FreeSSL™ 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. Compliance 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, Inc. ("GeoTrust") Certificate Practice Statement (the "CPS") presents the principles and procedures GeoTrust employs in the issuance and life cycle management of GeoTrust FreeSSL™ Web Server 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

1. GeoTrust FreeSSL Web Server Certificates

GeoTrust FreeSSL Web Server Certificates are X.509 Certificates with SSL Extensions that chain to GeoTrust's UTN-USERFirst-Network Applications trusted root and which facilitate secure electronic commerce by providing limited authentication of a Subscriber's server and permitting SSL encrypted transactions between a Relying Party's browser and the Subscriber's server.

2. Operational Period of Certificates

GeoTrust Server FreeSSL Web Certificates have an Operational Period of three months, 379 days, 744 days, 1,109, or 1,474 days from the date of issuance (depending on whether the Subscriber has obtained a free three month trial certificate or purchased a one year, two year, three year, or four year Certificate), unless another time period or expiration date is specified on such Certificate, or unless the Certificate is revoked prior to the expiration of the Certificate's Operational Period.

4. Installation of Certificates:

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

5. Technical Requirements of Certificates

In order to use a Certificate, the appropriate server software must support SSLv3.

II. GENERAL PROVISIONS

A. Obligations

1. GeoTrust Obligations

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

2. Subscriber Obligations

Subscriber will submit truthful information about itself and its business entity, domain ownership and contacts, as applicable. Subscribers will not install a Certificate on more than a single server at a time. 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 FreeSSL Web Server Certificate for purposes of initiating SSL sessions. The Subscriber is solely responsible for the protection of its Private Key and for notifying GeoTrust immediately in the event that its Private Key has been Compromised.

3. Relying Party Obligations

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

2. Certificate Access Fees

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

3. Revocation or Status Information Fees

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

4. Fees for Other Services Such as Policy Information

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

5. Refund Policy

GeoTrust will refund fees and will revoke a Certificate upon request by the Subscriber within seven days of issuance or renewal of the Certificate. To request a refund, please call GeoTrust's

customer service Monday through Friday, 8:30 am – 5:00 pm Eastern Time (US holidays excluded) at +1 (888) 348-8043 Toll Free (United States), +1 (678) 942-0400 (International), +1 (770) 360-9571 (Fax). 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.

C. Compliance Audit

An annual WebTrust for Certification Authorities examination will be performed for the Certificates issued under this CPS. Customer-specific CAs are not specifically audited as part of the audit of GeoTrust's operations unless required by the Customer. GeoTrust's CA compliance audits are performed by a public accounting firm that (1) demonstrates proficiency in public key infrastructure technology, information security tools and techniques, security auditing, and the third-party attestation function, and (2) is accredited by the American Institute of Certified Public Accountants (AICPA), which requires the possession of certain skill sets, quality assurance measures such as peer review, competency testing, standards with respect to proper assignment of staff to engagements, and requirements for continuing professional education. Compliance audits of GeoTrust's operations will be performed by a public accounting firm that is independent of GeoTrust. The scope of GeoTrust's annual WebTrust for Certification Authorities examination will include certificate life cycle management and CA business practices disclosure.

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

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

D. Limited Warranty/Disclaimer

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

EXCEPT FOR THE LIMITED WARRANTY DESCRIBED ABOVE, GEOTRUST EXPRESSLY DISCLAIMS AND MAKES NO REPRESENTATION, WARRANTY OR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, WITH RESPECT TO THIS CPS OR ANY CERTIFICATE ISSUED HEREUNDER, INCLUDING WITHOUT LIMITATION, ALL WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE OR USE OF A CERTIFICATE OR ANY SERVICE (INCLUDING, WITHOUT LIMITATION, ANY SUPPORT SERVICES) PROVIDED BY GEOTRUST AS DESCRIBED HEREIN, AND ALL WARRANTIES, REPRESENTATIONS, CONDITIONS, UNDERTAKINGS, TERMS AND OBLIGATIONS IMPLIED BY STATUTE OR COMMON LAW, TRADE USAGE, COURSE OF DEALING OR OTHERWISE ARE HEREBY EXCLUDED TO THE FULLEST EXTENT PERMITTED BY LAW. EXCEPT FOR THE LIMITED WARRANTY

DESCRIBED ABOVE, GEOTRUST FURTHER DISCLAIMS AND MAKES NO REPRESENTATION, WARRANTY OR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, TO ANY APPLICANT, SUBSCRIBER OR ANY RELYING PARTY THAT (A) THE SUBSCRIBER TO WHICH IT HAS ISSUED A CERTIFICATE IS IN THE FACT THE PERSON, ENTITY OR ORGANIZATION IT CLAIMS TO HAVE BEEN (B) A SUBSCRIBER IS IN FACT THE PERSON, ENTITY OR ORGANIZATION LISTED IN THE CERTIFICATE, OR (C) THAT THE INFORMATION CONTAINED IN THE CERTIFICATES OR IN ANY CERTIFICATE STATUS MECHANISM COMPILED, PUBLISHED OR OTHERWISE DISSEMINATED BY GEOTRUST, OR THE RESULTS OF ANY CRYPTOGRAPHIC METHOD IMPLEMENTED IN CONNECTION WITH THE CERTIFICATES IS ACCURATE, AUTHENTIC, COMPLETE OR RELIABLE.

