DigiCert

Certification Practices Statement for GeoTrust and RapidSSL

Version 1.5

Effective Date: April 18, 2019

DigiCert Certification Practices Statement for GeoTrust and RapidSSL

Revision date: April 18, 2019

Trademark Notices

Table of Contents

Change History Table

Version	Description of Changes
1.1	Miscellaneous clerical and administrative changes.
1.1.1	Updated maximum validity period from one year to thirteen months; Miscellaneous clerical and administrative changes.
1.1.2	Manual verification updated through e-mail.
1.1.3	Updates to key sizes throughout the document.
1.1.4	General updates from Verisign to Symantec.
1.1.5	Added RapidSSL, RapidSSL Wildcard & RapidSSL Enterprise certificates throughout; New certificate information provided for renewal certificates are subject to the same I&A as initial certificate requests; Certificate shall not be installed on more than a single server unless agreed at enrolment & fees have been paid; Removed description of GeoTrust as "a Delaware corporation"; Subscriber shall immediately request revocation if the private key is compromised; Removed the 2010 deadline for 2048 migration as the migration is now completed;
1.1.6	Added FreeSSL Server certificates throughout; Removed authentication of the ownership of IP address.
1.1.7	Revisions to Sections 1.3.1 & 1.4.2 - Compliance with the Mozilla Root program;
1.1.8	Miscellaneous clerical and administrative changes, All updates reflecting compliance with CABF Requirements for DV and OV certificates, Effective July 1, 2012. (See PWG Approval Mapping Matrix for GeoTrust CPS).
1.1.9	All updates reflecting compliance with CABF Requirements for EV Code Signing Certificates, v1.4.; Miscellaneous clerical and administrative changes.
1.1.10	Addition of 2048 DSA CA hierarchies
1.1.11	Re-alignment with CABF EV v1.4 Guidelines; .
1.1.12	Addition of new Roots; Addition of Mozilla IDN Verification requirements
1.1.13	Identified conformity to CABF Baseline Requirements; Added clarity regarding subscriber certificates under 2048bit will have EKU without server auth flag and designated OID; Added clarity regarding subscriber certificates under 2048bit will have EKU without server auth flag and designated OID.
1.1.14	Replaced 'privacy policy' with 'Privacy Statement'; updated references to the externally facing CABF URLs to the websites with the updated policies.
1.1.15	Added language to specifically include Certificate Authority Authorization (CA)
1.1.16	Added CABF references.
1.1.17	Removed fax number.
1.1.18	Changed record retention.
1.1.19	Miscellaneous clerical and administrative changes; GeoTrust provides Relying Parties with information on how to find the

	appropriate repository to check Certificate status and, if OCSP (Online Certificate Status Protocol) is available, how to find the right OCSP responder; Removed reference to 1024-bit keys; Modified text to state that key usage criticality is generally set to TRUE;
1.1.20	Miscellaneous clerical and administrative changes.
1.1.21	Miscellaneous clerical and administrative changes; Removed aged reference to internal server name and reserved IP address deprecation; EV certificates use the applicable CABF policy OIDs; Removed aged reference to internal server name and reserved IP address deprecation; Removed list of 6 methods, updated the method numbers of the most commonly used methods, Appended technical support exclusion to "customer service personnel, with the exception of technical support analysts" Appended CAA results to "Documentation supporting certificate applications, including CAA results…" Changed repeat of background checks to 10 years. Changed self-signed root certificate maximum validity to 25 years; Updated FIPS 140-1 references to FIPS 140-2; Added CA EKU constraint language; Added RFC 6960 support disclaimer
1.2	Revisions completed to rebrand the product from Symantec to DigiCert. Other various clerical and administrative changes made throughout the document.
1.3	Changes made throughout the document to meet the updates on the DigiCert CP/CPS v.4.16 changes including: Removed frequent password changing practice from section 6.4.1 to comply with NIST Special Publication 800-63-3: Digital Authentication Guidelines. Added sections 1.5.2.1 for Revocation Reporting Contact Person and additions/revisions to section 4.9 to meet the revocation requirements for CABF ballot SC6.
1.4	Modified section 3 to include footnote describing the CABF SC7 ballot changes for IP address validation are handled in the DigiCert CP and CPS. Editorial changes to address grammar issues throughout the document. Modified section 4.10.2 to make the SLA reference more accurate. Changed "Issuer CA" to "Issuing CA" instances within the document to reflect the defined term.
1.5	Edited sections 3.1.6, 3.2.1, and 6.1.3 to clarify naming and proof-of-possession requirements.

1. INTRODUCTION

This document is the DigiCert Certification Practices Statement for GeoTrust and RapidSSL ("CPS"). It states the practices that DigiCert's GeoTrust certification authorities ("CAs") employ in providing certification services that include, but are not limited to, issuing, managing, revoking, and renewing certificates. This document contains both the requirements of a Certificate Policy and a Certificate Practice Statement. DigiCert's GeoTrust PKI operates as a single, independent PKI with a single CPS. This document should not be considered subordinate to other DigiCert Certificate Policies.

1.1 Overview

This Certificate Practice Statement (the "CPS") presents the principles and procedures employed in the issuance and life cycle management of DigiCert-issued, GeoTrust or RapidSSL branded digital certificates. This CPS and any and all amendments thereto are incorporated by reference into GeoTrust and RapidSSL-branded Certificates under this CPS.

Internet service providers, hosting companies, or other businesses ("Partners") may perform some functions relating to the issuance of Certificates on behalf of Subscribers other than domain or IP address validation (e.g., the gathering of Subscriber information, generating and forwarding of a Certificate Signing Request, or installation and use of a Certificate following issuance). In such event, the processes and procedures stated in this CPS will be applied to the Partners as if they were the Subscribers as closely as practicable.

This GeoTrust CPS conforms to the Internet Engineering Task Force (IETF) RFC 3647 for Certificate Policy and Certification Practice Statement construction. GeoTrust CAs conform to the current version of the CA/Browser Forum (CABF) requirements including:
- Guidelines for the Issuance and Management of Extended Validation (EV) Certificates,
- Guidelines for the Issuance and Management of Extended Validation (EV) Code-Signing Certificates, and,
- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates,

published at *www.cabforum.org*. In the event of any inconsistency between this document and those Requirement, those Requirements take precedence over this document.

At this time, DigiCert's Extended Validation (EV) SSL certificates, Extended Validation (EV) Code-Signing certificates and Domain-validated (DV), Individual-validated (IV) and Organization-validated (OV) SSL certificates issued by GeoTrust CAs under this CPS conform with the CABF Requirements. Such DV and OV certificates are issued containing the corresponding policy identifier(s) specified in section 1.2 indicating adherence to and conformance with these requirements. GeoTrust CAs shall also assert that all Certificates issued containing these policy identifier(s) are issued and managed in conformance with the CABF Requirements.

Effective February 1, 2017 and after, DigiCert adopts the current version of the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates published at https://aka.ms/csbr. If there is any inconsistency between this document and those Requirements, those Requirements take precedence over this document. Code signing certificates issued on or after February 1st, 2017 and intended for use in Microsoft Authenticode and subsequent technologies will include the applicable certificate policy identifier, 2.23.140.1.4.1, to indicate compliance with the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates.

Management may make exceptions to this policy on a case by case basis to mitigate material, imminent impacts to customers, partners, relying parties, and/or others within the certificate ecosystem where practical workarounds do not exist. Any such management exceptions are documented, tracked, and reported as part of the audit process.

DigiCert shall not issue SSL inspection intermediate CAs from publicly-trusted GeoTrust roots. Only roots with no current or previous trust in Application Software Supplier products (private roots) may be used to create intermediate CAs used for SSL inspection.

DigiCert discloses all Cross Certificates that identify the GeoTrust Root CA as the Subject in an established trust relationship.

1.2 Document Name and Identification

This document is the DigiCert Certification Practice Statement for GeoTrust and RapidSSL. The object identifier (OID) values corresponding to GeoTrust are as follows:

GeoTrust Certificate Policy for Extended Validation (EV) certificates: 1.3.6.1.4.1.14370.1.6
GeoTrust Certificate Policy certificates (non-EV): 1.3.6.1.4.1.14370.1.7

Prior to acquisition of the Website Security business unit by DigiCert, Symantec assigned a reserved OID value for asserting conformance with the current version of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates. This OID value is reserved for use by any brand of Symantec CA as a means of asserting compliance with these CABF Requirements and as such does not distinguish a particular brand or class of Certificate.

The Symantec Reserved Certificate Policy identifier:
Symantec/id-CABF-OVandDVvalidation: 2.16.840.1.113733.1.7.54

All OV certificates issued on or after March 5th, 2015 include the applicable CABF policy OID:

- CABF OID for OV certificates: 2.23.140.1.2.2

All DV certificates issued on or after April 28th, 2015 include the applicable CABF policy OID:

- CABF OID for DV certificates: 2.23.140.1.2.1

All IV certificates issued on or after December 1, 2016 include the applicable CABF policy OID:

- CABF OID for IV certificates: 2.23.140.1.2.3

EV certificates use the applicable CABF policy OIDs:

- SSL/TLS certificates: 2.23.140.1.1
- Code Signing certificates: 2.23.140.1.3

Code signing certificates issued on or after February 1st, 2017 will include the applicable certificate policy identifier, 2.23.140.1.4.1, to indicate compliance with the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates.

1.3 PKI Participants

1.3.1 Certification Authorities

The term Certification Authority (CA) is a trusted third-party entity that issues Certificates and performs all of the functions associated with issuing such Certificates under this CPS. GeoTrust Root CAs also issue certificates to subordinate CAs, including CAs owned by third parties. All such subordinate CAs are required to operate in conformance with this CPS.

1.3.2 Registration Authorities

A Registration Authority is an entity that performs identification and authentication of certificate applicants for end-user certificates, initiates or passes along revocation requests for certificates for end-user certificates, and approves applications for renewal or re-keying of certificates on behalf of a GeoTrust CA. DigiCert may act as an RA for certificates it issues. DigiCert does not delegate domain or IP address validation to external RAs or third parties for the issuing CAs it operates.

Third parties, who enter into a contractual relationship with DigiCert, may operate their own RA and authorize the issuance of certificates by a GeoTrust CA. Third party RAs must abide by all the requirements of the DigiCert CPS for GeoTrust and the terms of their agreement with DigiCert. RAs may, however implement more restrictive practices based on their internal requirements. Under the GeoRoot subordinate CA program, which is subject to the same WebTrust audits as DigiCert-operated CAs, organizations operate subordinate CAs that gain trust from GeoTrust roots and perform validation for certificates they issue solely for their own consumption. GeoRoot customers are responsible for their own audits covering the scope of their publicly trusted PKI.

1.3.3 Subscribers

Subscribers include all end users (including entities) of certificates issued by a GeoTrust CA. A subscriber is the entity named as the end-user Subscriber of a certificate. End-user Subscribers may be individuals, organizations or, infrastructure components such as firewalls, routers, trusted servers or other devices used to secure communications within an Organization.

CAs are technically also subscribers of GeoTrust certificates either as a CA issuing a self-signed Certificate to itself, or as a CA issued a Certificate by a superior CA. References to "end entities" and "subscribers" in this CPS, however, apply only to end-user Subscribers.

1.3.4 Relying Parties

A Relying Party is an individual or entity that acts in reliance of a certificate and/or a digital signature issued by a GeoTrust CA. A Relying Party may, or may not also be a Subscriber of GeoTrust certificates.

1.3.5 Other Participants

No Stipulation

1.4 Certificate Usage

1.4.1 Appropriate Certificate Usages

GeoTrust Certificates are X.509 Certificates with TLS Extensions, Code Signing and/or Client Authentication Extensions (as appropriate) that chain to a GeoTrust Trusted Root.

GeoTrust **SSL Certificates** facilitate secure electronic commerce by providing limited authentication of a Subscriber's server and permitting SSL/TLS encrypted transactions between a Relying Party's browser and the Subscriber's server. DigiCert may issue Wildcard Certificates, which are X.509 Certificates with TLS Extensions that are vetted to a specified level domain and may be used in connection with all next level higher domains that contain the specified vetted level domain. In addition, DigiCert may also enable the Certificate for use as a client Certificate.

GeoTrust **Publisher Certificates** may only be used for the purposes of (i) identification of the Publisher as the party accessing the code signing portal, and (ii) locally signing the code for subsequent resigning by the appropriate Code Confirmation certificate.

GeoTrust **Code Confirmation** Certificates allow DigiCert to use the associated Private Key to digitally resign application code which has been digitally signed by a Publisher Certificate Private Key, upon request of code confirmation from the Publisher.

GeoTrust **My Credential**™ client Certificates are X.509 Certificates with S/MIME Extensions which facilitate secure electronic commerce by providing limited authentication of a Subscriber's client and permitting secure VPN access and S/MIME communications between a Relying Party and the Subscriber's client.

