True Credentials® for Code Signing Certificate Practice Statement

TABLE of CONTENTS

I. INTRODUCTION

A. Overview

This GeoTrust Certificate Practice Statement (the "CPS") presents the principles and procedures GeoTrust employs in the issuance and life cycle management of
True Credentials for Code Signing Certificates. This CPS also presents the principles and procedures GeoTrust as a means of delivering GeoTrust True Credentials for Code Signing Certificates to organizations that have enrolled in the service. 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 Publisher Certificates and Code Confirmation Certificates (“Certificates”)

1. Publisher Certificates

Publisher Certificates are X.509 Certificates with Code Signing and Client Authentication Extensions that chain to the GeoTrust Global CA trusted root. These Certificates facilitate secure delivery of electronic documents by providing limited authentication of a Publisher's electronic documents or code between a Relying Party's Microsoft Windows Smartphone and the Publisher's electronic documents or code. Additionally, these Certificates may be associated with the ability to resign code with another trusted CA.

2. Code Confirmation Certificates

Code Confirmation Certificates are X.509 Certificates with Code Signing that chain to the GeoTrust Windows Powered Mobile Device CA 1 root or the GeoTrust Windows Powered Mobile Device CA 2 root. The Certificates issued in order for GeoTrust to use the associated Private Key to digitally resign Microsoft Smartphone application code which has been digitally signed by a Publisher Certificate Private Key, upon request of code confirmation from the Publisher.

3. Operational Period of Publisher Certificates

Publisher Certificates have an Operational Period of 379 days, 744 days, or 1,109 days from the date of issuance (depending on whether the Publisher has purchased a one year, two year, or three 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. Additionally, these Certificates may be associated with a resigning service, if so, then a preset number of resignings will be associated with this offering.

4. Operational Period of Code Confirmation Certificates

Code Confirmation Certificates have an Operational Period of ten (10) years from the date of issuance, unless the Code Confirmation Certificate is revoked prior to the expiration of the Code Confirmation Certificate's Operational Period.

5. Installation of Certificates:

Certificates may not be installed on more than one client or cryptographic token at a time.

6. Technical Requirements of Certificates

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

II. GENERAL PROVISIONS

A. Obligations

1. GeoTrust Obligations

GeoTrust will: (i) issue Certificates in accordance with this CPS; (ii) perform limited authentication of Publishers 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. Publisher Obligations

Publisher will submit truthful information about itself and its business entity, as applicable. Publishers will not install a Certificate on more than one client or cryptographic device. Publishers will at all times abide by this CPS and a Publisher will immediately request revocation of a Certificate if the related Private Key is Compromised. The Publisher will only use the GeoTrust True Credentials for Code Signing Certificates for purposes of initiating an SSL v.3 client authenticated session or form signing code. The Publisher 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 True Credentials for Code Signing 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 Publishers 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 replace a True Credentials for Code Signing Certificates upon request by the Publisher within seven days of issuance or renewal of a True Credentials for Code Signing Certificates if the certificates or cryptographic token is loss in delivery or defective. 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 Publisher has paid the fees for the Certificate to another party such as a reseller, the Publisher 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, PUBLISHER OR ANY RELYING PARTY THAT (A) THE PUBLISHER TO WHICH IT HAS ISSUED A CERTIFICATE IS IN THE FACT THE PERSON, ENTITY OR ORGANIZATION IT CLAIMS TO HAVE BEEN (B) A PUBLISHER 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 PUBLISHER AND/OR RELYING PARTY OF ANY TRANSACTION ENTERED INTO BY THE PUBLISHER AND/OR RELYING PARTY INVOLVING THE USE OF OR RELIANCE UPON A CERTIFICATE. GEOTRUST SHALL NOT HAVE ANY OTHER OBLIGATIONS WITH RESPECT TO THE QUALITY OF THE CODE SIGNED BY A CODE CONFIRMATION CERTIFICATE. THE SIGNATURE OF BY A PRUBLISHER CERTIFICATE OR RE-SIGNATURE OF CODE BY GEOTRUST SHALL NOT UNDER ANY CIRCUMSTANCES BE CONSTRUED AS A WARRANTY OR REPRESENTATION AS TO THE FUNCTIONING, SUITABILITY, MERCHANTABILITY, PRESENCE OR ABSENCE OF DEFECTS, OR ANY OTHER MATTER PERTAINING TO OR ARISING FROM SUCH CODE WHICH IS NOT EXPLICITLY WITHIN THE SCOPE OF THE ABOVE WARRANTIES

