF COMPANY, SUBSCRIBER, AND/OR ANY RELYING PARTY OR ANYONE ELSE;

(III) ANY LOSS OF GOODWILL OR REPUTATION; OR

(IV) ANY OTHER INDIRECT, CONSEQUENTIAL, INCIDENTAL, MULTIPLE, SPECIAL, PUNITIVE, EXEMPLARY DAMAGES

IN ANY CASE WHETHER OR NOT SUCH LOSSES OR DAMAGES WERE WITHIN THE CONTEMPLATION OF THE PARTIES AT THE TIME OF THE APPLICATION FOR, INSTALLATION OF, USE OF OR RELIANCE ON THE CERTIFICATE, OR AROSE OUT OF ANY OTHER MATTER OR SERVICES (INCLUDING, WITHOUT LIMITATION, ANY SUPPORT SERVICES) UNDER THIS CPS OR WITH REGARD TO THE USE OF OR RELIANCE ON THE CERTIFICATE.

BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, THE ABOVE EXCLUSIONS OF INCIDENTAL AND CONSEQUENTIAL DAMAGES MAY NOT APPLY TO AN APPLICANT, COMPANY, SUBSCRIBER, AND/OR A RELYING PARTY BUT SHALL BE GIVEN EFFECT TO THE FULL EXTENT PERMITTED BY LAW.

THE FOREGOING LIMITATIONS OF LIABILITY SHALL APPLY ON A CERTIFICATE-BY-CERTIFICATE BASIS, REGARDLESS OF THE NUMBER OF TRANSACTIONS OR CLAIMS RELATED TO EACH CERTIFICATE, AND SHALL BE APPORTIONED FIRST TO THE EARLIER CLAIMS TO ACHIEVE FINAL RESOLUTION.

In no event will GeoTrust be liable for any damages to Applicants, Company, Subscribers, Relying Parties or any other party arising out of or related to the use or misuse of, or reliance on any Certificate issued under this CPS that: (i) has expired or been revoked; (ii) has been used for any purpose other than as set forth in the CPS (See Section I(c) for more detail); (iii) has been tampered with; (iv) with respect to which the Key Pair underlying such Certificate or the cryptography algorithm used to generate such Certificate's Key Pair, has been Compromised by the action of any party other than GeoTrust (including without limitation the Company, Subscriber

or Relying Party); or (v) is the subject of misrepresentations or other misleading acts or omissions of any other party, including but not limited to Applicants, Company, Subscribers and Relying Parties.

In no event shall GeoTrust be liable to the Applicant, Company, Subscriber, Relying Party or other party for damages arising out of any claim that a Certificate infringes any patent, trademark, copyright, trade secret or other intellectual property right of any party.

## **F. Force Majeure**

GeoTrust shall not be liable for any default or delay in the performance of its obligations hereunder to the extent and while such default or delay is caused, directly or indirectly, by fire, flood, earthquake, elements of nature or acts of God, acts of war, terrorism, riots, civil disorders, rebellions or revolutions in the United States, strikes, lockouts, or labor difficulties or any other similar cause beyond the reasonable control of GeoTrust.

## **G. Financial Responsibility**

### 1. Fiduciary Relationships

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

### 2. Indemnification by Applicant and Company

Unless otherwise set forth in this CPS and/or Subscriber Agreement, Applicant and Company, as applicable, hereby agrees to indemnify and hold GeoTrust (including, but not limited to, its officers, directors, employees, agents, successors and assigns) harmless from any claims, actions, or demands that are caused by the use or publication of a Certificate and that arises from (a) any false or misleading statement of fact by the Applicant (or any person acting on the behalf of the Applicant); (b) any failure by the Applicant or the Company to disclose a material fact, if such omission was made negligibly or with the intent to deceive; (c) any failure on the part of the Company to protect its Private Key and Certificate or to take the precautions necessary to prevent the Compromise, disclosure, loss, modification or unauthorized use of the Private Key or Certificate; or (d) any failure on the part of the Company to promptly notify GeoTrust, as the case may be, of the Compromise, disclosure, loss, modification or unauthorized use of the Private Key or Administrator's Certificate once the Company has constructive or actual notice of such event.

