

# **Acrobat Credentials Certificate Practice Statement**

## **TABLE of CONTENTS**

### **I. INTRODUCTION**

- A. Overview
- B. Definitions
- C. Description and Use of CDS 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 ("GeoTrust") Certificate Practice Statement (the "CPS") presents the principles and procedures GeoTrust employs in the issuance and life cycle management of Acrobat Credentials CDS Certificates. This CPS and any and all amendments thereto are incorporated by reference into all of the above-listed CDS 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 CDS Certificates ("CDS Certificates")**

##### 1. CDS Certificates

CDS Certificates are X.509 Certificates that chain to the Adobe Root CA. These CDS Certificates may be used solely for purposes of digitally signing and verifying Adobe Acrobat documents.

##### 2. Operational Period of CDS Certificates

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

##### 3. Installation of Certificates

The Private Key of the CDS Certificates may not be installed on more than one client or cryptographic token at a time.

##### 4. Technical Requirements of CDS Certificates

In order to use a CDS Certificate, the appropriate application for client authentication must be used.

### **II. GENERAL PROVISIONS**

#### **A. Obligations**

##### 1. GeoTrust Obligations

GeoTrust will: (i) issue CDS 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, as applicable. Subscribers will not install a CDS Certificate on more than one client or cryptographic device. Subscribers will at all times abide by this CPS. The Subscriber will only use the CDS Certificates for purposes of digitally signing and verifying Adobe Acrobat documents. 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 CDS Certificates, Relying Parties must verify that the CDS Certificate is valid by examining the Certificate Revocation List before validating a certified document. In addition, Relying Parties may only rely on a CDS-signed document if verified on a Supported Platform, including, without limitation, via the userNotice field within each CDS Certificate. GeoTrust does not accept responsibility for reliance on a fraudulently obtained CDS Certificate or a CDS 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 CDS Certificates. The fees charged will be as stated on GeoTrust's Web site or in any applicable contract at the time the CDS 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 CDS Certificate available in a repository or otherwise making CDS Certificates available to Relying Parties.

### 3. Revocation or Status Information Fees

GeoTrust does not charge a fee as a condition of making the CRL 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 a Subscriber has paid the fees for the CDS 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. 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 has complied in all material respects with the CDS CP and this CPS; (ii) the information contained within the Certificate accurately reflects the information provided to GeoTrust by the Applicant in all material respects; (iii) it has taken reasonable steps to verify that the information within the Certificate is accurate; and (iv) it has required the Subscriber to accept the Subscriber Agreement. The nature of the steps GeoTrust takes to verify the information contained in a CDS 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 CDS 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 CDS CERTIFICATE, OR (C) THAT THE INFORMATION CONTAINED IN THE CDS CERTIFICATES OR IN ANY CDS CERTIFICATE STATUS MECHANISM COMPILED, PUBLISHED OR OTHERWISE DISSEMINATED BY GEOTRUST, OR THE RESULTS OF ANY CRYPTOGRAPHIC METHOD IMPLEMENTED IN CONNECTION WITH THE CDS 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 CDS CERTIFICATE.

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

THE SUBSCRIBERS AND RELYING PARTIES AGREE AND ACKNOWLEDGE THAT CDS 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 CDS 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 CDS 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 CDS 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 CDS 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 FIVE THOUSAND U.S. DOLLARS (\$5,000.00).

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 CDS 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 CDS 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 FULLEST 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 CDS 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 CDS 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 CDS Certificate or the cryptography algorithm used to generate such CDS Certificate's Key Pair, has been Compromised by the action of any party other than GeoTrust (including without limitation the Subscriber or Relying Party); (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; or (vi) not verified on a Supported Platform, including, without limitation, via the userNotice field within each CDS Certificate.

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 CDS 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 and Adobe (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 CDS 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 CDS Certificate or to take the precautions necessary to prevent the Compromise, disclosure, loss, modification or unauthorized use of the Private Key or CDS Certificate; (d) any failure on the part of the Subscriber to immediately notify GeoTrust, as the case may be, of the Compromise, disclosure, loss, modification or unauthorized use of the Private Key or CDS Certificate once the Subscriber has constructive or actual notice of such event; or (e) caused by any breach of the Subscriber Agreement, including without limitation, as a result of reliance on any misrepresentation of a material fact by Subscriber.