True Credentials® and **True Credential Express** Client Certificates are X.509 Certificates with S/MIME Extensions which facilitate secure electronic commerce by providing limited authentication of a Subscriber's client and permitting TLS Client Authentication, secure VPN access and S/MIME communications between a Relying Party and the Subscriber's client, and in some instances may also be used for code signing and document signing.

RapidSSL, RapidSSL Wildcard and **RapidSSL Enterprise** Certificates are X.509 Certificates with SSL Extensions that chain to the GeoTrust trusted root(s). RapidSSL certificates facilitate secure electronic commerce by providing limited authentication of a Subscriber's server and SSL encrypted transactions between a Relying Party's browser and the Subscriber's server. In addition, DigiCert may also enable the Certificate for use as a client Certificate.

RapidSSL Wildcard Certificates are vetted to a specified level domain and may be used in connection with all next level higher domains that contain the specified vetted level domain.

The **RapidSSL Enterprise** Certificate is intended for use only within the enterprise intranet. RapidSSL Enterprise Certificates are only available to Symantec Managed PKI for SSL customers.

Note that the use of Certificates with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Name has been deprecated by the CA / Browser Forum and was eliminated October 2016.

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

1.4.2 Prohibited Certificate Uses

The GeoTrust Root CAs and CAs subordinate to those CAs shall not issue any certificate that can be used for man-in-the-middle (MITM) or traffic management of domain names or IPs that the certificate holder does not legitimately own or control. Such certificate usage is expressly prohibited.

Certificates shall be used only to the extent the use is consistent with applicable law, and in particular shall be used only to the extent permitted by applicable export or import laws.

GeoTrust Certificates are not designed, intended, or authorized for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage. Client Certificates are intended for client applications and shall not be used as server or organizational Certificates.

DigiCert periodically rekeys Intermediate CAs. Third party applications or platforms that have an Intermediate CA embedded as a root certificate may not operate as designed after the Intermediate CA has been rekeyed. DigiCert therefore does not warrant the use of Intermediate CAs as root certificates and recommends that Intermediate CAs not be embedded into applications and/or platforms as root certificates.

1.5 Policy Administration

1.5.1 Organization Administering the Document

This CPS and the documents referenced herein are maintained by the DigiCert Policy Authority (DCPA), which can be contacted at:

DigiCert Policy Authority
Suite 500
2801 N. Thanksgiving Way
Lehi, UT 84043 USA
Tel: 1-801-701-9600
Fax: 1-801-705-0481
www.digicert.com
support@digicert.com

1.5.2 Contact Person

Attn: Legal Counsel
DigiCert Policy Authority
Suite 500
2801 N. Thanksgiving Way
Lehi, UT 84043 USA
www.digicert.com
support@digicert.com

Contact information for the CA/Browser Forum is available here: https://cabforum.org/leadership/

1.5.2.1 Revocation Reporting Contact Person

Attn: Support
DigiCert Technical Support
Suite 500
2801 N. Thanksgiving Way
Lehi, UT 84043 USA
https://www.digicert.com/certificate-revocation.htm

To request that a Certificate be revoked, please email revoke@digicert.com.

Entities submitting certificate revocation requests must list their identity and explain the reason for requesting revocation. DigiCert or an RA will authenticate and log each revocation request according to Section 4.9 of the DigiCert CP and this CPS. DigiCert will always revoke a Certificate if the request is authenticated as originating from the Subscriber or the Affiliated Organization listed in the Certificate. If revocation is requested by someone other than an authorized representative of the Subscriber or Affiliated Organization, DigiCert or an RA will investigate the alleged basis for the revocation request prior to taking action in accordance with Section 4.9.1 and 4.9.3.

1.5.3 CPS Approval Procedure

This CPS (and all amendments to this CPS) is subject to approval by DigiCert. DigiCert may change this CPS at any time without prior notice. The CPS and any amendments thereto are available through https://www.digicert.com/legal-repository. Amendments to this CPS will be evidenced by a new version number and date, except where the amendments are purely clerical.

1.6 Definitions and Acronyms

See Appendix A for a table of acronyms and definitions

2. Publication and Repository Responsibilities

2.1 Repositories

DigiCert shall operate CRLs that will be available to both Subscribers and Relying Parties of GeoTrust Certificates. Each CRL is signed by the issuing CA. The procedures for revocation are as stated elsewhere in this CPS.

2.2 Publication of Certificate Information

DigiCert retains copies of all Certificates for the life of the CA, but does not archive or retain expired or superseded CRLs. DigiCert provides Relying Parties with information on how to find the appropriate repository to check Certificate status and, if OCSP (Online Certificate Status Protocol) is available, how to find the right OCSP responder.

2.3 Time or Frequency of Publication

Updates to Subscriber Agreements and Relying Party Agreements are published as necessary. DigiCert offers CRLs showing the revocation of GeoTrust Certificates and offers status checking services through the GeoTrust Repository. CRLs for end-user Subscriber Certificates are issued at least once per day. CRLs for CAs that only issue CA Certificates are issued at least annually, and also whenever a CA Certificate is revoked. If a Certificate listed in a CRL expires, it may be removed from later issued CRLs after the Certificate's expiration. DigiCert develops, implements, enforces, and annually updates this Certification Practices Statement which describes in detail how DigiCert implements the latest version of the CA/Browser Forum Baseline Requirements.

2.4 Access Controls on Repository

Information published in the repository portion of the GeoTrust/DigiCert web site is publicly-accessible information. DigiCert requires persons to agree to a Relying Party Agreement as a condition to accessing Certificates, Certificate status information, or CRLs. DigiCert implements controls to prevent unauthorized persons from adding, deleting, or modifying repository entries. DigiCert makes its repository publicly available in a read-only manner, and specifically at the link stated in section 1.5.3.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

Certificates contain an X.501 distinguished name in the Subject name field and consist of the components specified in the table below.

Attribute	Value
Country (C) =	2 letter ISO country code or not used
Organization (O) =	The Organization attribute is used as follows: • Subscriber organizational name for web server Certificates and individual Certificates that have an organization affiliation, or • A domain name, or "GeoTrust Verified Site" or similar language in the Organization field (for web server certificates that have domain control validation only and no organization verification), or • When applicable, wording to the effect that the organization has not been authenticated.
Organizational Unit (OU) =	GeoTrust Certificates may contain multiple OU attributes. Such attributes may contain one or more of the following: • Subscriber organizational unit (for organizational Certificates and individual Certificates that have an organization affiliation) • Text to describe the type of Certificate. • Text to describe the entity that performed the verification • "Domain Control Validated", where appropriate • Business registration number, if available • The address of the customer
State or Province (S) =	When used, indicates the Subscriber's State or Province. State will appear in any certificates in the scope of the CA/Browser Forum Baseline Requirements in cases where no meaningful value for locality exists for the subject.
Locality (L) =	When used, indicates the Subscriber's Locality
Common Name (CN) =	This attribute may include:

Attribute	Value
	• Domain name (for web server Certificates)* • Organization name (for code/object signing Certificates and RapidSSL Enterprise) • Name of individual (for certificates issued to individuals). • IP Address (TrueBusiness ID, RapidSSL Enterprise)[1] • Host name (RapidSSL Enterprise) * For internationalized domain names, the Common Name will be represented as a Unicode encoded U-label value designed for human comprehension and that Common Name will be represented in the Subject Alternative Name extension as a puny-coded A-label value designed for automated comprehension. These different encodings of the same name are treated as equal values for the purposes of Common Name to Subject Alternative Name duplication requirements.
E-Mail Address (E) =	When used, the e-mail address associated with the certificate

Table 1 – Distinguished Name Attributes in Subscriber Certificates

EV SSL certificate content and profile requirements are discussed in Appendix B2 to this CPS.

3.1.1.1 CABF Naming Requirements

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the respective CA / Browser Forum requirements as set forth in the DigiCert CP and CPSCP and CPS.

3.1.2 Need for Names to be Meaningful

End-user Subscriber Certificates contain names with commonly understood semantics permitting the determination of the identity of the individual or organization that is the Subject of the Certificate.

3.1.3 Anonymity or Pseudonymity of Subscribers

With the exception of **True Credential** and **True Credential Express**, Subscribers are not permitted to use pseudonyms (names other than a Subscriber's true personal or organizational name).

3.1.4 Rules for Interpreting Various Name Forms

No stipulation

3.1.5 Uniqueness of Names

The names of Subscribers are unique within DigiCert's and a Customer's Sub-domain for a specific type of Certificate. It is possible for a Subscriber to have two or more certificates with the same Subject Distinguished Name (DN).

---

[1] Any reference to IP address inclusion in Certificates are for legacy purposes or exceptional circumstances that are validated and controlled by DigiCert as per the DigiCert CPS section 3.2.2.

3.1.6 Recognition, Authentication, and Role of Trademarks

Certificate Applicants are prohibited from using names in their Certificate Applications that infringe upon the Intellectual Property Rights of others. For EV SSL Certificates, DigiCert implements a process that prevents EV Certificates from including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless DigiCert has verified this information in accordance with the EV Guidelines and section 3.2 of the DigiCert CP and CPS. For all other Certificate types, DigiCert does not verify whether a Certificate Applicant has Intellectual Property Rights in the name appearing in a Certificate Application or arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any domain name, trade name, trademark, or service mark. DigiCert is entitled, without liability to any Certificate Applicant, to reject or suspend any Certificate Application because of such dispute.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The certificate applicant may demonstrate that it rightfully holds the private key corresponding to the public key to be listed in the Certificate. The method to prove possession of a private key is to submit a PKCS #10 signed using the private key, another cryptographically equivalent demonstration, or another DigiCert-approved method. This process does not apply where a key pair is generated by DigiCert on behalf of a Subscriber, for example where pre-generated keys are placed on smart cards.

3.2.2 Authentication of Organization Identity

Whenever an organization name is included in the Certificate, DigiCert or the RA will take reasonable steps to establish that a Certificate request made on behalf of that Organization is legitimate and properly authorized. DigiCert will ensure the following:

(a) the Organizational Name appears in conjunction with a country and possibly a state or province or other locality to sufficiently identify its place of registration or a place where it is currently doing business; and

(b) in the case of an Organization that could reasonably be expected to be registered with a local, state or national authority, DigiCert will obtain, view and verify copies of the registration documents. For instance, DigiCert may
(i) verify the validity of the registration through the authority that issued it, or
(ii) verify the validity of the registration through a reputable third party database or other resource, or
(iii) verify the validity of the Organization through a trusted third party, or
(iv) confirm that the Organization exists if such Organization is not the type that is typically registered or is capable of being verified under clause (b).

(c) confirm by telephone, confirmatory postal mail, or comparable procedure to the Certificate Applicant certain information about the organization, that the organization has authorized the Certificate Application, and that the person submitting the Certificate Application on behalf of the Certificate Applicant is authorized to do so. When a certificate request includes the name of an individual as an authorized representative of the Organization, the employment of that individual and his/her authority to act on behalf of the Organization shall also be confirmed.

Additional procedures are performed for specific types of Certificates as described in Table 2 below.

Certificate Type	Additional Procedures
Extended Validation (EV) Certificates	Supplemental validation procedures for issuing EV SSL Certificates are described in the DigiCert CP and CPS.
EV Code Signing Certificates	DigiCert adheres to the current version of the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation (EV) Code Signing Certificates which can be accessed at https://cabforum.org/ev-code-signing-certificate-guidelines/.
Organization Validated (OV) and Domain Validated (DV) Certificates	DigiCert's procedures for issuing OV and DV certificates are listed in the DigiCert CP and CPS in section 3.2.2, distinguished throughout the CPS as 'CABF requirements for OV and DV certificates'. Furthermore, DigiCert adheres to the current version of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates which can be accessed at https://cabforum.org/baseline-requirements-documents/.
Hardware Protected EV Code-Signing Certificate	DigiCert verifies that the key pair was generated on FIPS 140 certified hardware

Table 2 – Specific Authentication Procedures

3.2.2.1 CABF Verification Requirements for Organization Applicants

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the respective CA / Browser Forum requirements as set forth in the DigiCert CP and CPS.

3.2.2.2 Mozilla Verification Requirements for Organization Applicants

For requests for internationalized domain names (IDNs) in Certificates, DigiCert performs domain name owner verification to detect cases of homographic spoofing of IDNs.

DigiCert actively participates in the CA/Browser Forum providing input to the standards for IDN Certificates and fully commits to conforming with standards drafted by that body.

3.2.2.3 Authentication of Domain Name

When a domain name is included in a Certificate together with an organization name, DigiCert or the RA will verify that the Subscriber had the right to use the domain name submitted by the Subscriber at the time it submitted its application using the methods described in section 3.2.2. of the DigiCert CPS.