## **H. Interpretation & Enforcement**

### 1. Governing Law

The enforceability, construction, interpretation, and validity of this CPS and any Certificates issued by GeoTrust shall be governed by the substantive laws of the Commonwealth of Massachusetts, United States of America, excluding (i) the conflicts of law provisions thereof and (ii) the United Nations Convention on Contracts for the International Sale of Goods.

### 2. Dispute Resolution Procedures

Any dispute, controversy or claim arising under, in connection with or relating to this CPS or any Certificate issued by GeoTrust shall be subject to and settled finally by binding arbitration in accordance with the Arbitration Rules of the American Arbitration Association (AAA). All arbitration proceedings shall be held in Boston, Massachusetts. There shall be one arbitrator

appointed by the AAA who shall exhibit a reasonable familiarity with the issues involved or presented in such dispute, controversy or claim. The award of the arbitrator shall be binding and final upon all parties, and judgment on the award may be entered by any court having proper jurisdiction thereof. This CPS and the rights and obligations of the parties hereunder and under any Certificate issued by GeoTrust shall remain in full force and effect pending the outcome and award in any arbitration proceeding hereunder. In any arbitration arising hereunder, each party to the proceeding shall be responsible for its own costs incurred in connection with the arbitration proceedings, unless the arbitrator determines that the prevailing party is entitled to an award of all or a portion of such costs, including reasonable attorneys fees actually incurred.

### 3. Conflict of Provisions

This CPS represents the entire agreement between any Company (including the Enrollment Agreement, if any) or Relying Party and GeoTrust and supersedes any and all prior understandings and representations pertaining to its subject matter. In the event, however, of a conflict between this CPS and any other express agreement a Company has with GeoTrust with respect to a Certificate, including but not limited to an Enrollment Agreement, such other agreement shall take precedence.

### 4. Severability

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

## **I. Repository and CRL**

With regard to GeoTrust True Credentials and True Credentials Express Client Certificates, GeoTrust shall operate a CRL that will be available to Company, Subscribers, and Relying Parties. GeoTrust shall post the CRL online at least weekly in a DER format (except as otherwise provided in GeoTrust's Business Continuity Plan). Each CRL is signed by the issuing GeoTrust CA. The procedures for revocation are as stated elsewhere in this CPS.

GeoTrust retains copies of all Certificates for the life of the CA, but does not archive or retain expired or superseded CRLs. GeoTrust does not provide other online status mechanisms (e.g., OCSP) for checking certificate status requests.

## **J. Confidentiality Policy**

### 1. Individual Subscriber Information

Information regarding Subscribers that is submitted on applications for Certificates will be kept confidential by GeoTrust and GeoTrust shall not release such information without the prior consent of the Subscriber. Notwithstanding the foregoing, GeoTrust may make such information available 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. The foregoing confidentiality obligation shall not apply, however, to information appearing on Certificates, information relating to Certificate revocation, or to information regarding Subscribers that is already in the possession of or separately acquired by GeoTrust. In addition, GeoTrust will release information regarding a Subscriber upon request submitted by the Subscriber in form satisfactory to GeoTrust.

### 2. Aggregate Subscriber Information

Notwithstanding the previous Section, GeoTrust may disclose Subscriber information on an aggregate basis, and the Subscriber hereby grants to GeoTrust a license to do so, including the

right to modify the aggregated Subscriber information and to permit third parties to perform such functions on its behalf. GeoTrust shall not disclose to any third party any personally identifiable information about any Subscriber that GeoTrust obtains in its performance of services hereunder.

#### **K. Waiver**

A failure or delay in exercising any right or remedy hereunder shall not operate as a waiver of that right or remedy, nor shall any single or partial exercise of any right or remedy preclude any other or further exercise thereof or the exercise of any other right or remedy.

#### **L. Survival**

The following sections shall survive, along with all definitions required thereby: Sections I, II, and VIII.