IT IS UNDERSTOOD AND AGREED UPON BY PUBLISHERS 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 PUBLISHERS AND RELYING PARTIES AGREE AND ACKNOWLEDGE THAT CERTIFICATES HAVE A LIMITED OPERATIONAL PERIOD AND MAY BE REVOKED AT ANY TIME. PUBLISHERS 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 PUBLISHERS 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, Publishers and Relying Parties agreea nd 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, Publishers 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, Publishers 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, PUBLISHER 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 THOUSAND U.S. DOLLARS ($50,000.00).

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 PUBLISHER 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, PUBLISHERAND/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-BYCERTIFICATE 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, Publishers, 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 Publisher 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, Publishers and Relying Parties.

In no event shall GeoTrust be liable to the Applicant, Publisher, 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 Publisher and the relationship between GeoTrust and the Applicant and the Publisher 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 Publisher has any authority to bind GeoTrust by contract or otherwise, to any obligation.

2. Indemnification by Applicant and Publisher

Unless otherwise set forth in this CPS and/or Publisher Agreement, Applicant and Publisher, 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 Publisher 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 Publisher 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 Publisher 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 Publisher 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 Publisher (including the Publisher 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 Publisher has with GeoTrust with respect to a Certificate, including but not limited to a Publisher Agreement, such other agreement shall take precedence.

4. Severability

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

I. Repository and CRL

With regard to GeoTrust True Credentials for Code Signing Certificates, GeoTrust shall operate a CRL that will be available to both Publishers and Relying Parties. GeoTrust shall post the updates to 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 Certificate will be published no later than twelve (12) hours after revocation by GeoTrust. 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 Publisher Information

Information regarding Publishers 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 Publisher. 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 Publisher 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 Certificates, information relating to Certificate revocation, or to information regarding Publishers that is already in the possession of or separately acquired by GeoTrust. In addition, GeoTrust will release information regarding a Publisher upon request submitted by the Publisher in form satisfactory to GeoTrust.

2. Aggregate Publisher Information

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

Publishers 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 Publisher Certificate shall complete a GeoTrust Publisher 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 an Organization or Individual Name within the Certificate application and an Organization will also appear on the Publisher Certificate. A Publisher Certificate may contain additional information as well. GeoTrust does not verify the authority of the Publisher to request a Publisher 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 Publisher’s Certificate request or otherwise check for errors and omissions.

B. Certificate Information

1. Organizational Name

If a Publisher Certificate contains an Organizational Name, GeoTrust will take reasonable steps to establish that a Publisher Certificate request made on behalf of that organization is legitimate and properly authorized. GeoTrust will not include an Organizational Name in a Publisher 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).

In addition, to prove that a Publisher Certificate is duly authorized by the organization, GeoTrust will typically request the name of a contact person who is employed by or is an officer of the organization. GeoTrust will also typically require a form of authorization from the organization confirming its intent to obtain a Publisher Certificate and will usually document the organization's contact person. GeoTrust normally confirms the contents of this authorization with the listed contact person.

C. Procedure for Processing Certificate Applications

Publishers submit their Public Key to GeoTrust for certification electronically through the use of a web browser or both the Public and Private Keys may be centrally generated and/or delivered via a web browser or on a cryptographic device by to the Publisher. As a minimum, the Publisher must provide the following data: Common Name, Organization, Location, Country, and the names, e-mail addresses, and telephone numbers for the Administrative, Technical, Support, and Billing points of contact.

For Publisher Certificates, GeoTrust will process the Certificate Applications to confirm the information on the Publisher Certificates as discussed above. However, GeoTrust reserves the right to waive such procedures and issue a Publisher Certificate utilizing different authentication procedures in certain circumstances; provided that the general principles for verifying the application information is 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.