3.2.3 Authentication of individual identity

An Applicant for a GeoTrust **My Credential** Certificate shall complete a GeoTrust My Credential enrollment application on behalf of Subscriber in a form prescribed by DigiCert. All applications are subject to review, approval and acceptance by DigiCert. All Applicants are required to include an e-mail contact address ("Contact Address") and telephone number ("Telephone Number") within the My Credential enrollment application and prove control over the Contact Address and Telephone Number. DigiCert does not otherwise verify the accuracy of the information contained in the Applicant's enrollment form or otherwise check for errors and omissions.

True Credential Subscribers must provide the following data in or with the CSR: *Common Name* and *E-mail Address* of Subscriber. The Company Administrator corresponding to the Subscriber will have sole responsibility for approving all Certificate requests for issuance.

Once approved, DigiCert will process the Certificate applications without confirming the information on the Certificates. Company will be required to agree to terms and conditions of use as necessary for issuance of Certificates through an enrolment agreement, and Subscribers receiving Certificates via the Service may be required to agree to additional terms and conditions of use as necessary to receive a Certificate authorized by the Administrator.

3.2.4 Non-Verified Subscriber Information

Non-verified Subscriber information includes:

• Organization Unit (OU) with certain exceptions[2]
• Country Code (within the **Power Server ID** and **Quick SSL** Certificate)
• Customer specified host name or organizational unit (within the **RapidSSL Enterprise** certificate)
• Any other information designated as non-verified in the certificate.

3.2.5 Validation of Authority

DigiCert will take reasonable steps to establish that a Certificate request made on behalf of an Organization is legitimate and properly authorized. Affirmation of authority is typically derived from the Applicant's actions in confirming the right to use or control the requested domain names using procedures listed in Section 3.2.2 of the DigiCert CPS. To prove that a Certificate is duly authorized by the Organization in other situations, DigiCert will typically request the name of a contact person who is employed by or is an officer of the Organization. DigiCert will also typically require a form of authorization from the Organization confirming its intent to obtain a Certificate and will usually document the Organization's contact person. DigiCert normally confirms the contents of this authorization with the listed contact person.

3.2.6 Criteria for Interoperation

No Stipulation

3.3 Identification and Authentication for Re-key Requests

Prior to the expiration of an existing Certificate, it is necessary for the Subscriber to obtain a new Certificate to maintain continuity of Certificate usage. Subscribers have the option of generating a new Key Pair to replace the expiring Key Pair (technically defined as "rekey") or of creating a new CSR for an existing Key Pair (technically defined as "renewal"), depending on their preferences and the capabilities and restrictions of the Subscriber's key generation tools. For purposes of this CPS, both a "rekey" and "renewal" as defined above will be treated as a renewal Certificate.

New certificate information submitted for renewal Certificates are subject to the same authentication steps outlined in this CPS as apply to initial issuance of a Certificate.

---

[2] Domain-validated and organization-validated certificates that attest compliance with CA/Browser guidelines may contain Organizational Unit values that are validated.

3.4 Identification and Authentication for Revocation Request

The only persons permitted to request revocation of a Certificate issued by DigiCert are the Subscriber (including designated representatives), the administrative contact or the technical contact, or an enterprise Administrator. Additionally, Relying Parties, Application Software Suppliers, and other third parties may submit Certificate Problem Reports informing the issuing CA of reasonable cause to revoke the certificate.

To request revocation, a Subscriber or Authorized requester must contact DigiCert, either by telephone, e-mail message, a national/regional postal service, facsimile, or overnight courier, and specifically request "revocation" (using that term) of a particular Certificate identified by the Subscriber.

Upon receipt of a revocation request, DigiCert will seek confirmation of the request by telephone, e-mail message, or other reliable means of communication. DigiCert will authenticate the validity of the revocation request before taking action. Upon confirmation of the revocation request, DigiCert will revoke the Certificate and post the revocation to the appropriate CRL, which will constitute notice to the Subscriber that the Certificate has been revoked.

DigiCert will require a confirming e-mail message back from either the administrative or technical contact authorizing revocation (or by other means of confirmation acceptable to DigiCert). Upon receipt of the confirming e-mail message, DigiCert will revoke the Certificate and the revocation will be posted to the appropriate CRL. Notification will be sent to the subject of the Certificate and the subject's designated contacts. There is no grace period available to the Subscriber prior to revocation, and DigiCert shall respond to the revocation request within the next business day and post the revocation to the next published CRL.

Enterprise Administrators may revoke certificates through a Web-based application.

4. Certificate Life-Cycle Operations

4.1 Certificate Application

4.1.1 Who Can Submit A Certificate Application?

Below is a list of people who may submit certificate applications:

• Any individual who is the subject of the certificate,
• Any authorized representative of an Organization or entity,
• Any authorized representative of a CA,
• Any authorized representative of an RA.

4.1.2 Enrollment Process and Responsibilities

4.1.2.1 End-User Certificate Subscribers

All end-user Certificate Subscribers shall manifest assent to the relevant Subscriber Agreement and undergo an enrollment process consisting of:

• completing a Certificate Application and providing true and correct information,
• generating, or arranging to have generated, a key pair,
• delivering his, her, or its public key, directly or through an RA, to DigiCert
• demonstrating possession of the private key corresponding to the public key delivered to DigiCert.

RapidSSL Enterprise certificate enrolments are only available through the Symantec Managed PKI (MPKI) for SSL program.

4.1.2.2 CABF Certificate Application Requirements

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the respective CA / Browser Forum requirements as set forth in the DigiCert CP and CPS.

4.1.2.3 CA and RA Certificates

Subscribers of CA and RA Certificates enter into a contract with DigiCert. CA and RA Applicants shall provide their credentials to demonstrate their identity and provide contact information during the contracting process. During this contracting process or, at the latest, prior to the Key Generation Ceremony to create a CA or RA key pair, the applicant shall cooperate with DigiCert to determine the appropriate distinguished name and the content of the Certificates to be issued by the applicant.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

DigiCert or an RA shall perform identification and authentication of all required Subscriber information in terms of Section 3.2.

At certain times during the enrolment process in which DigiCert is not able to verify information in an enrolment 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 enrolment form for a Certificate.

4.2.2 Approval or Rejection of Certificate Applications

DigiCert or an RA will approve an application for a certificate if the following criteria are met:

• Successful identification and authentication of all required Subscriber information in terms of Section 3.2
• Payment has been received

DigiCert or an RA will reject a certificate application if:

• identification and authentication of all required Subscriber information in terms of Section 3.2 cannot be completed, or
• The Subscriber fails to furnish supporting documentation upon request, or
• The Subscriber fails to respond to notices within a specified time, or
• Payment has not been received, or
• they believe that issuing a certificate to the Subscriber may bring the DigiCert PKI into disrepute

4.2.3 Time to Process Certificate Applications

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

A certificate application remains active until rejected or issued.

4.2.4 Certificate Authority Authorization

As of September 8, 2017, CAA issue and issuewild records are checked either within 8 hours of issuance or the CAA record's Time to Live (TTL), whichever is greater, except where CAA was similarly checked prior to the creation of a Certificate Transparency pre-certificate that was logged in at least 2 public CT log servers. CAA checking may be omitted for technically-constrained subordinate CAs.

DNS access failure is treated as permission to issue when the failure is proven to be outside GeoTrust infrastructure, was retried at least once, and the domain zone does not have a DNSSEC validation chain to the ICANN root.

DigiCert logs actions taken based on CAA records, and documents issuance prevented by CAA for feedback to the CA/Browser Forum.

Specifically related to this CPS, DigiCert recognizes any and all of the following Issuer Domain Names as permission to issue: digicert.com, symantec.com, thawte.com, geotrust.com, rapidssl.com, and FQDNs terminating in the base domain name digitalcertvalidation.com with reseller-specific licensed prefixes.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

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

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificates

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

4.3.3 CABF Requirement for Certificate Issuance by a Root CA

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the respective CA / Browser Forum requirements as set forth in the DigiCert CP and CPS.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The following conduct constitutes certificate acceptance:
- Downloading a Certificate or installing a Certificate from a message attaching it constitutes the Subscriber's acceptance of the Certificate.
- Failure of the Subscriber to object to the certificate or its content constitutes certificate acceptance.

4.4.2 Publication of the Certificate by the CA

No stipulation.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

RAs may receive notification of the issuance of certificates they approve.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Usage

Use of the Private key corresponding to the public key in the certificate shall only be permitted once the Subscriber has agreed to the Subscriber Agreement and accepted the certificate. The certificate shall be used lawfully in accordance with the applicable GeoTrust/DigiCert Subscriber Agreement and the terms of this CPS. Certificate use must be consistent with the KeyUsage field extensions included in the certificate (e.g., if Digital Signature is not enabled then the certificate must not be used for signing).

Subscribers shall protect their private keys from unauthorized use and shall discontinue use of the private key following expiration or revocation of the certificate. Parties other than the Subscriber shall not archive the Subscriber Private Key except as set forth in section 4.12.

The Certificate shall not be installed on more than a single server at a time unless the Subscriber enrollment and corresponding fees have stipulated installation on multiple servers.

4.5.2 Relying Party Public Key and Certificate Usage

Relying Parties must verify that the Certificate is valid by examining the Certificate Revocation List ("CRL") before initiating a transaction involving such Certificate. DigiCert does not accept responsibility for reliance on a fraudulently obtained Certificate or a Certificate that is on the CRL. Reliance on a certificate must be reasonable under the circumstances. If the circumstances indicate a need for additional assurances, the Relying Party must obtain such assurances for such reliance to be deemed reasonable.

Before any act of reliance, Relying Parties shall independently assess:
- the appropriateness of the use of a Certificate for any given purpose and determine that the Certificate will, in fact, be used for an appropriate purpose that is not prohibited or otherwise restricted by this CPS. DigiCert is not responsible for assessing the appropriateness of the use of a Certificate.
- That the certificate is being used in accordance with the KeyUsage field extensions included in the certificate (e.g., if Digital Signature is not enabled then the certificate may not be relied upon for validating a Subscriber's signature).

- The status of the certificate and all the CAs in the chain that issued the certificate. If any of the Certificates in the Certificate Chain have been revoked, the Relying Party is solely responsible to investigate whether reliance on a digital signature performed by an end user Subscriber Certificate prior to revocation of a Certificate in the Certificate chain is reasonable. Any such reliance is made solely at the risk of the Relying party.

Assuming that the use of the Certificate is appropriate, Relying Parties shall utilize the appropriate software and/or hardware to perform digital signature verification or other cryptographic operations they wish to perform, as a condition of relying on Certificates in connection with each such operation. Such operations include identifying a Certificate Chain and verifying the digital signatures on all Certificates in the Certificate Chain.

4.6 Certificate Renewal

4.6.1 Circumstances for Certificate Renewal

Prior to the expiration of an existing Certificate, it is necessary for the Subscriber to obtain a new Certificate to maintain continuity of Certificate usage. Subscribers have the option of generating a new Key Pair to replace the expiring Key Pair (technically defined as "rekey") or of creating a new CSR for an existing Key Pair (technically defined as "renewal"), depending on their preferences and the capabilities and restrictions of the Subscriber's key generation tools. For purposes of this CPS, both a "rekey" and "renewal" as defined above will be treated as a renewal Certificate.

Renewal Certificates are subject to the same authentication steps outlined in this CPS as apply to initial issuance of a Certificate.

4.6.2 Who May Request Renewal

Only the subscriber for an individual certificate or an authorized representative for an Organizational certificate may request certificate renewal

4.6.3 Processing Certificate Renewal Requests

See section 4.2.

4.6.4 Notification of New Certificate Issuance to Subscriber

Notification of issuance of certificate renewal to the Subscriber is in accordance with Section 4.3.2.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Conduct constituting Acceptance of renewed certificate is in accordance with Section 4.4.1.

4.6.6 Publication of the Renewal Certificate by the CA

No stipulation.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

RAs may receive notification of the issuance of certificates they approve.

4.7 Certificate Re-Key

See Section 3.3.

4.7.1 Circumstances for Re-Key

See Section 3.3.

4.7.2 Who May Request Certification of a New Public Key

Only the subscriber for an individual certificate or an authorized representative for an Organizational certificate may request certificate renewal/rekey.

4.7.3 Processing Certificate Re-Keying Requests

The provisions of Section 4.2 apply.

4.7.4 Notification of New Certificate Issuance to Subscriber

Notification of issuance of a re-keyed certificate to the Subscriber is in accordance with Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Conduct constituting Acceptance of a re-keyed certificate is in accordance with Section 4.4.1.

4.7.6 Publication of the Re-Keyed Certificate by the CA

No stipulation.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

RAs may receive notification of the issuance of certificates they approve.