#### **M. Export**

Subscribers and Relying Parties acknowledge and agree to use Certificates in compliance with all applicable laws and regulations, including without limitation U.S. export laws and regulations. GeoTrust may refuse to issue or may revoke Certificates if in the reasonable opinion of GeoTrust such issuance or the continued use of such Certificates would violate applicable laws and regulations.

### **III. OPERATIONAL REQUIREMENTS**

#### **A. Enrollment Requirements**

An Applicant for the Service shall complete a GeoTrust True Credentials enrollment application on behalf of Company 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") within the True Credentials and True Credentials Express enrollment application and prove control over that email address as specified below. GeoTrust does not verify the authority of the Applicant to enroll in the Service. GeoTrust performs the Contact Address control verification steps listed below (and checks generally for errors and omissions relevant to the verification steps taken), but does not otherwise verify the accuracy of the information contained in the Applicant's enrollment form or otherwise check for errors and omissions.

#### **B. Company Information**

##### 1. Contact Address

GeoTrust does not verify that the Company had control over the Contact Address it provided at the time it submitted its application. Contact Addresses do not have to be meaningful or unique. GeoTrust is not involved in the recognition, authentication, or role of trademarks or domain names involved in Contact Addresses. Name disputes (including trademark disputes) in Contact Addresses are not resolved by GeoTrust, but are to be resolved between the Company and other disputing parties by the InterNIC at time of domain name application according to applicable InterNIC rules and/or by courts of competent jurisdiction.

##### 2. Organizational Name

Company may optionally choose to issue Certificates from a unique Certificate Authority that may or may not chain to the GeoTrust's True Credentials CA 2 (which is chained to GeoTrust's

Equifax Secure eBusiness CA-1 trusted root). Company attests to valid organizational representation by agreeing to the True Credentials enrollment agreement.

GeoTrust will insert the phrase “GeoTrust True Credentials Express Customer – Organization not validated” or similar language in the Organization field for all Client Certificates issued from the True Credentials Express service to indicate that Company has not been authenticated by GeoTrust.

### 3. RA Functions

Company will be responsible for performing all RA Functions prior to issuing Certificates to Subscribers, and GeoTrust will not perform any RA Functions except as described herein for issuance of the Administrator Certificate for access to the True Credentials and True Credentials Express service by Company. GeoTrust will insert the following Organization Unit fields for the True Credentials Express certificates issued:

“OU = Registration Authority (RA) - <Contact Address provided by Company>”

“OU = Identity authenticated by Registrations Authority (RA)”

“OU = Email control validated by GeoTrust”

or similar language in Certificates to inform Subscribers, Relying Parties, and others that questions concerning the RA Functions performed in connection with a Certificate may be directed to the Contact Address for which GeoTrust established control by Company at the time of enrollment.

### **C. Procedure for Processing Certificate Applications**

True Credential Express Subscribers submit their public key to GeoTrust for certification electronically through the use of a PKCS#10 Certificate Signing Request (CSR) or other package digitally signed by the Subscriber's private key in a session secured by Secure Sockets Layer (SSL). True Credential Subscribers submit their public key to GeoTrust for certification electronically through the use of a PKCS#10 CSR, other package digitally signed by the Subscriber's private key in a session secured by SSL, or via a P12 request. At a minimum, the Subscriber 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.

### **D. Application Issues**

At certain times during the application process, a customer service representative may be assigned to facilitate the completion of the application process.

### **E. Certificate Delivery**

If GeoTrust finds that a Subscriber's Certificate application contains all required information, then the Applicant's Certificate will be signed by GeoTrust. Upon signing the Applicant's Certificate, GeoTrust will attach such Certificate to an e-mail and send such e-mail to the appropriate contact. The e-mail will typically be sent to the Subscriber and Administrator, and will include the date the

Certificate was issued, the date the Certificate will expire, and the type of Certificate that was issued. Notification will not be sent to others than the subject of the Certificate and the Administrator. In certain circumstances the e-mail may include a GeoTrust customer service representative telephone number and e-mail address for any technical or customer service problems. GeoTrust, in its sole discretion, may provide such technical or customer support to the Company and to Subscribers. GeoTrust does not distribute Certificates via Integrated Circuit Cards (ICC) to Subscribers.