### **3. Indemnification by Relying Parties**

The Relying Party hereby agrees to indemnify and hold GeoTrust and Adobe (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 any breach of any Relying Party agreements, Adobe end user license agreement, including, without limitation any failure to check the CDS Certificate status prior to any reliance on a digital signature from a Subscriber.

## **H. Interpretation & Enforcement**

### **1. Governing Law**

The enforceability, construction, interpretation, and validity of this CPS and any CDS 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 CDS 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 CDS 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 CDS 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**

GeoTrust shall operate a CRL that will be available to both Subscribers and Relying Parties. GeoTrust shall post the updates to the CRL online no later than twenty-four (24) hours after revocation by GeoTrust in a DER format (except as otherwise provided in GeoTrust's Business Continuity Plan). Information relating to the status of a CDS Certificate will be published no later than twelve (12) hours after revocation by GeoTrust. Relying parties must retrieve CRLs at least once every 24 hours before relying on a document signed using a CDS Certificate. Each CRL is signed by the issuing GeoTrust CA. The procedures for revocation are stated elsewhere in this CPS.

GeoTrust retains copies of all Certificates online for two years, 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 enrollment forms for CDS 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 (a) courts, law enforcement agencies or other third parties (including release in response to civil discovery) upon receipt of a court order or subpoena or upon the advice of GeoTrust's legal counsel, (b) law enforcement officials and others for the purpose of investigating suspected fraud, misrepresentation, unauthorized access, or potential illegal activity by the Subscriber in the opinion of GeoTrust, and (c) third parties as may be necessary for GeoTrust to fulfill its obligations under this Agreement. The foregoing confidentiality obligation shall not apply, however, to information appearing on CDS Certificates, information relating to CDS 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 CDS 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 CDS Certificates if in the reasonable opinion of GeoTrust such issuance or the continued use of such CDS Certificates would violate applicable laws and regulations.

### **III. OPERATIONAL REQUIREMENTS**

#### **A. Application Requirements**

##### **1. Organizations**

The following process is applicable to Applicants requesting CDS Certificates for use in his/her role on behalf of the Organization either on an individual basis or in connection with a Function.

##### **1.1 Enrollment of Organization and Registration of Initial Applicant**

Before any Applicant can request a CDS Certificate, the Organization must enroll in the service.

The Applicant, on behalf of the Organization, shall complete a GeoTrust CDS Certificate enrollment form as prescribed by GeoTrust. The enrollment form requires the Applicant to complete information regarding the Organization as well as information regarding the Applicant. All enrollment forms are subject to review, approval and acceptance by GeoTrust.

The Applicant must, at a minimum, provide the following Organization data on the enrollment form: Organization Name, Address, City/Locality, State/Province, Country, and, if applicable, Organization Representative name, Organization Representative Phone Number, and Organization Representative E-mail Address. The following data may also be required either on the enrollment form or in the LOA: Organization Unit and Dun & Bradstreet number (or similar third party verification). The Applicant is also required to provide the following: individual name and email address.

Each Applicant shall agree in the Subscriber Agreement to use the CDS Certificate in compliance with all applicable laws and regulations, including without limitation U.S. export laws and regulations.

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 authority of the Applicant to request a CDS Certificate or verify accuracy of the information contained in the Applicant's CDS Certificate request or otherwise check for errors and omissions.

GeoTrust will take reasonable steps to establish that the CDS Certificate request made on behalf of the Organization is legitimate and properly authorized. To prove that a CDS Certificate is duly authorized by the Organization, GeoTrust will require the Applicant to submit a letter of authorization ("LOA") on the Organization's letterhead that is signed by an Organization Representative and includes the following: Organization Representative's name and title, list of Applicants' names that will request a CDS Certificate, each Applicant's email address, work telephone number, and mobile phone number, and a statement that the Applicant(s) listed are member(s) of the Organization and are authorized to request a CDS Certificate. If the Applicant is requesting a CDS Certificate on behalf of a Function, then the LOA shall also identify the name of such Function and a statement that such Applicant is authorized to request a CDS Certificate on behalf of the Function. The Organization Representative may also include a statement that one or more of the Applicants is being designated by the Organization as the Registration Authority ("RA") for additional requests by Applicants for CDS Certificates and such RA has the authority to approve such requests. If the Organization Representative designates an RA, then the Organization Representative must also include the following information regarding the RA in the LOA name, title, telephone number, mobile phone number, and email address as well as the RA's signature. Before issuing a CDS Certificate to the RA, GeoTrust shall verify that the RA's email address matches the domain name of the Organization by accessing a third party database of domain names and their owners.