4.8 Certificate Modification

4.8.1 Circumstances for Certificate Modification

Certificate modification refers to the application for the issuance of a new certificate due to changes in the information in an existing certificate (other than the subscriber's public key). Certificate modification is considered a Certificate Application in terms of Section 4.1.

4.8.2 Who May Request Certificate Modification

See Section 4.1.1.

4.8.3 Processing Certificate Modification Requests

DigiCert or an RA shall perform identification and authentication of all required Subscriber information in terms of Section 3.2.

4.8.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

See Section 4.4.1.

4.8.6 Publication of the Modified Certificate by the CA

Not applicable.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

DigiCert will revoke a Certificate within 24 hours if one or more of the following occurs:
> 1. The Subscriber requests in writing that DigiCert revoke the Certificate;
> 2. The Subscriber notifies DigiCert that the original Certificate request was not authorized and does not retroactively grant authorization;
> 3. DigiCert obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise; or
> 4. DigiCert obtains evidence that the validation of domain authorization or control for any FDQN or IP address in the Certificate should not be relied upon.

DigiCert may revoke a certificate within 24 hours and will revoke a Certificate within 5 days if one or more of the following occurs:
> 1. The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of the CA/B Forum Baseline Requirements;
> 2. DigiCert obtains evidence that the Certificate was misused;
> 3. The Subscriber or the cross-certified CA breached a material obligation under the CP, this CPS, or the relevant agreement;
> 4. DigiCert confirms any circumstance indicating that use of a FQDN or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name registrant and the Applicant has terminated, or the Domain Name registrant has failed to renew the Domain Name);
> 5. DigiCert confirms that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate FQDN;
> 6. DigiCert confirms a material change in the information contained in the Certificate;
> 7. DigiCert confirms that the Certificate was not issued in accordance with the CA/B Forum requirements or the DigiCert CP, DigiCert CPS, or this CPS;
> 8. DigiCert determines or confirms that any of the information appearing in the Certificate is inaccurate;
> 9. DigiCert's right to issue Certificates under the CA/B Forum requirements expires or is revoked or terminated, unless DigiCert has made arrangements to continue maintaining the CRL/OCSP Repository;

10. Revocation is required by the DigiCert CP, DigiCert CPS, or this CPS; or

11. DigiCert confirms a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, methods have been developed that can easily calculate it based on the Public Key (such as a debian weak key, see http://wiki.debian.org/SSLkeys), or if there is clear evidence that the specific method used to generate the Private Key was flawed.

DigiCert will revoke a Subordinate CA Certificate within seven (7) days if one or more of the following occurs:

1. The Subordinate CA requests revocation in writing;

2. The Subordinate CA notifies DigiCert that the original Certificate request was not authorized and does not retroactively grant authorization;

3. DigiCert obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a key compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of the CA/B Forum Baseline Requirements;

4. DigiCert obtains evidence that the CA Certificate was misused;

5. DigiCert confirms that the CA Certificate was not issued in accordance with or that Subordinate CA has not complied with this document or the applicable Certificate Policy or Certification Practice Statement;

6. DigiCert determines that any of the information appearing in the CA Certificate is inaccurate or misleading;

7. DigiCert or the Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the CA Certificate;

8. DigiCert's or the Subordinate CA's right to issue Certificates under the Baseline Requirements expires or is revoked or terminated, unless DigiCert has made arrangements to continue maintaining the CRL/OCSP Repository;

9. Revocation is required by DigiCert's Certificate Policy and/or Certification Practice Statement; or

10. The technical content or format of the CA Certificate presents an unacceptable risk to application software suppliers or Relying Parties.

DigiCert shall revoke a Certificate:
- in the event of compromise of the GeoTrust CA Private Key used to sign a certificate;
- in the event the SSL Certificate is installed on more than a single server at a time without permission of DigiCert.
- If an RA reasonably determines that a Publisher Certificate is being used in a manner that compromises the trust status of relying parties.
- In the case of code signing certificates,
  - An Application Software Supplier requests the CA revoke and an investigation indicates that the certificate is being used to sign malware or other unwanted software,
  - A report is submitted to DigiCert indicating that the certificate was used to sign malware.

DigiCert always revokes a Certificate if the binding between the subject and the subject's Public Key in the certificate is no longer valid or if an associated Private Key is compromised.

Subscribers shall state the reason(s) for requesting revocation upon submitting the request.

DigiCert will revoke a cross-Certificate if the cross-certified entity (including DigiCert) no longer meets the stipulations of the corresponding policies, as indicated by policy OIDs listed in the policy mapping extension of the cross-Certificate.

If DigiCert initiates revocation of a Certificate, DigiCert shall notify the administrative and technical contact provided by Subscriber by e-mail message of the revocation.

In the event that DigiCert ceases operations and there is no plan for transition of DigiCert's services to a successor or no plan to otherwise address such event, all Certificates issued by DigiCert shall be revoked prior to the date that DigiCert ceases operations, and DigiCert shall notify the technical contact provided by Publisher by e-mail message of the revocation and the reason for the revocation.

4.9.1.1 CABF Requirements for Reasons for Revocation

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the respective CA / Browser Forum requirements as set forth in the DigiCert CPS, section 4.9.1.

4.9.2 Who Can Request Revocation

The only persons permitted to request revocation of a Certificate issued by DigiCert are the Subscriber (including designated representatives), the administrative contact or the technical contact, an enterprise Administrator, DigiCert and Microsoft (under certain circumstances).

Any person claiming to have witnessed certificate misuse, inappropriate conduct related to certificates, fraud or key compromise may submit a Certificate Problem Report using the online form available at the GeoTrust/DigiCert website. DigiCert will investigate all Certificate Problem Reports and take action within the prescribed timing stated in the CABF Baseline Requirements.

4.9.3 Procedure for Revocation Request

DigiCert processes a revocation request as follows:
1. DigiCert logs the identity of the entity making the request or problem report and the reason for requesting revocation based on the list in section 4.9.1. DigiCert may also include its own reasons for revocation in the log.
2. DigiCert may request confirmation of the revocation from a known administrator, where applicable, via out-of-band communication (e.g., telephone, fax, etc.).
3. If the request is authenticated as originating from the Subscriber, DigiCert revokes the Certificate based on the timeframes listed in 4.9.1 as listed for the reason for revocation.
4. For requests from third parties, DigiCert personnel begin investigating the request within 24 hours after receipt and decide whether revocation is appropriate based on the following criteria:
   a. the nature of the alleged problem,
   b. the number of reports received about a particular Certificate or website,
   c. the identity of the complainants (for example, complaints from a law enforcement official that a web site is engaged in illegal activities have more weight than a complaint from a consumer alleging they never received the goods they ordered), and
   d. relevant legislation.
5. If DigiCert determines that revocation is appropriate, DigiCert personnel revoke the Certificate and update the CRL.

If DigiCert deems appropriate, DigiCert may forward the revocation reports to law enforcement.

DigiCert maintains a continuous 24/7 ability to internally respond to any high priority revocation requests.

4.9.3.1 Procedure for Requesting the Revocation of an End-User Subscriber Certificate

See Section 3.4.

4.9.3.2 CABF Requirements for Certificate Revocation Process

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the respective CA / Browser Forum requirements as set forth in the DigiCert CP and CPS.

4.9.3.2 Procedure for Requesting the Revocation of a CA or RA Certificate

A CA or RA requesting revocation of its CA or RA Certificate is required to communicate the request to DigiCert and DigiCert will seek confirmation of the request. DigiCert will then revoke the Certificate. RapidSSL for Enterprise certificates are revoked through the Symantec MPKI for SSL Service and do not require an out-of-band confirmation.

DigiCert may also initiate CA or RA Certificate revocation.

4.9.4 Revocation Request Grace Period

Revocation requests shall be submitted as promptly as possible within a commercially reasonable time. There is no grace period available to the Subscriber prior to revocation.

4.9.5 Time within Which CA Must Process the Revocation Request

Certificate problem reports are submitted by third parties and subject to investigation. Revocation requests are submitted by DigiCert, an RA, or the Subscriber.

Within 24 hours after receiving a Certificate problem report, DigiCert investigates the facts and circumstances related to a Certificate problem report and will provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate problem report.

After reviewing the facts and circumstances, DigiCert works with the Subscriber and any entity reporting the Certificate problem report or other revocation-related notice to establish whether or not the certificate will be revoked, and if so, a date which DigiCert will revoke the certificate. The period from receipt of the Certificate problem report or revocation-related notice to published revocation must not exceed the time frame set forth in Section 4.9.1. The date selected by DigiCert will consider the following criteria:
1. The nature of the alleged problem (scope, context, severity, magnitude, risk of harm);
2. The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties);
3. The number of Certificate problem reports received about a particular Certificate or Subscriber;
4. The entity making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that she didn't receive the goods she ordered); and
5. Relevant legislation.

Under normal operating circumstances, DigiCert will revoke Certificates as quickly as practical after validating the revocation request following the guidelines of this section and Section 4.9.1, generally within the following time frames:
1. Certificate revocation requests for publicly-trusted Certificates are processed within 18 hours after their receipt,
2. Revocation requests received two or more hours before CRL issuance are processed before the next CRL is published, and
3. Revocation requests received within two hours of CRL issuance are processed before the following CRL is published.

DigiCert takes commercially reasonable steps to process revocation requests without delay. DigiCert complies with the revocation timeframes specified for malware in the Minimum Requirements for Issuance and Management of Publicly-Trusted Code Signing Certificates in section 13.1.5.3 for code signing certificates.

4.9.6 Revocation Checking Requirements for Relying Parties

Relying Parties shall check the status of Certificates on which they wish to rely. One method by which Relying Parties may check Certificate status is by consulting the most recent CRL from the CA that issued the Certificate on which the Relying Party wishes to rely. Certificate Revocation Lists are available at http://crl3.digicert.com or *www.geotrust.com, as specified in a given certificate*. Certificate Revocation Lists are available at *www.FreeSSL.com/legal and www.RapidSSL.com/legal* for FreeSSL certificates and RapidSSL certificates respectively.

4.9.7 CRL Issuance Frequency

DigiCert shall post the CRL online at least weekly (but no later than twenty-four (24) hours after revocation of a Certificate) in a DER format except as otherwise provided in DigiCert's Business Continuity Plan. If a Certificate listed in a CRL expires, it may be removed from later-issued CRLs after the Certificate's expiration.

4.9.7.1 CABF Requirements for CRL Issuance

CRL issuance for EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the respective CA / Browser Forum requirements as set forth in the DigiCert CP and CPSCP and CPS.

4.9.8 Maximum Latency for CRLs

CRLs are posted to the repository within a commercially reasonable time after generation.

4.9.9 On-Line Revocation/Status Checking Availability

The CRL is available at: http://crl3.digicert.com or *www.geotrust.com, as specified in a given certificate*. Certificate Revocation Lists are available at *www.FreeSSL.com/legal and www.RapidSSL.com/legal* for FreeSSL certificates and RapidSSL certificates respectively.

4.9.9.1 CABF Requirements for OCSP Availability

OCSP availability for EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the respective CA / Browser Forum requirements as set forth in the DigiCert CP and CPS.

4.9.10 On-Line Revocation Checking Requirements

A Relying Party must check the status of a certificate on which he/she/it wishes to rely. If a Relying Party does not check the status of a Certificate on which the Relying Party wishes to rely by consulting the most recent relevant CRL, the Relying Party shall check Certificate status by consulting the applicable repository or by requesting Certificate status using the applicable OCSP responder (where OCSP services are available).

4.9.11 Other Forms of Revocation Advertisements Available

Not Applicable.

4.9.12 Special Requirements Regarding Key Compromise

In the event of compromise of a DigiCert Private Key used to sign Certificates, DigiCert will send an e-mail message as soon as practicable to all Subscribers with Certificates issued off the Private Key stating that the Certificates will be revoked by the next business day and that posting the revocation to the appropriate CRL will constitute notice to the Subscriber that the Certificate has been revoked.

4.9.13 Circumstances for Suspension

DigiCert does not support Certificate suspension.

4.9.14 Who can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits of Suspension Period

Not applicable.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The status of certificates is available via CRL and via an OCSP responder (where available).

4.10.2 Service Availability

Certificate Status Services are available 24✕7.

Certificate status services for EV SSL Certificates, EV Code Signing, and Organization-validated and Domain-validated SSL Certificates, conform to the respective CA / Browser Forum requirements as set forth in the DigiCert CP and CPS.

4.10.3 Optional Features

Not applicable.

4.11 End of Subscription

A subscriber may end a subscription for a GeoTrust certificate by:
1. Allowing his/her/its certificate to expire without renewing or re-keying that certificate
2. Revoking of his/her/its certificate before certificate expiration without replacing the certificates.