#### **F. Certificate Acceptance**

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

#### **G. Certificate Renewal and Rekey**

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to obtain a new certificate to maintain continuity of Certificate usage. GeoTrust generally requires that the Subscriber generate a new key pair to replace the expiring key pair (technically defined as "rekey"). However, because the Subscriber key pair is generated on a Client and most Client key generation tools permit the creation of a new Certificate Signing Request for an existing key pair, for some Certificates GeoTrust permits Subscribers to request a new Certificate for an existing key pair (technically defined as "renewal").

Certificate renewal is offered for True Credentials and True Credentials Express, so the Subscriber may either resubmit the prior CSR for resigning (renewal) or generate a new Public Key and complete a new Certificate request (rekey) before the Subscriber will be able to obtain a new Certificate. The fee for Certificate renewal is the same as for purchasing a new Certificate.

#### **H. Certificate Expiration**

GeoTrust will attempt to notify all Subscribers of the expiration date of their Certificate. Notification will generally be by e-mail message to the Subscriber and to Administrator, and will likely occur during the 21 days prior to the expiration date.

#### **I. Certificate Revocation**

##### 1. Circumstances For Revocation

Certificate revocation is the process by which GeoTrust or the Administrator prematurely ends the Operational Period of a Certificate.

##### a. Permissive Revocation

A Subscriber or the Administrator may request revocation of its Certificate at any time for any reason.

##### b. Required Revocation

A Subscriber shall inform the Administrator and promptly request revocation of a Certificate:

- whenever any of the information on the Certificate changes or becomes obsolete; or
- whenever the Private Key, or the media holding the Private Key, associated with the Certificate is compromised; or
- upon a change in the ownership of a Subscriber's Client; .

The Administrator shall revoke a Subscriber's Certificate:

- upon request of a Subscriber;
- upon the Subscriber's breach of either this CPS or Subscriber Agreement;
- if GeoTrust determines that the Certificate was not properly issued; or
- in the event the Certificate is installed on more than a single client at a time without permission of GeoTrust.

The Administrator shall inform GeoTrust and promptly request revocation of the Administrator's Certificate:

- whenever any of the information on the Administrator's Certificate changes or becomes obsolete; or
- whenever the Private Key, or the media holding the Private Key, associated with the Administrator's Certificate is compromised; or
- upon a change in the ownership of a Administrator's Client.

GeoTrust shall revoke an Administrator's Certificate:

- upon request of the Administrator;
- in the event of Compromise of GeoTrust's Private Key used to sign a Certificate (including an Administrator's Certificate); or
- upon the Company's breach of either this CPS or Enrollment Agreement;
- if GeoTrust determines that a Certificate was not properly issued;

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

## 2. Who Can Request Revocation

The only persons permitted to request revocation of or revoke a Certificate issued by GeoTrust is the Subscriber, Administrator, and GeoTrust.

## 3. Procedure For Revocation Request

If the Administrator wishes to revoke a Subscriber's Certificate, the Administrator may do so through the Web based applications provided to the Administrator by Company. The Administrator shall have sole responsibility for notifying Subscriber that the Certificate has been revoked. Upon revocation by the Administrator, GeoTrust will confirm the revocation request to the Administrator through the Web based application, the Certificate will be revoked, and the revocation will be posted to the appropriate CRL. Posting the revocation to the appropriate CRL will constitute notice to the Subscriber that the Certificate has been revoked. No further notification will be sent by GeoTrust to the Administrator, Subscriber, or others. There is no grace period available to the Subscriber prior to revocation, and GeoTrust shall revoke such Certificate within the next business day and post the revocation to the next published CRL.