GeoTrust will not include an Organization Name in a CDS Certificate without first ensuring the following: (a) the Organizational Name appears in conjunction with a country and possibly a state or province of other locality to sufficiently identify its place of registration or a place where it is currently doing business; and (b) in the case of an organization or individual that could reasonably be expected to be registered with a local, state or national authority, in certain circumstances GeoTrust will obtain, view, and verify copies of the registration documents. For instance, GeoTrust may (w) verify the validity of the registration through the authority that issued it, or (x) verify the validity of the registration through a reputable third party database or other resource, or (y) verify the validity of the organization through a trusted third party, or (z) confirm that the organization exists if such organization is not the type that is typically registered or is capable of being verified under clause (y).

## **1.2 Registration of Other Applicants**

Applicants shall complete a GeoTrust enrollment form in addition to performing the steps below.

### **a. Organizations that have Designated an RA**

If the Organization has designated an RA, the RA will be responsible for approving authorized Applicants for CDS Certificates. RAs may approve CDS Certificate requests either via a Letter of Authorized Applicants ("LOAA") or a secure web-based or API session. If the RA is not using the web-based or API session then GeoTrust will require the Applicant to submit an LOAA on the Organization's letterhead that is signed by the RA and includes the following: RA's name and title, list of Applicants' names that will apply for CDS Certificates, each Applicant's email address, work telephone number, and mobile telephone number, and a statement that the Applicant(s) listed are member(s) of the Organization and are authorized to request a CDS Certificate. If the Applicant is requesting a CDS Certificate on behalf of a Function, then the LOAA shall also identify the name of such Function and a statement that such Applicant is authorized to request a CDS Certificate on behalf of the Function.

### **b. Organizations that do not Designate an RA**

If the Organization has not designated an RA, GeoTrust will refer to the LOA to determine whether the Applicant is duly authorized by the Organization to request a CDS Certificate. If the Applicant is not included on the LOA, GeoTrust will require the Applicant to submit an additional LOA which specifically identifies the Applicant.

## **2. Individuals**

The following process is applicable to Applicants requesting CDS Certificates for use in representing him or her self and not in connection with an Organization.

The Applicant shall complete a GeoTrust CDS Certificate enrollment form as prescribed by GeoTrust. The enrollment form requires the Applicant to complete information regarding him or herself. All enrollment forms are subject to review, approval and acceptance by GeoTrust.

The Applicant must, at a minimum, provide the following personal data on the enrollment form: Name, Address, City/Locality, State/Province, Country, and, if applicable, Phone Number, and E-mail Address.

Each Applicant shall agree in the Subscriber Agreement to use the CDS Certificate in compliance with all applicable laws and regulations, including without limitation U.S. export laws and regulations.

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 authority of the Applicant to request a CDS Certificate or verify accuracy of the information contained in the Applicant's CDS Certificate request or otherwise check for errors and omissions.

GeoTrust will take reasonable steps to establish that the CDS Certificate request made on behalf of the individual is legitimate. To prove that a CDS Certificate is requested by the individual, GeoTrust will require the Applicant to submit a fax copy of the an official form of government-issued photo identification ("Identification").

GeoTrust will not include an Individual Name in a CDS Certificate for an individual without first ensuring the individual's name, country and possibly a state or province or other locality provided on the enrollment form match that which is shown on the Identification. GeoTrust may also (a) verify the validity of the Identification through the authority that issued it, or (b) verify the validity of the Identification through a reputable third party database or other resource, or (c) verify the identity of the individual through a trusted third party.