4.12 Key Escrow and Recovery

The Root Keys for each CA Certificate were generated and are stored in hardware and are backed up but not escrowed. GeoTrust CA participants may escrow end-user Subscriber private keys.

4.12.1 Key Escrow and Recovery Policy and Practices

The private keys of end-user Subscribers may be escrowed.

When applicable, private keys are stored in DigiCert's premises in encrypted PKCS#12 structures. A unique symmetric key is generated for each Subscriber's private key. A PKCS#12 structure is generated with the Subscriber's private key and certificate. The PKCS#12 structure is encrypted with the symmetric key using 128-bit AES. The symmetric key is then encrypted with the public key of the Enterprise's Master Key Recovery Certificate using 128-bit AES. The encrypted PKCS#12 and the encrypted symmetric key are stored in DigiCert's premises.

Recovery of a private key and digital certificate requires the Administrator who has access to the Master Key Recovery Certificate to securely access their Enterprise account with GeoCenter and select the enrolment record associated with the private key that is to be recovered. The Administrator then downloads the encrypted PKCS#12 and initiates the Recovery process. A java applet is downloaded to the local workstation and the Administrator is prompted to identify the location of the Master Key Recovery certificate and the password for accessing the Master Key Recovery certificate. The java applet accesses the private key of the Master Key Recovery certificate and uses the private key to decrypt the encrypted symmetric key. The symmetric key is then displayed, and the Administrator can use the symmetric key to access the encrypted PKCS#12.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

See section 4.12.1.

5. Facility, Management, and Operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

DigiCert's CA and RA operations are conducted within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information and systems whether covert or overt.

5.1.2 Physical Access

Only authorized DigiCert employees can access the CA facility using biometrics, and proximity card access

5.1.3 Power and Air Conditioning

DigiCert's CA facility is equipped with primary and backup:
- o Power systems to ensure continuous, uninterrupted access to electric power and
- o Heating/ventilation/air conditioning systems to control temperature and relative humidity.

5.1.4 Water Exposures

DigiCert has taken reasonable precautions to minimize the impact of water exposure to DigiCert systems.

5.1.5 Fire Prevention and Protection

DigiCert has taken reasonable precautions to prevent and extinguish fires or other damaging exposure to flame or smoke. DigiCert's fire prevention and protection measures have been designed to comply with local fire safety regulations.

5.1.6 Media Storage

All media containing production software and data, audit, archive, or backup information is stored with appropriate physical and logical access controls designed to limit access to authorized personnel and protect such media from accidental damage.

5.1.7 Waste Disposal

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

5.1.8 Off-Site Backup

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

5.2 Procedural Controls

5.2.1 Trusted Roles

Trusted Persons include all employees, contractors, and consultants that have access to or control authentication or cryptographic operations that may materially affect:
- • the validation of information in Certificate Applications;
- • the acceptance, rejection, or other processing of Certificate Applications, revocation requests, renewal requests, or enrollment information;

- the issuance, or revocation of Certificates, including personnel having access to restricted portions of its repository;
- the handling of Subscriber information or requests.

Trusted Persons include, but are not limited to:
- customer service personnel,
- cryptographic business operations personnel,
- security personnel,
- system administration personnel,
- designated engineering personnel, and
- executives that are designated to manage infrastructural trustworthiness.

DigiCert considers the categories of personnel identified in this section as Trusted Persons having a Trusted Position. Persons seeking to become Trusted Persons by obtaining a Trusted Position must successfully complete the screening requirements set out in this CPS.

5.2.2 Number of Persons Required per Task

DigiCert has established, maintains, and enforces rigorous control procedures to ensure the segregation of duties based on job responsibility and to ensure that Trusted Persons are required to perform sensitive tasks.

Policy and control procedures are in place to ensure segregation of duties based on job responsibilities. The most sensitive tasks, such as access to and management of CA cryptographic hardware (cryptographic signing unit or CSU) and associated key material, require Trusted Persons. These internal control procedures are designed to ensure that trusted personnel are required to have either physical or logical access to the device. Access to CA cryptographic hardware is strictly allowed by Trusted Persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction.

5.2.3 Identification and Authentication for Each Role

For all personnel seeking to become Trusted Persons, verification of identity is performed through the personal (physical) presence of such personnel before Trusted Persons performing DigiCert Human Resources or security functions and a check of well-recognized forms of identification (e.g., passports and driver's licenses). Identity is further confirmed through the background checking procedures in CPS § 5.3.1.

DigiCert ensures that personnel have achieved Trusted Status and departmental approval has been given before such personnel are:
- issued access devices and granted access to the required facilities;
- issued electronic credentials to access and perform specific functions on the GeoTrust CA, RA, or other IT systems.

5.2.4 Roles Requiring Separation of Duties

Roles requiring Separation of duties or multi-person controls include (but are not limited to):
1. the validation of information in Certificate Applications;
2. the generation, issuing or destruction of a CA certificate
3. the loading of a CA to a Production environment

5.3 Personnel Controls

Personnel seeking to become Trusted Persons must present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily, as well as proof of any government clearances, if any, necessary to perform certification services under government contracts. Background checks are repeated at least every 10 years for personnel holding Trusted Positions.

5.3.1 Qualifications, Experience, and Clearance Requirements

DigiCert requires that personnel seeking to become Trusted Persons present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily, as well as proof of any government clearances, if any, necessary to perform certification services under government contracts.

5.3.2 Background Check Procedures

Prior to commencement of employment in a Trusted Role, DigiCert conducts background checks which include the following:

- confirmation of previous employment,
- check of professional reference,
- confirmation of the highest or most relevant educational degree obtained,
- search of criminal records (local, state or provincial, and national), and
- check of civil judgment records.

To the extent that any of the requirements imposed by this section cannot be met due to a prohibition or limitation in local law or other circumstances, DigiCert will utilize a substitute investigative technique permitted by law that provides substantially similar information, including but not limited to obtaining a background check performed by the applicable governmental agency.

The factors revealed in a background check that may be considered grounds for rejecting candidates for Trusted Positions or for taking action against an existing Trusted Person generally include (but are not limited to) the following:

- Misrepresentations made by the candidate or Trusted Person,
- Highly unfavorable or unreliable professional references,
- Certain criminal convictions, and
- Indications of a lack of financial responsibility.

Reports containing such information are evaluated by human resources and security personnel, who determine the appropriate course of action in light of the type, magnitude, and frequency of the behavior uncovered by the background check. Such actions may include measures up to and including the cancellation of offers of employment made to candidates for Trusted Positions or the termination of existing Trusted Persons.

The use of information revealed in a background check to take such actions is subject to the applicable federal, state, and local laws.

5.3.3 Training Requirements

For EV SSL Certificates, EV Code Signing, and Organization-validated and Domain-validated SSL Certificates, personnel training is provided in conformity with the respective CA/Browser Forum requirements as set forth in the DigiCert CP and CPS.

5.3.4 Retraining Frequency and Requirements

DigiCert provides refresher training and updates to their personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily.

5.3.5 Job Rotation Frequency and Sequence

Not applicable.

5.3.6 Sanctions for Unauthorized Actions

Appropriate disciplinary actions are taken for unauthorized actions or other violations of DigiCert policies and procedures. Disciplinary actions may include measures up to and including termination and are commensurate with the frequency and severity of the unauthorized actions.

5.3.7 Independent Contractor Requirements

In limited circumstances, independent contractors or consultants may be used to fill Trusted Positions. Any such contractor or consultant is held to the same functional and security criteria that apply to a DigiCert employees in a comparable position.

Independent contractors and consultants who have not completed or passed the background check procedures specified in CPS Section 5.3.2 are permitted access to DigiCert's secure facilities only to the extent they are escorted and directly supervised by Trusted Persons at all times.

5.3.8 Documentation Supplied to Personnel

DigiCert provides its employees the requisite training and other documentation needed to perform their job responsibilities competently and satisfactorily.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

DigiCert records CA event data.

Types of auditable events include:
1. Operational events (including but not limited to (1) the generation of a CA's own keys and the keys of subordinate CAs, (2) start-up and shutdown of systems and applications, (3) changes to CA details or keys, (4) cryptographic module lifecycle management-related events (*e.g.*, receipt, use, de-installation, and retirement), (5) possession of activation data for CA private key operations, physical access logs, (6) system configuration changes and maintenance, (7) Records of the destruction of media containing key material, activation data, or personal Subscriber information)

2. Certificate lifecycle events (including but not limited to initial issuance, re-key, renew, revocation, suspension)
3. Trusted employee events (including but not limited to (1) logon and logoff attempts, (2) attempts to create, remove, set passwords or change the system privileges of the privileged users, (3) personnel changes)
4. Discrepancy and compromise reports (including but not limited to unauthorized system and network logon attempts)
5. Failed read and write operations on the Certificate and repository
6. Changes to Certificate creation policies e.g., validity period

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the respective CA /Browser Forum requirements as set forth in the DigiCert CP and CPS.

5.4.2 Frequency of Processing Log

The GeoTrust CA event journal is processed at least monthly. Event journals are subject to review.

5.4.3 Retention Period for Audit Log

Audit logs shall be retained onsite for at least two (2) months after processing and thereafter archived in accordance with Section 5.5.2.

5.4.4 Protection of Audit Log

Audit logs are protected in accordance with Section 5.1.6.

5.4.5 Audit Log Backup Procedures

See Section 5.4.3.

5.4.6 Audit Collection System (Internal vs. External)

No stipulation.

5.4.7 Notification to Event-Causing Subject

Where an event is logged by the audit collection system, no notice is required to be given to the individual, organization, device, or application that caused the event.

5.4.8 Vulnerability Assessments

No Stipulation.

5.4.9 Archive Collection System (Internal or External)

No Stipulation.

5.4.10 Procedures to Obtain and Verify Archive Information

Only authorized Trusted Personnel are able to obtain access to the archive. The integrity of the information is verified when it is restored.

5.5 Records Archival

5.5.1 Types of Records Archived

DigiCert archives the following type of records:

- Certificate application information
- Documentation supporting certificate applications, including CAA results
- Certificate lifecycle information e.g., revocation, rekey and renewal application information

5.5.2 Retention Period for Archive

Records shall be retained for at least 7 years after any Certificate based on that documentation ceases to be valid.

5.5.3 Protection of Archive

DigiCert protects the archive so that only authorized Trusted Persons are able to obtain access to the archive. The archive is protected against unauthorized viewing, modification, deletion, or other tampering by storage within a Trustworthy System. The media holding the archive data and the applications required to process the archive data shall be maintained to ensure that the archive data can be accessed for the time period set forth in this CPS.

5.5.4 Archive Backup Procedures

No Stipulation.

5.5.5 Requirements for Time-Stamping of Records

Certificates, CRLs, and other revocation database entries shall contain time and date information. Such time information need not be cryptographic-based.

5.5.6 Archive Collection System (Internal or External)

No stipulation.

5.5.7 Procedures to Obtain and Verify Archive Information

Only authorized Trusted Personnel are able to obtain access to the archive. The integrity of the information is verified when it is restored.

5.6 Key Changeover

The GeoTrust CA key pairs are retired from service at the end of their respective lifetimes as defined in this CPS. GeoTrust CA Certificates may be renewed. New CA key pairs will be generated as necessary, for example to replace CA key pairs that are being retired, to supplement existing, active key pairs and to support new services.

When GeoTrust CA key pairs reach the end of their validity period, such CA key pairs will be archived for a period of at least 5 years. Archived CA key pairs will be securely stored using hardware cryptographic modules. Procedural controls will prevent archived CA key pairs from being returned to production use. Upon the end of the archive period, archived CA private keys will be securely destroyed.

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

GeoTrust Root CA key pair lifetimes
- Root 1 – Equifax Secure Certificate Authority: Expired Aug 22, 2018
- Root 2 – GeoTrust Global CA: Expires May 21, 2022
    - Root 3 – GeoTrust Universal CA: Expires March 04, 2029
    - Root 4 – Equifax Secure eBusiness CA-1: Expires Jun 21, 2020
    - Root 5 – Equifax Secure Global eBusiness CA-1: Expires Jun 21, 2020
    - Root 6 – GeoTrust Global CA2: Expires March 04, 2019
    - Root 7 – GeoTrust Universal CA2: Expires March 04, 2029
    - Root 8 – Equifax Secure eBusiness CA-2: Expires Jun 21, 2020
    - Root 9 – GeoTrust CA for Adobe: Expires 15 Jan 2015
    - Root 10 – GeoTrust Mobile Device Root – Unprivileged: Expires Jul 29 2023
    - Root 11 – GeoTrust Mobile Device Root – Privileged: Expires Jul 29 2023
    - Root 12 – GeoTrust CA for UTI: Expires 23 Jan 2024
    - Root 13 – GeoTrust True Credentials CA 2: Expires Jun 21, 2020
    - Root 14 – GeoTrust Primary Certification Authority: Expires July 16, 2036
    - Root 15 – GeoTrust Primary Certification Authority - G2: Expires January 18, 2038
    - Root 16 – GeoTrust Primary Certification Authority – G3: Expires December 1, 2037
    - Root 16 – GeoTrust Primary Certification Authority – G4: Expires December 1, 2037

New Roots and CAs created after publication of this CPS will have the following maximum validity periods:
- Self-signed Root CA Certificates: 25 years
- Intermediate CA Certificates: 15 years

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

Backup copies of essential business and CA information are made routinely. In general, back-ups are performed daily on-site and weekly to an off-site location, but may be performed less frequently in DigiCert's discretion according to production schedule requirements.