As to revocation of client Certificates provided by GeoTrust to the Administrator for access to the Service, the Administrator must contact GeoTrust, either by e-mail message, a national/regional postal service, facsimile, or overnight courier, to request revocation of a Certificate. Upon receipt of a revocation request, GeoTrust will seek confirmation of the request by e-mail message to the Administrator. 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 Administrator that the Certificate has been revoked. GeoTrust will require a confirming e-mail message back from the Administrator authorizing revocation (or by other means

acceptable to GeoTrust). Upon receipt of the confirming e-mail message, the Certificate will be revoked and the revocation will be posted to the appropriate CRL. Notification will not be sent to others than the subject of the Certificate and the subject's designated contacts. There is no grace period available to the Administrator prior to revocation, and GeoTrust shall revoke such Certificate within the next business day and post the revocation to the next published CRL.

In the event of Compromise of GeoTrust's Private Key used to sign a Certificate; GeoTrust will send an e-mail message as soon as practicable to the Administrator and 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.

#### **J. Certificate Suspension**

GeoTrust does not support Certificate suspension for the Certificates.

#### **K. Key Management**

GeoTrust does not provide Subscriber private key protection or other Subscriber key management services in connection with its True Credentials Express Client Certificates. GeoTrust does provide Subscriber private key recovery services as a paid optional service in connection with its True Credential Client Certificates.

#### **L. Subscriber Key Pair Generation**

GeoTrust does not provide Subscriber key pair generation or Subscriber private key protection for the Certificates in connection with its True Credentials Express service. GeoTrust does provide Subscriber key pair generation or Subscriber private key protection for the Certificates in connection with its True Credentials service as an optional service.

#### **M. Records Archival**

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

#### **N. CA Termination**

In the event that it is necessary for GeoTrust or its CAs to cease operation, GeoTrust makes a commercially reasonable effort to notify Subscribers, Company, 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, Company, and Relying Parties, informing them of the status of the CA,
- Handling the cost of such notice,
- The revocation of the Certificate issued by GeoTrust,
- The preservation of the GeoTrust CA archives and records for the time periods required in this CPS,
- The continuation of Subscriber, Company, and customer support services,
- The continuation of revocation services, such as the issuance of CRLs,
- The revocation of unexpired unrevoked Certificates of Subscribers and Administrators, if necessary,
- The payment of compensation (if necessary) to Subscribers and/or Company (as appropriate) 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 GeoTrust CA private keys and the hardware tokens containing such private keys,
  - Provisions needed for the transition of the GeoTrust CA's services to a successor CA, and
  - The identity of the custodian of GeoTrust's CA and RA archival records. Unless a different custodian is indicated through notice to Subscribers and Relying Parties, the Registered Agent for GeoTrust, Inc., a Delaware corporation, shall be the custodian.

## **IV. PHYSICAL SECURITY CONTROLS**

### **A. Site Location and Construction**

GeoTrust's CA operations are conducted within GeoTrust's facilities in Billerica, Massachusetts and Suwanee, Georgia which meet WebTrust for CAs audit requirements. All GeoTrust CA operations are conducted within a physically protected environment designed to deter, prevent, and detect covert or overt penetration.

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

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

### **B. Physical Access Controls**

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

### **C. Power and Air Conditioning**

GeoTrust's CA facility is equipped with primary and backup:

- Power systems to ensure continuous, uninterrupted access to electric power and
- Heating/ventilation/air conditioning systems to control temperature and relative humidity.

### **D. Water Exposures**

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

### **E. Fire Prevention and Protection**

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

## **F. Media Storage**

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

## **G. Waste Disposal**

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed or zeroized in accordance with the manufacturers' guidance prior to disposal. Other waste is disposed of in accordance with GeoTrust's normal waste disposal requirements.

## **H. Off-Site Backup**

GeoTrust performs routine backups of critical system data, audit log data, and other sensitive information. Critical CA facility backup media are stored in a physically secure manner at an off-site facility.