## **B. Certificate Information**

Minimum CDS Certificate Profile

<b>X.509 v3 Certificate Attributes/ Extensions</b>	<b>Critical / Non Critical</b>	<b>Value / Notes</b>
<b>Attributes</b>		
Version		v3
SerialNumber		integer; unique to each certificate issued in the GeoTrust CA for Adobe PKI domain
Signature		sha-1 w/ RSAEncryption – {1.2.840.113549.1.1.5}
Issuer		cn=GeoTrust CA for Adobe, o=GeoTrust Inc. , c=US
Validity		<ul style="list-style-type: none"> <li>• Minimum = 1 day</li> <li>• Maximum = 10 years</li> </ul>
Subject		Based application information
SubjectPublicKeyInfo		<ul style="list-style-type: none"> <li>• rsaEncryption – {1.2.840.113549.1.1.1}</li> </ul> RSA public key is 2048 bit public key
<b>Extensions</b>		
AuthorityKeyIdentifier	Non-critical	contains a 20 byte SHA-1 hash of the SUB-Root CA public key
KeyUsage	Critical	Minimum Key Usages <ul style="list-style-type: none"> <li>• Digital Signature</li> <li>• Non-Repudiation</li> </ul>
SubjectKeyIdentifier	Non-critical	contains a 20 byte SHA-1 hash of the subjectPublicKey in this certificate
CertificatePolicies	Critical	1.2.840.113583.1.2.2 This certificate has been issued in accordance with the Acrobat Credentials CPS located at <a href="http://www.geotrust.com/resources/cps/pdfs/acrobat_cps.pdf">http://www.geotrust.com/resources/cps/pdfs/acrobat_cps.pdf</a>
ExtendedKeyUsage	Non-critical	1.2.840.113583.1.1.5
CRLDistributionPoints	Non-critical	<a href="http://crl.geotrust.com/crls/adobeca1.crl">http://crl.geotrust.com/crls/adobeca1.crl</a>

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

Subscribers will generate both the public and private keys on a cryptographic device. Subscribers will submit their Public Key to GeoTrust for certification electronically through the use of a web browser or other electronic means.

GeoTrust will process the Certificate enrollment forms to confirm the information on the CDS Certificates as discussed in III.A. above. However, GeoTrust reserves the right to waive such procedures and issue a CDS Certificate utilizing different authentication procedures in certain circumstances; provided that the general principles for verifying the application information are maintained. In addition, GeoTrust may use subcontractors or other third parties to assist in the performance of its operational requirements or any other obligation under this CPS. GeoTrust may delegate specific registration activities to a Registration Authority ("RA") provided that GeoTrust shall remain responsible for the services of its RA.

In addition, GeoTrust may waive its standard authentication procedures and the requirement that an Applicant utilize an Approved Hardware Device and issue CDS Certificates to Applicants, (including GeoTrust and authorized Adobe representatives) for testing purposes. A test CDS Certificate ("Test CDS Certificate") may be issued if (i) the GeoTrust administrator approves a request; and (ii) the CDS Certificate has the word "test" in the CDS Certificate's CN field. The Test CDS Certificate shall comply with the minimum test CDS Certificate Profile as shown below.

Minimum Test CDS Certificate Profile

X.509 v3 Certificate Attributes/ Extensions	Critical / Non Critical	Value / Notes
<b>Attributes</b>		
Version		v3
SerialNumber		integer; unique to each certificate issued in the GeoTrust CA for Adobe PKI domain
Signature		sha-1 w/ RSAEncryption – { 1.2.840.113549.1.1.5 }
Issuer		cn=GeoTrust CA for Adobe, o=GeoTrust Inc. , c=US
Validity		<ul style="list-style-type: none"> <li>• Minimum = 1 day</li> <li>• Maximum = 10 years</li> </ul>
Subject		Based application information
SubjectPublicKeyInfo		<ul style="list-style-type: none"> <li>• rsaEncryption – { 1.2.840.113549.1.1.1 }</li> </ul> RSA public key is 2048 bit public key
<b>Extensions</b>		
AuthorityKeyIdentifier	Non-critical	contains a 20 byte SHA-1 hash of the SUB-Root CA public key
KeyUsage	Critical	Minimum Key Usages <ul style="list-style-type: none"> <li>• Digital Signature</li> <li>• Non-Repudiation</li> </ul>
SubjectKeyIdentifier	Non-critical	contains a 20 byte SHA-1 hash of the subjectPublicKey in this certificate
CertificatePolicies	Critical	1.2.840.113583.1.2.2 This test certificate has been issued for the sole purpose of conducting quality assurance testing and should not be trusted or relied upon.
ExtendedKeyUsage	Non-critical	1.2.840.113583.1.1.5
CRLDistributionPoints	Non-critical	<a href="http://crl.geotrust.com/crls/adobeca1.crl">http://crl.geotrust.com/crls/adobeca1.crl</a>