5.7.2 Computing Resources, Software, and/or Data are Corrupted

In the event of the corruption of computing resources, software, and/or data, such an occurrence is reported to DigiCert Security. Appropriate escalation, incident investigation, and incident response will ensue.

5.7.3 Entity Private Key Compromise Procedures

In the event of the Compromise of one or more of the GeoTrust Root Key(s) (including the CA Certificates), DigiCert shall promptly notify all Subscribers via e-mail and notify Relying Parties and others via the CRL and additional notice posted at digicert.com, and shall revoke all Certificates issued with such GeoTrust Root Key(s).

5.7.4 Business Continuity Capabilities after a Disaster

DigiCert 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.

DigiCert has developed a Disaster Recovery Plan (DRP) for its PKI services including the GeoTrust PKI service. The DRP identifies conditions for activating the plan and what constitutes an acceptable system outage and recovery time.

The DRP defines the procedures for the teams to maintain or reconstitute GeoTrust business operations following interruption to or failure of critical business processes by using backup data and backup copies of the GeoTrust keys. Specifically, DigiCert's DRP includes:
1. Emergency procedures,
2. Fallback procedures,
3. Resumption procedures,
4. Recovery time objective (RTO),
5. Frequency for taking backup copies of essential business information and software,
6. Requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location,
7. Separation distance of the Disaster recovery site to the CA's main site,
8. Procedures for securing the Disaster facility during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site,

DigiCert's DRP identifies administrative requirements including:
1. maintenance schedule for the plan;
2. Awareness and education requirements;
3. Responsibilities of the individuals; and
4. Regular testing of contingency plans.

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 DigiCert's disaster

recovery site, but may be performed less frequently in DigiCert's discretion according to production schedule requirements.

Additionally, for EV SSL Certificates, EV Code Signing, and Organization-validated and Domain-validated SSL Certificates, DigiCert's DRP meets the respective CA / Browser Forum requirements as set forth in the DigiCert CP and CPS.

5.8 CA or RA Termination

In the event that it is necessary for DigiCert or its CAs to cease operation, DigiCert 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, DigiCert 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 DigiCert,
- The preservation of the CA's archives and records for the time periods required in this CPS,
- The continuation of Subscriber and customer support services,
- The continuation of revocation services, such as the issuance of CRLs,
- The revocation of unexpired unrevoked Certificates of Subscribers and subordinate CAs, if necessary,
- The payment of compensation (if necessary) to Subscribers whose unexpired unrevoked Certificates are revoked under the termination plan or provision, or alternatively, the issuance of replacement Certificates by a successor CA,
- Disposition of the CA's Private Key and the hardware tokens containing such Private Key, and
- Provisions needed for the transition of the CA's services to a successor CA.

5.9 Data Security

For the issuance of EV SSL Certificates, EV Code Signing, and Organization-validated and Domain-validated SSL Certificates, DigiCert conforms to the respective CA / Browser Forum requirements for Data Security as set forth in the DigiCert CP and CPS.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

CA Key Pair generation is performed by multiple trained and trusted individuals using secure systems and processes that provide for the security and required cryptographic strength for the keys that are generated. The activities performed in each key generation ceremony are recorded, dated and signed by all individuals involved. These records are kept for audit and tracking purposes for a length of time deemed appropriate by DigiCert management.

At a minimum, the cryptographic modules used for key generation and storage meet the requirements of FIPS 140-2 level 3. The Root Keys for each CA Certificate are generated and are stored in hardware and are backed up but not escrowed. The Root Keys for each of the CA Certificates may be used for Certificate signing, CRL signing, and off-line CRL signing.

GeoTrust CA Key Pairs are maintained in a trusted and highly secured environment with backup and key recovery procedures.

6.1.2 Private Key Delivery to Subscriber

Not Applicable

6.1.3 Public Key Delivery to Certificate Issuer

End-user Subscribers and RAs submit their public key to DigiCertthrough the use of a PKCS#10 Certificate Signing Request (CSR) or other digitally signed package in a session secured by Transport Layer Security (TLS). Where CA, RA, or end-user Subscriber key pairs are generated by DigiCert, this requirement is not applicable.

6.1.4 CA Public Key Delivery to Relying Parties

DigiCert makes the CA Certificate available to Subscribers and Relying Parties through their inclusion in web browser software. For specific applications, the GeoTrust Public Keys are provided by the application vendors through the applications' root stores. DigiCert generally provides the full certificate chain (including the issuing CA Certificate and any CA Certificates in the chain) to the Subscriber upon Certificate issuance. GeoTrust CA Certificates may also be downloaded from *www.geotrust.com/resources*.

6.1.5 Key Sizes

Key pairs shall be of sufficient length to prevent others from determining the key pair's private key using cryptanalysis during the period of expected utilization of such key pairs. The current DigiCert Standard for minimum key sizes for its Roots and CAs is the use of key pairs equivalent in strength to 2048 bit RSA or higher.

DigiCert recommends that Registration Authorities and end-user Subscribers generate 2048 bit RSA key pairs. DigiCert will continue to approve end entity certificates generated with a key pair size of less than 2048 bit RSA, DSA, ECDSA within a selected group and closed system. GeoTrust CAs, RAs and end entity certificates use SHA-2 for digital signature hash. SHA-1 may be used to support legacy applications and use cases other than SSL and EV Code Signing provided that such usage does not violate procedures and policies set forth by the CA/Browser Forum and related Application Software Suppliers.

6.1.5.1 CABF Requirements for Key Sizes

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the respective CA /Browser Forum requirements as set forth in the DigiCert CP and CPS.

GeoTrust Root CA Certificates meet the following requirements for algorithm type and key size:

	Validity period beginning on or before 31 Dec 2010	Validity period beginning after 31 Dec 2010

Digest algorithm	MD5 Not Recommended, SHA-1, SHA-256, SHA-384 or SHA-512	SHA-1*, SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	2048**	2048
Minimum DSA modulus size (bits)	N/A	2048
ECC curve	NIST P-256, P-384 or P-521	NIST P-256, P-384 or P-521

Table 4A – Algorithms and key sizes for Root CA Certificates

GeoTrust Subordinate CA Certificates meet the following requirements for algorithm type and key size:

	Validity period beginning on or before 31 Dec 2010 and ending on or before 31 Dec 2013	Validity period beginning after 31 Dec 2010 or ending after 31 Dec 2013
Digest algorithm	SHA-1, SHA-256, SHA-384 or SHA-512	SHA-1*, SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	1024	2048
Minimum DSA modulus size (bits)	N/A	2048
ECC curve	NIST P-256, P-384 or P-521	NIST P-256, P-384 or P-521

Table 4B – Algorithms and key sizes for Subordinate CA Certificates

GeoTrust CAs shall only issue Subscriber certificates with keys containing the following algorithm types and key sizes.

	Validity period ending on or before 31 Dec 2013	Validity period ending after 31 Dec 2013
Digest algorithm	SHA-1*, SHA-256, SHA-384 or SHA-512	SHA-1*, SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	1024	2048
Minimum DSA modulus size (bits)	2048	2048
ECC curve	NIST P-256, P-384 or P-521	NIST P-256, P-384 or P-521

Table 4C – Algorithms and key sizes for Subscriber Certificates

* SHA-1 MAY be used with RSA keys in accordance with the criteria defined in Section 7.1.3 of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates and Mozilla Root Policy 2.5 or greater where applicable.

** A Root CA Certificate issued prior to 31 Dec 2010 with an RSA key size less than 2048 bits may still serve as a trust anchor Subscriber Certificates issued in accordance with these Requirements.

GeoTrust CAs shall reject a certificate request if the requested Public Key does meet the minimum algorithm key sizes set forth in this section.

6.1.6 Public Key Parameters Generation and Quality Checking

Not Applicable

6.1.7 Key Usage Purposes (as per x.509 v3 Key Usage Field)

Refer to section 7.1.2.1

6.2 Private Key Protection and Cryptographic Module Engineering Controls

DigiCert has implemented a combination of physical, logical, and procedural controls to ensure the security of GeoTrust CA private keys. DigiCert shall encrypt its Private Key with an algorithm and key-length that, according to the state of the art, are capable of withstanding cryptanalytic attacks for the residual life of the encrypted key or key part. Protection of the Private Key outside the validated cryptographic module must consist of physical security, encryption, or a combination of both, implemented in a manner that prevents disclosure of the Private Key. DigiCert shall implement physical and logical safeguards to prevent unauthorized certificate issuance.

Subscribers are required by contract to take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of private keys in accordance with section 4.5.1.

6.2.1 Cryptographic Module Standards and Controls

For issuing Root CA key pair generation and CA private key storage, DigiCert uses hardware cryptographic modules that, at a minimum, are certified at or meet the requirements of FIPS 140-1 Level 3.

6.2.2 Private Key (m of n) Multi-Person Control

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

The CA Private Key shall be backed up, stored, and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment.

6.2.3 Private Key Escrow

The Root Keys for each CA Certificate are backed up but not escrowed.

6.2.4 Private Key Backup

GeoTrust CA Key Pairs are maintained in a trusted and highly secured environment with backup procedures.

6.2.5 Private Key Archival

When GeoTrust CA Key Pairs reach the end of their validity period, such CA Key Pairs will be archived for a period of at least 5 years. Archived CA Key Pairs will be securely stored using offline media. Procedural controls will prevent archived CA Key Pairs from being returned to production use. Upon the end of the archive period, archived CA Private Keys will be securely destroyed.

6.2.6 Private Key Transfer Into or From Cryptographic Module

Private key transfer into or from a cryptographic module is performed in secure fashion in accordance to manufacturer guidelines for the module.

6.2.7 Private Key Storage on Cryptographic Module

Private key storage on cryptographic modules is secure in accordance to manufacturer guidelines for the module.

6.2.8 Method of Activating Private Key

All GeoTrust PKI Participants shall protect the activation data for their private keys against loss, theft, modification, unauthorized disclosure, or unauthorized use.

6.2.9 Method of Deactivating Private Key

GeoTrust RA private keys (used for authentication to the RA application) are deactivated upon system log off. GeoTrust RAs are required to log off their workstations when leaving their work area.

Subscribers have an obligation to adequately protect their private key(s).

6.2.10 Method of Destroying Private Key

Archived CA Key Pairs will be securely stored using offline media. Procedural controls will prevent archived CA Key Pairs from being returned to production use.

Cryptographic devices are physically destroyed or zeroized in accordance the manufacturers' guidance prior to disposal.

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

No stipulation.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

A Certificate's period of validity typically begins on the date the Certificate is issued (or such later date as specified in the Certificate), and ends on the date and time it expires as noted in the Certificate unless the Certificate is revoked before its expiration. The Operational Period for key pairs is the same as the Operational Period for the associated Certificates, except that they may continue to be used for decryption and signature verification.

6.3.2.1 CABF Validity Period and Validation Data Reuse Requirements

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the respective CA /Browser Forum requirements as set forth in the DigiCert CP and CPS.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

DigiCert RAs are required to select strong passwords to protect their private keys. Password selection guidelines require that system logon passwords:

• be generated by the user;
• have at least eight characters;
• have at least one alphabetic and one numeric character;
• have at least one lower-case letter;
• not contain many occurrences of the same character;
• not be the same as the operator's profile name; and
• not contain a long substring of the user's profile name.

6.4.2 Activation Data Protection

DigiCert shareholders are required to safeguard their Secret Shares and sign an agreement acknowledging their shareholder responsibilities.

DigiCert RAs are required to store their Administrator/RA private keys in encrypted form using password protection.

DigiCert strongly recommends that end-user Subscribers store their private keys in encrypted form and protect their private keys through the use of a hardware token and/or strong passphrase. The use of two factor authentication mechanisms (e.g., token and passphrase, biometric and token, or biometric and passphrase) is encouraged.

6.4.3 Other Aspects of Activation Data

6.4.3.1 Activation Data Transmission

To the extent activation data for private keys are transmitted, DigiCert CA Participants shall protect the transmission using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys. To the extent Windows or network logon user name/password combination is used as activation data for an end-user Subscriber, the passwords transferred across a network shall be protected against access by unauthorized users.