# **V. TECHNICAL SECURITY CONTROLS**

## **A. CA Key Pair**

CA key pair generation is performed by multiple trained and trusted individuals using secure systems and processes that provide for the security and required cryptographic strength for the keys that are generated. All CA key pairs are generated in pre-planned key generation ceremonies in accordance with the requirements of GeoTrust security and audit requirements guidelines. The activities performed in each key generation ceremony are recorded, dated and signed by all individuals involved. These records are kept for audit and tracking purposes for a length of time deemed appropriate by GeoTrust management.

True Credentials Express Client Certificates and True Credentials Client Certificates (when not issued from a Customer branded CA) are issued from GeoTrust's True Credentials CA 2 (which is chained to GeoTrust's Equifax Secure eBusiness CA-1 trusted root), are generated in hardware, and are at least 1024 bit using the RSA generation algorithm. The cryptographic modules used for key generation and storage meet the requirements of FIPS 140-2 level 3. The True Credentials CA 2 and Equifax Secure eBusiness CA-1 CA Private Keys are backed up but not escrowed. The CA does not use an m of n multiperson control key split due to the internal hardware configuration.

The True Credentials CA 2 and Equifax Secure eBusiness CA-1 CA Root Keys may be used for Certificate signing (secure e-mail and server authentication).

GeoTrust makes the Equifax Secure eBusiness CA-1 CA Certificate available to Subscribers and Relying Parties through their inclusion in Microsoft and Netscape web browser software. For specific applications, GeoTrust's Public Keys are provided by the application vendors through the applications' root stores.

GeoTrust generally provides the full certificate chain (including the issuing CA and any CAs 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>.

There are no restrictions on the purposes for which the CA Key Pair may be used. The usage period or active lifetime for the Equifax Secure eBusiness CA-1 CA Public and Private keys is

through June 20, 2020, and are generally available in the Root Key Store of the applicable browser or application software. The usage period or active lifetime for the True Credentials CA 2 CA Public and Private Keys is through April 13, 2020.

GeoTrust CA Key Pairs are maintained in a trusted and highly secured environment with backup and key recovery procedures. In the event of the Compromise of one or more of the GeoTrust Root Key(s) (including the True Credentials CA 2 and Equifax Secure eBusiness CA-1 CAs), 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).

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 off-line media. Procedural controls will prevent archived CA Key Pairs from being returned to production use. Upon the end of the archive period, archived CA Private Keys will be securely destroyed.

GeoTrust CA Key Pairs are retired from service at the end of their respective maximum lifetimes as defined above, and so there is no key changeover. Certificates may be renewed as long as the cumulative certified lifetime of the Certificate key pair does not exceed the maximum CA Key Pair lifetime. New CA Key Pairs will be generated as necessary, for example to replace CA Key Pairs that are being retired, to supplement existing, active Key Pairs and to support new services in accordance with this CPS.

## **B. Subscriber Key Pairs**

GeoTrust recommends that Subscribers select the 1024-bit encryption strength option (or equivalent selection depending on the Subscriber's client software) when generating their certificate requests, although GeoTrust can support lesser encryption strength.

Generation of Subscriber Key Pairs is generally performed by the Subscriber, and may be generated in either hardware or software. For True Credentials Express and True Credentials Services, GeoTrust requires access to the crypto functions in Subscriber's Internet Explorer or Netscape browser software. Key Pairs generated by the Subscriber for GeoTrust True Credentials and True Credentials Express Client Certificates may be used for SSL client authentication, VPN, and S/MIME uses. There are no purposes for which GeoTrust restricts the use of the Subscriber key.

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

## **C. Business Continuity Management Controls**

GeoTrust has business continuity plans (BCP) to maintain or restore the GeoTrust CAs business operations in a reasonably timely manner following interruption to or failure of critical business processes. The BCP define the following time periods for acceptable system outage and recovery time:

1. Vet a Subscriber - 1 week
2. Issue a Certificate - 2 weeks
3. Publish a CRL - 2 weeks
4. Audit Vetting Procedures - 2 months

Backup copies of essential business and CA information are made daily. The recovery facilities are approximately 800 miles from the GeoTrust CA facility's main site.