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

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

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

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

(III) ANY LOSS OF GOODWILL OR REPUTATION; OR

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

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

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

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

In no event will GeoTrust be liable for any damages to Applicants, Subscribers, Relying Parties or any other party arising out of or related to the use or misuse of, or reliance on any Certificate issued under this CPS that: (i) has expired or been revoked; (ii) has been used for any purpose other than as set forth in the CPS (See Section I(c) for more detail); (iii) has been tampered with; (iv) with respect to which the Key Pair underlying such Certificate or the cryptography algorithm used to generate such Certificate's Key Pair, has been Compromised by the action of any party other than GeoTrust (including without limitation the Subscriber or Relying Party); or (v) is the subject of misrepresentations or other misleading acts or omissions of any other party, including but not limited to Applicants, Subscribers and Relying Parties.

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

F. Force Majeure

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

G. Financial Responsibility

1. Fiduciary Relationships

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

2. Indemnification by Applicant and Subscriber

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

H. Interpretation & Enforcement

1. Governing Law

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

2. Dispute Resolution Procedures

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

3. Conflict of Provisions

This CPS represents the entire agreement between any Subscriber (including the Subscriber Agreement, if any) or Relying Party and GeoTrust and supersedes any and all prior understandings and representations pertaining to its subject matter. In the event, however, of a

conflict between this CPS and any other express agreement a Subscriber has with GeoTrust with respect to a Certificate, including but not limited to a Subscriber Agreement, such other agreement shall take precedence.

4. Severability

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

I. Repository and CRL

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

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

J. Confidentiality Policy

1. Individual Subscriber Information

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. Application Requirements

An Applicant for a GeoTrust FreeSSL Web Server Certificate shall complete a GeoTrust FreeSSL Web Server Certificate application in a form prescribed by GeoTrust. All applications are subject to review, approval and acceptance by GeoTrust. All Applicants are required to include a Domain Name within the FreeSSL Certificate application. GeoTrust does not verify the authority of the Subscriber to request a Certificate. GeoTrust performs the authentication steps listed below (and checks generally for errors and omissions relevant to the authentication steps taken), but does not otherwise verify the accuracy of the information contained in the Subscriber's Certificate request or otherwise check for errors and omissions.

B. Certificate Information

1. Domain Name Control.

GeoTrust will verify that the Subscriber has control over such Domain Name at the time it submitted its application. 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) after approval a manual process conducted by GeoTrust, to another e-mail address containing the Domain Name that is listed as the Common Name in the Certificate order. Upon receipt of a confirming e-mail message authorizing issuance of the Certificate, GeoTrust will issue the Certificate as described below.

Domain names do not have to be meaningful or unique, but must match a second level domain name as posted by the InterNIC. GeoTrust is not involved in the recognition, authentication, or role of trademarks involved in domain names. Name disputes (including trademark disputes) are not resolved by GeoTrust, but are to be resolved between the Subscriber and other disputing parties by the InterNIC at time of application according to applicable InterNIC rules and/or by courts of competent jurisdiction.

2. Organizational Name

GeoTrust will insert an Organization Unit field "Organization Not Validated" or similar language for all FreeSSL Web Server Certificates.

C. Procedure for Processing Certificate Applications

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

the Subscriber must provide the following data in or with the CSR: Common Name and the names, e-mail addresses, and telephone numbers for the Administrative, Technical, Support, and Billing points of contact.

GeoTrust will process the QuickSSL Certificate Applications in the manner described above. However, GeoTrust reserves the right to use subcontractors or other third parties to assist in the performance of its operational requirements or any other obligation under this CPS.

D. Application Issues

At certain times during the application process in which GeoTrust is not able to verify information in a Certificate application, 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 application for a Certificate.

E. Certificate Delivery

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

F. Certificate Acceptance

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

G. Certificate Renewal and Rekey

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to obtain a new certificate to maintain continuity of Certificate usage. For some PKI digital certificates, 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 Certificate Signing Request for an existing key pair (technically defined as "renewal"), depending on their preferences and the capabilities and restrictions of the Subscriber's web server and web server key generation tools.

Certificate renewal is not offered for FreeSSL, and so the Subscriber is required to generate a new Public Key and complete a new Certificate request (rekey) before the Subscriber will be able to obtain a renewal Certificate. The process and cost for obtaining the new FreeSSL Certificate upon expiration of a previous FreeSSL Certificate will be the same as if the Subscriber is simply buying a FreeSSL Certificate for the first time. Free three month FreeSSL trial Certificates will not be provided more than once to the same Domain Name.

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 administrative, technical, and/or billing contacts listed in the enrollment application submitted by Subscriber, and will likely occur during the 21 days prior to the expiration date. If Subscriber's application was submitted by another

party on Subscriber's behalf, GeoTrust likely will not send expiration notices to that party due to contractual limitations.