6.4.3.2 Activation Data Destruction

When applicable, activation data for CA private keys shall be decommissioned using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of the private keys protected by such activation data.

6.5 Computer Security Controls

DigiCert performs all CA and RA functions using Trustworthy Systems.

6.5.1 Specific Computer Security Technical Requirements

DigiCert requires the use of passwords that have a minimum character length and a combination of alphanumeric and special characters.

6.5.1.1 CABF Requirements for System Security

EV SSL Certificates, EV Code Signing, and domain validated and organization validated SSL Certificates conform to the respective CA /Browser Forum requirements as set forth in the DigiCert CP and CPS.

6.5.2 Computer Security Rating

No Stipulation

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

No Stipulation

6.6.2 Security Management Controls

No Stipulation

6.6.3 Life Cycle Security Controls

No Stipulation

6.7 Network Security Controls

CA and RA functions are performed using networks secured in accordance with the standards documented in the STN's confidential security policies (in the case of DigiCert and Affiliates) to prevent unauthorized access, tampering, and denial-of-service attacks. Communications of sensitive information are protected using point-to-point encryption for confidentiality and digital signatures for non-repudiation and authentication.

6.8 Time Stamping

Certificates, CRLs, and other revocation database entries shall contain time and date information. Such time information need not be cryptographic-based.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

GeoTrust Certificates generally conform to (a) ITU-T Recommendation X.509 (2005): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, August 2005, and (b) RFC *5280*: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, May 2008 ("RFC *5280*"). Certificate extensions and their criticality, as well as cryptographic algorithm object identifiers, are populated according to the IETF RFC*5280* standards and recommendations. As applicable to the Certificate type, GeoTrust Certificates conform to the current version of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates. Management may make exceptions to this policy on a case by case basis to mitigate material, imminent impacts to customers, partners, relying parties, and/or others within the certificate ecosystem where practical workarounds do not exist. Any such management exceptions are documented, tracked, and reported as part of the audit process.

The name forms for Subscribers are enforced through DigiCert'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. The policy constraints extensions and policy qualifiers syntax and semantics, when used, conform to the RFC *5280* standards.

EV Certificate content and profile requirements are discussed in Section 3 of Appendix B2 to this CPS.

7.1.1 Version Number(s)

CA certificates shall be X.509 Version 1 or Version 3 CA Certificates. End-user Subscriber Certificates shall be X.509 Version 3.

7.1.2 Certificate Extensions

7.1.2.1 Key Usage

X.509 Version 3 Certificates are generally populated in accordance with RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, May 2008. The criticality field of the *KeyUsage* extension is generally set to TRUE.

7.1.2.2 Certificate Policies Extension

CertificatePolicies extension of X.509 Version 3 Certificates are populated with the object identifier of this CPS in accordance with Section 7.1.6. The criticality field of this extension shall be set to FALSE.

CertificatePolicies extension for EV certificate is populated per Appendix B2 to this CPS.

7.1.2.2.1 CABF Requirement for Certificate Policies Extension

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the respective CA / Browser Forum requirements as set forth in the DigiCert CP and CPS.

7.1.2.3 Subject Alternative Names

The *subjectAltName* extension of X.509 Version 3 Certificates, when used, is populated in accordance with RFC 5280.

For all web server certificates, the SubjectAltName extension is populated with the authenticated value in the Common Name field of the subject DN (domain name or public iPAddress). The SubjectAltName extension may contain additional authenticated domain names or public iPAddresses. For internationalized domain names, the Common Name will be represented as a Unicode encoded U-label value designed for human comprehension and that Common Name will be represented in the Subject Alternative Name extension as a puny-coded A-label value designed for automated comprehension. These different encodings of the same name are treated as equal values for the purposes of Common Name to Subject Alternative Name duplication requirements.

7.1.2.4 Basic Constraints

GeoTrust X.509 Version 3 CA Certificates *BasicConstraints* extension shall have the CA field set to TRUE. End-user Subscriber Certificates *BasicConstraints* extension shall have the CA field set to FALSE. The criticality field of this extension shall be set to TRUE for CA Certificates, but may be set to TRUE or FALSE for end-user Subscriber Certificates.

GeoTrust X.509 Version 3 CA Certificates may have a "*pathLenConstraint*" field of the *BasicConstraints* extension set to the maximum number of CA certificates that may follow this Certificate in a certification path. End-user Subscriber certificates do not contain the path length constraint attribute.

7.1.2.5 Extended Key Usage

By default, *ExtendedKeyUsage* is set as a non-critical extension. Legacy GeoTrust CA Certificates may include the *ExtendedKeyUsage* extension as a form of technical constraint on the usage of certificates that they issue.

To explicitly comply with Microsoft Trusted Root Program Requirements section 4(A)(11) (http://aka.ms/rootcert), GeoTrust CA Certificates created after June 7, 2016 contain an EKU extension that includes at least the Server Authentication EKU and omits the Secure Email, Code Signing, and Time Stamping uses.

Subordinate CA Certificates created after January 1, 2019 for publicly trusted certificates, with the exception of cross-certificates that share a private key with a corresponding root certificate: will contain an EKU extension; and cannot include the anyExtendedKeyUsage KeyPurposeId; DigiCert no longer includes both the id-kp-serverAuth and id-kp-emailProtection KeyPurposeIds in the same certificate.

DigiCert's Technically Constrained Subordinate CA Certificates include an Extended Key Usage (EKU) extension specifying all extended key usages for which the Subordinate CA Certificate is authorized to issue certificates. The anyExtendedKeyUsage KeyPurposeId does not appear in the EKU extension of publicly trusted certificates.

Subscriber Certificates contain the *ExtendedKeyUsage* extension, aligning to Application Software Supplier granted trust bits and private PKI use cases. For certificates issued after February 1, 2017, all End-user Subscriber certificates contain an extended key usage for the purpose that the certificate was issued to the end user, and shall not contain the anyEKU value.

7.1.2.6 CRL Distribution Points

Most GeoTrust X.509 Version 3 end user Subscriber Certificates and CA Certificates include the *cRLDistributionPoints* extension containing the URL of the location where a Relying Party can obtain a CRL to check the Certificate's status.

7.1.2.7 Authority Key Identifier

DigiCert generally populates the Authority Key Identifier extension of X.509 Version 3 end user Subscriber Certificates and Intermediate CA Certificates.

7.1.2.8 Subject Key Identifier

Where DigiCert populates X.509 certificates with a *subjectKeyIdentifier* extension, the *keyIdentifier* is based on the public key of the Subject of the Certificate and is generated in accordance with one of the methods described in RFC *5280*.

7.1.3 Algorithm Object Identifiers

Cryptographic algorithm object identifiers, are populated according to the IETF RFC*5280* standards and recommendations.

7.1.4 Name Forms

DigiCert populates Certificates in accordance with Section 3.1.1. The Issuer Name shall be populated in each Certificate issued containing the Country, Organization Name and the Common Name of the Issuing CA.

7.1.5 Name Constraints

DigiCert may include name constraints in the nameConstraints field when appropriate.

7.1.6 Certificate Policy Object Identifier

The object identifier for the Certificate policy corresponding to the Certificate is set forth in Section 1.2. The *CertificatePolicies* extension in each X.509 Version 3 Certificate is populated in accordance with Section 1.2.

7.1.6.1 CABF Requirement for Certificate Policy Object identifier

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the respective CA / Browser Forum requirements as set forth in the DigiCert CP and CPS.

7.1.7 Usage of Policy Constraints Extension

No stipulation

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation

7.2 CRL Profile

As applicable to the Certificate type, corresponding CRLs conform to the current version of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.

7.2.1 Version Number(s)

GeoTrust supports both X.509 Version1 and Version 2 CRLs.

7.2.2 CRL and CRL Entry Extensions

No stipulation

7.3 OCSP Profile

OCSP (Online Certificate Status Protocol) is a way to obtain timely information about the revocation status of a particular certificate. DigiCert provides OCSP for checking certificate status requests.

OCSP responders conform to RFC 2560, RFC 5019, and RFC 6960, excluding client requested cipher support.

CABF Requirement for OCSP Signing

For EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates, DigiCert provides OCSP responses in conformity with the respective CA/Browser Forum requirements as set forth in the DigiCert CP and CPS.

7.3.1 Version Number(s)

Version 1 of the OCSP specification as defined by RFC2560, RFC 5019, and RFC 6960 are supported. RFC 6960 support excludes client requested ciphers.

7.3.2 OCSP Extensions

No Stipulation

8. Compliance Audit and Other Assessments

8.1 Frequency and Circumstances of Assessment

Compliance Audits are conducted at least annually. Audits are conducted over unbroken sequences of audit periods with each period no longer than one year duration. WebTrust "Principles and Criteria for Certification Authorities - Version 2.0" or later, and where applicable, WebTrust "Principles and Criteria for Certification Authorities – SSL Baseline with Network Security - Version 2.2" or later, WebTrust "Principles and Criteria for Certification Authorities -

Extended Validation SSL 1.4.5" or later and/or WebTrust Principles and Criteria for Certification Authorities - Extended Validation Code SigningWebTrust for Certification Authorities v2.0 or later examinations are performed.

CABF Requirement for Self-Audits
For EV SSL Certificates, EV Code Signing, and Organization-validated and Domain-validated SSL Certificates, DigiCert conducts self-audits in conformity with the respective CA/Browser Forum requirements as set forth in the DigiCert CP and CPS.

8.2 Identity/Qualifications of Assessor

DigiCert's CA compliance audits are performed by a public accounting firm that:
- Demonstrates proficiency in conducting the WebTrust for Certification Authorities v2.0 or later,
- Demonstrates proficiency in public key infrastructure technology, information security tools and techniques, security auditing, and the third-party attestation function,
- 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.
- Is bound by law, government regulation, or professional code of ethics; and
- Maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage.

8.3 Assessors Relationship to Assessed Entity

Compliance audits of DigiCert's operations are performed by a public accounting firm that is independent of DigiCert.

8.4 Topics Covered by Assessment

The scope of DigiCert's annual WebTrust for Certification Authorities v2.0 or later (or equivalent) audit includes CA environmental controls, key management operations and Infrastructure/ Administrative CA controls, certificate life cycle management and CA business practices disclosure.

8.5 Actions Taken as a Result of Deficiency

With respect to compliance audits of DigiCert's operations, significant exceptions or deficiencies identified during the Compliance Audit will result in a determination of actions to be taken. This determination is made by DigiCert management with input from the auditor. DigiCert management is responsible for developing and implementing a corrective action plan. If DigiCert determines that such exceptions or deficiencies pose an immediate threat to the security or integrity of the DigiCert CA, a corrective action plan will be developed and implemented within a commercially reasonable period of time. For less serious exceptions or deficiencies, DigiCert Management will evaluate the significance of such issues and determine the appropriate course of action.

8.6 Communications of Results

DigiCert makes its annual Audit Report publicly available no later than three (3) months after the end of the audit period. In the event of a delay greater than three months, DigiCert shall provide an explanatory letter signed by the Qualified Auditor. A copy of DigiCert's WebTrust for CA audit report can be found at from the DigiCert Website by clicking on the WebTrust Seal.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

DigiCert, is entitled to charge end-user Subscribers for the issuance, management, and renewal of Certificates.

9.1.2 Certificate Access Fees

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

9.1.3 Revocation or Status Information Access Fees

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

9.1.4 Fees for Other Services

DigiCert does not charge a fee for access to this CPS. Any use made for purposes other than simply viewing the document, such as reproduction, redistribution, modification, or creation of derivative works, shall be subject to a license agreement with the entity holding the copyright to the document.

9.1.5 Refund Policy

DigiCert's refund policy is available for review on the DigiCert and GeoTrust web sites at digicert.com/legal-repository, *www.geotrust.com/resources, www.RapidSSL.com/legal or www.FreeSSL.com/legal*. If a Subscriber has paid the fees for the Certificate to another party such as a reseller, the Subscriber should request the refund from that party.

In most cases, a Subscriber may apply a refund toward the issuance of a substitute Certificate. To obtain a substitute Certificate, the Subscriber must provide a new Certificate Signing Request ("CSR") to DigiCert or request reissue of a Certificate based upon a prior CSR previously provided to DigiCert by the Subscriber.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

DigiCert maintains commercial general liability insurance coverage.

9.2.2 Other Assets

Enterprise Customers shall have sufficient financial resources to maintain their operations and perform their duties, and they must be reasonably able to bear the risk of liability to Subscribers and Relying Parties.