## **D. Event Logging**

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

## **VI. CERTIFICATE AND CRL PROFILE**

### **A. Certificate Profile**

GeoTrust Certificates conform to (a) ITU-T Recommendation X.509 Version 3 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997, and (b) RFC 2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, January 1999 ("RFC 2459"). Certificate extensions and their criticality, as well as cryptographic algorithm object identifiers, are populated according to the IETF RFC 2459 standards and recommendations. The name forms for Subscribers are enforced through 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 2459 standards.

### **B. CRL Profile**

GeoTrust issued CRLs conform to all RFC 2459 standards and recommendations.

## **VII. CPS ADMINISTRATION**

### **A. CPS Authority**

The authority administering this CPS is the GeoTrust PKI Policy Authority. Inquiries to GeoTrust's PKI Policy Authority should be addressed as follows:

GeoTrust, Inc.  
117 Kendrick Street, Suite 350  
Needham, MA 02494 USA  
+1 (781) 292-4100 (voice)  
+1 (781) 444-3961 (fax)  
[kipolicy@geotrust.com](mailto:pkipolicy@geotrust.com)

GeoTrust does not support a Certificate Policy (CP) for True Credentials and True Credentials Express Client Certificates.

### **B. Contact Person**

Address inquiries about the CPS to [kipolicy@geotrust.com](mailto:pkipolicy@geotrust.com) or to the following address:

PKI Policy Administrator  
GeoTrust, Inc.  
117 Kendrick Street, Suite 350  
Needham, MA 02494 USA  
+1 (781) 292-4100 (voice)  
+1 (781) 444-3961 (fax)

## C. CPS Change Procedures

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

## VIII. DEFINITIONS

**Administrator.** A person appointed by the Company with authority to perform the RA Functions and to order, manage, and revoke the digital certificates provided under the Service on behalf of Company.

**Applicant.** A person or authorized agent that seeks enrollment in the Service and requests the issuance of an Administrator's Certificate on behalf of the Company.

**CA.** Certification Authority.

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

**Certificate Revocation List.** A time-stamped list of revoked Certificates that has been digitally signed by the CA.

**Certification Authority.** An entity which issues Certificates and performs all of the functions associated with issuing such Certificates.

**Company.** The company that enrolls for the Service.

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

**CRL.** See Certificate Revocation List.

**Extension.** A means to place additional information about a Certificate within a Certificate. The X.509 standard defines a set of Extensions that may be used in Certificates.

**GeoTrust.** GeoTrust, Inc.

**Key Pair.** Two mathematically related keys, having the following properties: (i) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally impractical to discover the other key.

**Operational Period.** A Certificate's period of validity. It would typically begin on the date the Certificate is issued (or such later date as specified in the Certificate), and ends on the date and time it expires as noted in the Certificate or is earlier revoked unless it is suspended.

**Private Key.** The key of a Key Pair used to create a digital signature. This key must be kept a secret.

**Public Key.** The key of a Key Pair used to verify a digital signature. The Public Key is made freely available to anyone who will receive digitally signed messages from the holder of the Key

Pair. The Public Key is usually provided via a Certificate issued by GeoTrust. A Public Key is used to verify the digital signature of a message purportedly sent by the holder of the corresponding Private Key.

**RA Functions.** The registration authority functions performed by the Administrator before issuing a Certificate to a Subscriber on behalf of the Company.

**Relying Party.** A recipient of a digitally signed message who relies on a Certificate to verify the digital signature on the message. Also, a recipient of a Certificate who relies on the information contained in the Certificate.

**Root Key(s).** The Private Key used by GeoTrust to sign the Certificates.

**Subscriber.** A person or entity who (1) is the subject named or identified in a Certificate issued to such person or entity, (2) holds a Private Key that corresponds to a Public Key listed in that Certificate, and (3) the person or entity to whom digitally signed messages verified by reference to such Certificate are to be attributed. For the purpose of this CPS, Subscriber includes both the Company that enrolls for the Service and also the individuals who are issued client Certificates by the company's designated Administrator.

Copyright 2004, GeoTrust, Inc.

[v. 2.3 11-17-04]