I. Certificate Revocation

1. Circumstances For Revocation

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

a. Permissive Revocation

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

b. Required Revocation

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

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

GeoTrust shall revoke a Certificate:

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

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

2. Who Can Request Revocation

The only persons permitted to request revocation of or revoke a Certificate issued by GeoTrust is the Subscriber (including designated representatives) and GeoTrust.

3. Procedure For Revocation Request

Subscriber must contact GeoTrust, either by e-mail message, a national/regional postal service, facsimile, or overnight courier, and request revocation of a Certificate. Upon receipt of a revocation request, GeoTrust will seek confirmation of the request by e-mail message to the administrative and technical contacts provided by the Subscriber at the time the Certificate was issued. 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 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 Subscriber 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 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 FreeSSL Web Server Certificates.

L. Subscriber Key Pair Generation

GeoTrust does not provide Subscriber key pair generation or Subscriber private key protection for the Certificates.

M. Records Archival

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

N. CA Termination

In the event that it is necessary for GeoTrust or its CAs to cease operation, GeoTrust 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 end-user Subscribers and subordinate CAs, if necessary,
- The payment of compensation (if necessary) to Subscribers whose unexpired unrevoked Certificates are revoked under the termination plan or provision, or alternatively, the issuance of replacement Certificates by a successor CA,
- Disposition of the CA's private key and the hardware tokens containing such private key,
- Provisions needed for the transition of the CA's services to a successor CA, and
- The identity of the custodian of GeoTrust's CA and RA archival records. Unless a different custodian is indicated through notice to Subscribers and Relying Parties, the Registered Agent for GeoTrust, Inc., a Delaware corporation, shall be the custodian.

IV. PHYSICAL SECURITY CONTROLS

A. Site Location and Construction

GeoTrust's CA operations are conducted within GeoTrust's facilities in Wellesley Hills, Massachusetts and Alpharetta, 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
- Card key access for specially approved employees with defined levels of management approval required

B. Physical Access Controls

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

C. Power and Air Conditioning

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

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

D. Water Exposures

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

E. Fire Prevention and Protection

Fire prevention for GeoTrust's CA facility is by strict building fire prevention protocol. Detection is by centralized and 24 hour a day/7 day a week monitored smoke, heat, and ionization detection. Fire suppression is by FM 200 in all computing areas and by dry pipe water in all office areas.

F. Media Storage

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

G. Waste Disposal

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

H. Off-Site Backup

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

FreeSSL Web Server Certificates are issued off the UTN-USERFirst-Network Applications CA, are generated in software, and are at least 2048 bit using the RSA generation algorithm. The UTN-USERFirst-Network Applications CA private signature keys are backed up but not escrowed. The CA private key is maintained under m out of n multiperson control.

The UTN-USERFirst-Network Applications CA key may be used for Digital Signature , Non-Repudiation , Certificate Signing (secure e-mail and server authentication), Off-line CRL Signing, and CRL Signing.

GeoTrust makes the CA Certificates available to Subscribers and Relying Parties through their inclusion in Microsoft 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 end-user 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 UTN-USERFirst-Network Applications CA public and private keys is through July 9, 2019, and is generally available in the Root Key Store of the applicable browser or application software.

GeoTrust CA key pairs are maintained in a trusted and highly secured environment with backup and key recovery procedures. In the event of the Compromise of one or more of the GeoTrust Root Key(s) (including the UTN-USERFirst-Network Applications CA), 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, 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 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 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 end-user Subscribers select the 1024-bit encryption strength option when generating their certificate requests. All GeoTrust certificates are 128-bit, which will accommodate the use of 128-, 56-, and 40-bit strength browsers and web servers.

Generation of end-user Subscriber key pairs is generally performed by the Subscriber, and may be generated in either hardware or software. For server Certificates, the Subscriber typically uses the key generation utility provided with the web server software. GeoTrust does not require any particular standard for the module used to generate the keys. Key pairs generated by the Subscriber for GeoTrust FreeSSL Web Server Certificates may be used for server authentication. 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.
40 Washington Street, Suite 20
Wellesley Hills, MA 02481 USA
+1 (781) 235-4677 (voice)
+1 (781) 235-4732 (fax)
pkipolicy@geotrust.com

GeoTrust does not support a Certificate Policy (CP) for FreeSSL Web Server Certificates)

B. Contact Person

Address inquiries about the CPS to pkipolicy@geotrust.com or to the following address:

PKI Policy Administrator
GeoTrust, Inc.
40 Washington Street, Suite 20
Wellesley Hills, MA 02481 USA
+1 (781) 235-4677 (voice)
+1 (781) 235-4732 (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

Applicant. A person or authorized agent that requests the issuance of a Certificate on behalf of the Subscriber.

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.

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.

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

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

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

Subscriber. A person or entity who (1) is the subject named or identified in a Certificate issued to such person or entity, (2) holds a Private Key that corresponds to a Public Key listed in that Certificate, and (3) the person or entity to whom digitally signed messages verified by reference to such Certificate are to be attributed. For the purpose of this CPS, a person or entity who applies for a Certificate by the submission of an application is also referred to as a Subscriber.

Copyright 2002, GeoTrust, Inc.