#### D. Application Issues

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

#### E. Certificate Delivery

- (i) If GeoTrust finds that the Applicant's CDS Certificate enrollment form was sufficiently verified, then the Applicant's Certificate will be signed by GeoTrust. GeoTrust shall deliver the CDS Certificate as follows: GeoTrust will invoke the Applicant's web browser to generate a Public and Private Key Pair onto an Approved Hardware Device by limiting the available Cryptographic Service Provider ("CSP") drivers that enable an Applicant to generate a Key Pair; (ii) or, if approved by the Organization Representative, or authorized Registration Authority, the Subscriber may generate the Public and Private Key Pair with a FIPS 140-1 Level 3 cryptographic hardware module.

The Public Key material will be sent to GeoTrust for signing and the Applicant's CDS Certificate will be signed by GeoTrust and delivered back to the Applicant. The Applicant may utilize his/her own Approved Hardware Device or, if the Applicant does not already have one, the Applicant may purchase one from GeoTrust. If the Applicant purchases an Approved Hardware Device from GeoTrust then the Applicant shall have the option of requesting GeoTrust to generate a Public

and Private Key Pair onto the Approved Hardware Device at GeoTrust's facilities and deliver the Approved Hardware Device containing the Certificate to Subscriber. In such case, the Approved Hardware Device shall be delivered to the Subscriber by U.S. mail or other delivery service or by courier or other in-person delivery and may require signature for delivery. GeoTrust shall obtain and keep all receipts for delivery. In certain circumstances the delivery 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

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

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

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

Prior to the expiration of an existing Subscriber's CDS Certificate, it is necessary for the Subscriber to obtain a new CDS Certificate to maintain continuity of CDS Certificate usage. Subscribers must generate a new Key Pair to replace the expiring Key Pair (technically defined as "rekey") Rekeying will count as a new CDS Certificate request. The Subscriber must pay the fees and comply with the other terms and conditions for renewal as presented on GeoTrust's web site.

Expiring CDS Certificates are not revoked by GeoTrust upon issuance of the rekeyed CDS Certificate.

GeoTrust does not provide renewal services for CDS Certificates.

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

GeoTrust will attempt to notify all Subscribers of the expiration date of their CDS Certificate. Notification will generally be by e-mail message to the administrative, technical, and/or billing contacts listed in the enrollment form submitted by Subscriber, and will likely occur during the 90 days prior to the expiration date. If Subscriber's enrollment form 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 CDS Certificate.

GeoTrust shall revoke a CDS Certificate:

- Upon receipt of a request for revocation from the Adobe Policy Authority.
- Upon GeoTrust's determination that Subscriber has violated the Subscriber Agreement, failed to meet its material obligations under the Subscriber Agreement, any applicable CP or CPS, or any other agreement, regulation, or law applicable to the CDS Certificate that may be in force.
- Upon GeoTrust's knowledge or reasonable suspicion of Compromise of Subscriber's Private Key.

- If GeoTrust determines that any material fact contained in the CDS Certificate is no longer true including, without limitation, the fact that Subscriber is no longer authorized to represent the Organization.
- If GeoTrust determines that the CDS Certificate was not properly issued in accordance with the Agreement and/or any applicable CP or CPS.
- In the event that GeoTrust ceases operations and there is no plan for transition of GeoTrust's services to a successor or no plan to otherwise address such event, any Certificate issued to and all Certificates issued by the GeoTrust shall be revoked prior to the date that the GeoTrust ceases operations.

If GeoTrust initiates revocation of a CDS Certificate, GeoTrust shall notify the administrative and technical contact provided by Subscriber by e-mail message of the revocation and the reason(s) for the revocation. In the event that GeoTrust ceases operations, all CDS 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 CDS Certificate issued by GeoTrust are the Subscriber (including authorized representatives), GeoTrust and the Adobe Policy Authority.

## 3. Procedures 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 CDS 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 CDS Certificate was issued. The message will state that upon confirmation of the revocation request GeoTrust will revoke the CDS Certificate and that posting the revocation to the appropriate CRL will constitute notice to the Subscriber that the CDS 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 CDS 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 CDS Certificate and the subject's designated contacts. There is no grace period available to the Subscriber prior to revocation, and GeoTrust shall revoke such CDS 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 CDS Certificate; GeoTrust will send an e-mail message as soon as practicable to all Subscribers with CDS Certificates issued off the Private Key stating that the CDS 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 CDS Certificate has been revoked.