D. Application Issues

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

E. Certificate Delivery

If GeoTrust finds that the Applicant's Publisher Certificate application was sufficiently verified, then the Applicant's Certificate will be signed by GeoTrust. Upon signing the Applicant's Publisher Certificate, Publisher smart cards shall be delivered to the Publisher by U.S. certified mail or other delivery service requiring signature for delivery, or by courier or messenger or other in-person delivery requiring signature for delivery. GeoTrust shall obtain and keep all receipts for delivery. In the alternative, GeoTrust may establish an alternative procedure to document that Publisher Private Keys were generated on Publisher smart cards and delivered to Publisher, including, but

not limited to, contractually requiring Publisher to download and store Publisher Private Keys on a smart card and provided such use and delivery procedure is of equal or greater reliability to show proof of receipt and confidentiality. The information will typically be sent to the administrative contact and/or the technical contact designated by the Publisher, and will include the date the Publisher Certificate was issued, the date the Publisher Certificate will expire, and the type of Publisher Certificate that was issued. Notification will not be sent to others than the subject of the Publisher Certificate and the subject's designated contacts. 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/Publishers.

F. Certificate Acceptance

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

G. Certificate Renewal and Rekey

Prior to the expiration of an existing Publisher's Certificate, it is necessary for the Publisher to obtain a new certificate to maintain continuity of Certificate usage. Publishers have the option of generating a new Key Pair to replacing 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 Publisher's application and /or key generation tools. Rekeying will count as a new certificate request. So long as the request for a renewal Certificate is presented to GeoTrust within the period running from 90 days prior to expiration of an existing Certificate to 90 days after expiration, GeoTrust will provide a renewal Certificate to a Publisher upon presentation of a CSR for an existing Key Pair so long as the Publisher's Distinguish Name (DN) remains the same as on the Publisher's previous order. The Publisher must pay the fees and comply with the other terms and conditions for renewal as presented on GeoTrust's Web site.

At GeoTrust's discretion, Renewal Certificates may be subject to the same authentication steps outlined in this CPS as apply to initial issuance of a Certificate. Expiring Certificates are not revoked by GeoTrust upon issuance of the renewal Certificate.

H. Certificate Expiration

GeoTrust will attempt to notify all Publishers 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 Publisher, and will likely occur during the 90 days prior to the expiration date. If Publisher's application was submitted by another party on Publisher'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. Required Revocation of Publisher Certificates

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

Upon request of the Publisher to GeoTrust in writing or by electronic means provided by GeoTrust.

Upon GeoTrust's determination that Publisher has failed to meet its material obligations under the Publisher Agreement, any applicable CP or CPS, or any other agreement, regulation, or law applicable to the Certificate that may be in force.

If Microsoft reasonably determines that certificate is being used in a manner that compromises the trust status of Smartphone Applications.

Upon GeoTrust's knowledge or reasonable suspicion of compromise of the private key.

If GeoTrust determines that any material fact contained in the certificate is no longer true.

If GeoTrust determines that the Certificate was not properly issued in accordance with the Agreement and/or any applicable CP or CPS.

b. Required Revocation of Code Confirmation Certificates:

GeoTrust shall revoke Code Confirmation Certificates:

If Microsoft reasonably determines that certificate is being used in a manner that compromises the trust status of Microsoft Smartphone applications.

Upon request by Publisher to GeoTrust in writing or other electronic means provided by GeoTrust.

If the GeoTrust determines that any material information contained in the certificate is no longer true.

If the GeoTrust determines that the certificate was not properly issued in accordance with this Agreement and any applicable CP or CPS.

If the GeoTrust determines that the private key associated with the certificate is, or that it suspects it has been, compromised.

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 Certificate, GeoTrust shall notify the administrative and technical contact provided by Publisher 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 Publisher 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 Publisher (including designated representatives) and GeoTrust and Microsoft.

3. Procedure For Revocation Request

Publisher 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 Publisher 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 Publisher 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 Publisher prior to revocation, and GeoTrust shall revoke such Certificate within the next business day and post the revocation to the next published CRL. For the Enterprise SSL service, the Publisher's Certificate Administrator may revoke a Certificate issued by GeoTrust without notice to GeoTrust. 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 Publishers 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 Publisher that the Certificate has been revoked.