## **J. Certificate Suspension**

GeoTrust does not support Certificate suspension for the CDS Certificates.

## **K. Key Management**

GeoTrust may provide Private Key management for certain services that allow GeoTrust to sign and or deliver both Private and Public Keys on behalf of the Subscriber.

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

GeoTrust may provide Subscriber Key Pair generation or Subscriber private key protection for the CDS Certificates. Subscribers must use cryptographic hardware modules that (a) meet or exceed FIPS 140-1 Level 2 standards, or (b) for which the cryptographic hardware module manufacturer has applied for FIPS 140-1 Level 2 status within the previous year without receiving a notice of noncompliance or other communication indicating that such device fails to meet such standard (“Approved Hardware Device”).

## **M. Records Archival**

GeoTrust shall maintain and archive records relating to the issuance of the CDS Certificates for three (3) years following the issuance of the applicable CDS 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 CDS Certificates of Subscribers and subordinate CAs, if necessary,
- The payment of compensation (if necessary) to Subscribers whose unexpired, unrevoked CDS Certificates are revoked under the termination plan or provision, or alternatively, the issuance of replacement CDS 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 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 taken 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 offsite facility.

## **V. TECHNICAL SECURITY CONTROLS**

### **A. CA Key Pairs**

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.

CDS Certificates are issued off the GeoTrust Global CA, are generated in hardware, and are at least 2048 bit using the RSA generation algorithm. The cryptographic modules used for key generation and storage meet the requirements of FIPS 140-1 level 3. The GeoTrust Global CA private signature keys are backed up but not escrowed. The CA private key is maintained under m out of n multiperson control. The GeoTrust Global CA key may be used for Certificate signing (code signing) Client Authentication, CRL signing, and off-line CRL signing. GeoTrust makes the CA Certificates 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 CDS 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 GeoTrust Global CA Public and Private Keys is through June 21, 2020, 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 Equifax Secure Certificate Authority 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](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 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**

Generation of Subscriber Key Pairs will be performed in accordance with Section III.E. of this CPS.

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 - 10 days
2. Issue a Certificate - 10 days
3. Publish a CRL - 48 hours
4. Audit Vetting Procedures - 2 months

Backup copies of essential business and CA information are made routinely. In general, backups are performed daily on-site, weekly to an off-site location, and monthly to GeoTrust's disaster recovery site, but may be performed less frequently in GeoTrust's discretion according to production schedule requirements. 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)  
[kipolicy@geotrust.com](mailto:pkipolicy@geotrust.com)

GeoTrust does not support a Certificate Policy (CP) for Acrobat Credentials CDS 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.  
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 past and current CPS and any amendments thereto are available through <http://www.geotrust.com/resources>. Amendments to this CPS will be evidenced by a new version number and date, except where the amendments are purely clerical.

### **VIII. DEFINITIONS**

**Adobe.** Adobe Systems Incorporated.

**Adobe Policy Authority.** Selected members of Adobe's management that define, review and approve policies related to the Adobe PKI.

**Adobe Root CA.** Adobe's root Certification Authority.

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

**CA.** Certification Authority.

**CDS.** Certified Document Services.

**CDS Certificate.** A signing certificate issued by GeoTrust for the purposes of digitally signing Acrobat documents.

**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.

**Certified Document Services Certificate Policy ("CDS CP").** The policy published and managed by Adobe Systems Incorporated that governs all third parties providing CA services for CDS.

**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 a Certificate.

**CRL.** See Certificate Revocation List.

**Extension.** 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.

**Function.** An organizational unit or department within an Organization

**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 typically begins on the date the Certificate is issued (or such later date as specified in the Certificate), and ends on the date and time it expires as noted in the Certificate or is earlier revoked unless it is suspended.

**Organization.** A legally recognized company, enterprise or governmental agency that has applied for or has been issued CDS Certificates.

**Organization Representative.** A representative of the Organization with the authority to contractually bind the Organization.

**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.

**Registration Authority or RA.** A representative designated by the Organization to review and approve requests for CDS Certificates.

**Supported Platform.** Those applications specified on the CDS information webpage, currently located on [http://adobe.com/security/partners\\_cds.html](http://adobe.com/security/partners_cds.html).

**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 2004, GeoTrust, Inc.

[v. 1.2 4-16-04]