J. Certificate Suspension

GeoTrust does not support Certificate suspension for the 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 Publisher.

L. Publisher Key Pair Generation

GeoTrust may provide Publisher Key Pair generation or Publisher 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 Publishers, 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 Publishers and Relying Parties. Such termination plans may address the following, as applicable:

- Provision of notice to parties affected by the termination, such as Publishers 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 Publisher and customer support services,
- The continuation of revocation services, such as the issuance of CRLs,
- The revocation of unexpired unrevoked Certificates of end-user Publishers and

subordinate CAs, if necessary,
- The payment of compensation (if necessary) to Publishers 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 Publishers and Relying Parties, the Registered Agent for GeoTrust, Inc., a Delaware corporation, shall be the custodian.

IV. PHYSICAL SECURITY CONTROLS

A. Site Location and Construction

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

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

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

B. Physical Access Controls

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

C. Power and Air Conditioning

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

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

D. Water Exposures

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

E. Fire Prevention and Protection

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

F. Media Storage

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

G. Waste Disposal

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed or zeroized in accordance 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 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.

1. Publisher 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 140-2 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 Publishers 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 Publisher 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 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 Publishers 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.

2. Code Confirmation Certificates are issued off either the GeoTrust Windows Powered Mobile Device CA 1 or the GeoTrust Windows Powered Mobile Device CA 2, 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. Both the GeoTrust Windows Powered Mobile Device CA 1 and the GeoTrust Windows Powered Mobile Device CA 2 private signature keys are backed up but not escrowed. The CA private key is maintained under m out of n multiperson control. Both the GeoTrust Windows Powered Mobile Device CA 1 and the GeoTrust Windows Powered Mobile Device CA 2 key may be used for Certificate signing (code signing), CRL signing, and off-line CRL signing.
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 Publisher upon Certificate issuance.

The usage period or active lifetime for both the GeoTrust Windows Powered Mobile Device CA 1 and the GeoTrust Windows Powered Mobile Device CA 2 Public and Private Keys is through April 1, 2022. Both the GeoTrust Windows Powered Mobile Device CA 1 and the GeoTrust Windows Powered Mobile Device CA 2 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), GeoTrust shall promptly notify all Publishers 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. Code Confirmation Certificates may be renewed as long as the cumulative certified lifetime of the Code Confirmation 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. Publisher Key Pairs

Generation of end-user Publisher 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 Publisher - 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, back-ups are performed daily on-site, weekly to an off-site location, and monthly to GeoTrust's disaster recovery site, but may be performed less frequently in GeoTrust's discretion according to production schedule requirements.. 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 Publishers 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 Publisher. GeoTrust does not apply any specific Certificate Policy Object Identifier(s), but instead refers to the applicable CPS version and URL address. The policy constraints extensions and policy qualifiers syntax and semantics, when used, conform to the RFC 2459 standards.

B. CRL Profile

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

VII. CPS ADMINISTRATION

A. CPS Authority

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

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

GeoTrust does not support a Certificate Policy (CP) for True Credentials for Code Signing Certificates.

B. Contact Person

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

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

C. CPS Change Procedures

This CPS (and all amendments to this CPS) is subject to approval by the PKI Policy Authority. GeoTrust may change this CPS at any time without prior notice. The 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

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

CA. Certification Authority.

Certificate. A record that, at a minimum: (a) identifies the CA issuing it; (b) names or otherwise identifies its Publisher; (c) contains a Public Key that corresponds to a Private Key under the control of the Publisher; (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 Administrator. An individual designated by the Publisher to submit Publisher domain names for vetting by GeoTrust and to approve the issuance of Certificates for the vetted domain names on behalf of Publisher as part of GeoTrust's Enterprise SSL™ service.

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.

Code Confirmation Certificate. A Certificate issued by GeoTrust in order for GeoTrust to use the associated Private Key to digitally resign Microsoft Smartphone application code which has been digitally signed by a Publisher Certificate Private Key, upon request of code confirmation from the Publisher.

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. 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.

Publisher Certificate. A Certificate issued by GeoTrust for software vendors who wish to use their associated Private Key to digitally sign code for a Microsoft Smartphone application.

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.

Publisher. 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 Publisher.

[v. 1.1 11-17-04]