9.2.3 Extended Warranty Coverage

The GeoSure Protection Plan is an extended warranty program that provides certain DigiCert certificate subscribers with protection against loss or damage that is due to a defect in DigiCert's issuance of the certificate or other malfeasance caused by DigiCert's negligence or breach of its contractual obligations, provided that the subscriber of the certificate has fulfilled its obligations under the applicable service agreement. For general information concerning the GeoSure Protection Plan, and a discussion of which Certificates are covered by it, see *www.geotrust.com/resources/cps/pdfs/GeoSure_Plan_v3.0.pdf*.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

Certain information regarding Subscribers that is submitted on enrolment forms for Certificates will be kept confidential by DigiCert (such as contact information for individuals and credit card information) and DigiCert shall not release such information without the prior consent of the Subscriber. Notwithstanding the foregoing, DigiCert may make such information available (a) to courts, law enforcement agencies or other third parties (including release in response to civil discovery) upon receipt of a court order or subpoena or upon the advice of DigiCert's legal counsel, (b) to law enforcement officials and others for the purpose of investigating suspected fraud, misrepresentation, unauthorized access, or potential illegal activity by the Subscriber in the opinion of DigiCert.

9.3.2 Information Not Within the Scope of Confidential Information

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

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

9.3.3 Responsibility to Protect Confidential Information

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

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

DigiCert has implemented a Privacy Statement, which is located at: digicert.com/legal-repository.

9.4.2 Information Treated as Private

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

9.4.3 Information Not Deemed Private

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

9.4.4 Responsibility to Protect Private Information

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

9.4.5 Notice and Consent to Use Private Information

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

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

DigiCert shall be entitled to disclose Confidential/Private Information if, in good faith, DigiCert believes that:
• disclosure is necessary in response to subpoenas and search warrants.
• disclosure is necessary in response to judicial, administrative, or other legal process during the discovery process in a civil or administrative action, such as subpoenas, interrogatories, requests for admission, and requests for production of documents.

This section is subject to applicable privacy laws.

9.4.7 Other Information Disclosure Circumstances

No Stipulation

9.5 Intellectual Property Rights

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

9.5.1 Property Rights in Certificates and Revocation Information

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

9.5.2 Property Rights in the CPS

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

9.5.3 Property Rights in Names

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

9.5.4 Property Rights in Keys and Key Material

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

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

DigiCert 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 DigiCert by the Applicant in all material respects; and (iii) it has taken reasonable steps to verify that the information within the Certificate is accurate (with the exception of True Credentials and True Credential Express Client Certificates). The nature of the steps DigiCert takes to verify the information contained in a Certificate is set forth in this CPS.

9.6.1.1 CABF Warranties and Obligations

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the respective CA / Browser Forum requirements as set forth in the DigiCert CP and CPS.

9.6.2 RA Representations and Warranties

RAs warrant that:
• There are no material misrepresentations of fact in the Certificate known or originating from the entities approving the Certificate Application or issuing the Certificate,

- There are no errors in the information in the Certificate that were introduced by entities approving the Certificate Application as a result of a failure to reasonable care in managing the Certificate Application,
- Their Certificates meet all material requirements of this CPS, and
- Revocation services (when applicable) and use of a repository comply with the applicable CPS in all material aspects.

Subscriber Agreements may include additional representations and warranties.

9.6.3 Subscriber Representations and Warranties

Subscribers warrant that:

- Each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the Subscriber and the Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created,
- Their private key is protected and that no unauthorized person has ever had access to the Subscriber's private key; further, the Subscriber shall immediately request revocation of a certificate if the related private key is compromised,
- All representations made by the Subscriber in the Certificate Application the Subscriber submitted are true,
- All information supplied by the Subscriber and contained in the Certificate is true,
- The Certificate is being used exclusively for authorized and legal purposes, consistent with this CPS, and
- The Subscriber is an end-user Subscriber and not a CA, and is not using the private key corresponding to any public key listed in the Certificate for purposes of digitally signing any Certificate (or any other format of certified public key) or CRL, as a CA or otherwise.

Subscriber Agreements may include additional representations and warranties.

9.6.4 Relying Party Representations and Warranties

Relying Parties acknowledge that they have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a Certificate, that they are solely responsible for deciding whether or not to rely on such information, and that they shall bear the legal consequences of their failure to perform the Relying Party obligations in terms of this CPS.

9.6.5 Representations and Warranties of Other Participants

No stipulation

9.7 Disclaimer of Warranties

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall disclaim DigiCert's possible warranties, including any warranty of merchantability or fitness for a particular purpose, outside the context of the GeoSure Protection Plan.

9.8 Limitation of Liability

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall disclaim DigiCert liability outside the context of the GeoSure Protection Plan. To the extent DigiCert has issued and managed the Certificate(s) at issue in compliance with its Certification Practice Statement, DigiCert shall have no liability to the Subscriber, any Relying Party, or any other third parties for any damages or losses suffered as a result of the use or reliance on such Certificate(s).

The liability (and/or limitation thereof) of Subscribers shall be as set forth in the applicable Subscriber agreements.

The liability (and/or limitation thereof) of enterprise RAs and the applicable CA shall be set out in the agreement(s) between them.

The liability (and/or limitation thereof) of Relying Parties shall be as set forth in the applicable Relying Party Agreements.

9.9 Indemnities

9.9.1 Indemnification by Subscribers

To the extent permitted by applicable law, Subscriber are required to indemnify DigiCert for:

• Falsehood or misrepresentation of fact by the Subscriber on the Subscriber's Certificate Application,
• Failure by the Subscriber to disclose a material fact on the Certificate Application, if the misrepresentation or omission was made negligently or with intent to deceive any party,
• The Subscriber's failure to protect the Subscriber's private key, to use a Trustworthy System, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's private key, or
• The Subscriber's use of a name (including without limitation within a common name, domain name, or e-mail address) that infringes upon the Intellectual Property Rights of a third party.

The applicable Subscriber Agreement may include additional indemnity obligations.

9.9.2 Indemnification by Relying Parties

To the extent permitted by applicable law, Relying Parties shall indemnify DigiCert for:

• The Relying Party's failure to perform the obligations of a Relying Party,
• The Relying Party's reliance on a Certificate that is not reasonable under the circumstances, or
• The Relying Party's failure to check the status of such Certificate to determine if the Certificate is expired or revoked.

9.9.3 Indemnification of Application Software Suppliers

Notwithstanding any limitations on its liability to Subscribers and Relying Parties, the CA understands and acknowledges that the Application Software Suppliers who have a Root Certificate distribution agreement in place with the GeoTrust Root CA do not assume any obligation or potential liability of the CA under these Requirements or that otherwise might exist because of the issuance or maintenance of Certificates or reliance thereon by Relying Parties or others.

Thus the CA shall defend, indemnify, and hold harmless each Application Software Supplier for any and all claims, damages, and losses suffered by such Application Software Supplier related to a Certificate issued by the CA, regardless of the cause of action or legal theory involved. This does not apply, however, to any claim, damages, or loss suffered by such Application Software Supplier related to a Certificate issued by the CA where such claim, damage, or loss was directly caused by such Application Software Supplier's software displaying as not trustworthy a Certificate that is still valid, or displaying as trustworthy: (1) a Certificate that has expired, or (2) a Certificate that has been revoked (but only in cases where the revocation status is currently available from the CA online, and the application software either failed to check such status or ignored an indication of revoked status).

9.10 Term and Termination

9.10.1 Term

The CPS becomes effective upon publication in the DigiCert repository. Amendments to this CPS become effective upon publication in the DigiCert repository.

9.10.2 Termination

This CPS as amended from time to time shall remain in force until it is replaced by a new version.

9.10.3 Effect of Termination and Survival

Upon termination of this CPS, GeoTrust PKI Participants are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

9.11 Individual Notices and Communications with Participants

Unless otherwise specified by agreement between the parties, GeoTrust PKI Participants shall use commercially reasonable methods to communicate with each other, taking into account the criticality and subject matter of the communication.

9.12 Amendments

9.12.1 Procedure for Amendment

DigiCert may change this CPS at any time without prior notice. The CPS and any amendments thereto are available through digicert.com/legal-repository. Amendments to this CPS will be evidenced by a new version number and date, except where the amendments are purely clerical.

9.12.2 Notification Mechanism and Period

No stipulation

9.12.2.1 Comment Period

Not applicable

9.12.2.2 Mechanism to Handle Comments

Not applicable

9.12.3 Circumstances under Which OID must be Changed

Not applicable

9.13 Dispute Resolution Provisions

9.13.1 Disputes among DigiCert, Affiliates and Customers

Disputes among GeoTrust PKI participants shall be resolved pursuant to provisions in the applicable agreements among the parties.

9.13.2 Disputes with End-User Subscribers or Relying Parties

Any dispute, controversy or claim arising under, in connection with or relating to this CPS or any Certificate issued by DigiCert 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 Utah County, Utah, United States of America. There shall be one arbitrator appointed by the AAA who shall exhibit a reasonable familiarity with the issues involved or presented in such dispute, controversy or claim. The award of the arbitrator shall be binding and final upon all parties, and judgment on the award may be entered by any court having proper jurisdiction thereof. This CPS and the rights and obligations of the parties hereunder and under any Certificate issued by DigiCert 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 attorney's fees actually incurred.

9.14 Governing Law

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

9.15 Compliance with Applicable Law

This CPS is subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information. DigiCert licenses its CAs in each jurisdiction that it operates where licensing is required by the law of such jurisdiction for the issuance of Certificates.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

Not Applicable

9.16.2 Assignment

Not Applicable

9.16.3 Severability

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

9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)

Not Applicable

9.16.5 Force Majeure

DigiCert 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 DigiCert.

9.17 Other Provisions

Not Applicable

Appendices

Appendix A:
Table of Acronyms and Definitions

Table of Acronyms

Term	Definition
AICPA	American Institute of Certified Public Accountants.
ANSI	The American National Standards Institute.
ACS	Authenticated Content Signing
BIS	The United States Bureau of Industry and Science of the United States Department of Commerce
CA	Certificate Authority
ccTLD	Country Code Top-Level Domain
CICA	Canadian Instituted of Chartered Accountants
CP	Certificate Policy
CPS	Certificate Practice Statement
CRL	Certificate Revocation List
DBA	Doing Business As
DCPA	DigiCert Policy Authority
DNS	Domain Name System
DV	Domain Validated (Certificate)
EAL	Evaluation Assurance Level
EV	Extended Validation
FIPS	United State Federal Information Processing Standards.
FQDN	Fully Qualified Domain Name
ICC	International Chamber of Commerce.
IM	Instant Messaging
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ISO	International Organization for Standardization
LSVA	Logical security vulnerability assessment.
NIST	(US Government) National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol.
OID	Object Identifier
OV	Organization Validated (Certificate)
PCA	Primary Certification Authority.
PIN	Personal identification number.
PKCS	Public-Key Cryptography Standard.
PKI	Public Key Infrastructure.
QGIS	Qualified Government Information Source
QIIS	Qualified Independent Information Source
RA	Registration Authority.
RFC	Request for comment.
S/MIME	Secure multipurpose Internet mail extensions.
SSL	Secure Sockets Layer.
TLD	Top-Level Domain
TLS	Transport Layer Security

Definitions

Term	Definition
Administrator	A Trusted Person within the organization that performs validation and other CA or RA Functions.
Administrator Certificate	A Certificate issued to an Administrator that may only be used to perform CA or RA functions.
Affiliate	A leading trusted third party, for example in the technology, telecommunications, or financial services industry, that has entered into an agreement with DigiCert as a distribution and services channel within a specific territory. In the CAB Forum context, the term "*Affiliate*" refers to: A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.
Applicant	The Private Organization or Government Entity that applies for (or seeks renewal of) an EV Certificate naming it as the Subject. The Applicant, its parent, affiliates, and subsidiaries are all considered interchangeable as Applicant.
Applicant Representative	An individual person employed by the Applicant for an EV certificate: (i) who signs and submits, or approves an EV Certificate Request on behalf of an Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of an Applicant.
Application Software Vendor	A developer of Internet browser software or other software that displays or uses certificates and distributes root certificates, such as KDE, Microsoft Corporation, Mozilla Corporation, Opera Software ASA, and Red Hat, Inc.
Attestation Letter	A letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information.
Audit Report	A report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the mandatory provisions of these Requirements.
Authorization Domain Name	The Domain Name used to obtain authorization for certificate issuance for a given FQDN. DigiCert may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. If the FQDN contains a wildcard character, then DigiCert removes all wildcard labels from the left most portion of requested FQDN. DigiCert may prune zero or more labels from left to right until encountering a Base Domain Name and may use any one of the intermediate values for the purpose of domain validation.
Authorized Port	One of the following ports: 80 (http), 443 (http), 115 (sftp), 25 (smtp), 22 (ssh).
Base Domain Name	The portion of an applied-for FQDN that is the first domain name node left of a registry-controlled or public suffix plus the registry-controlled or public suffix. For FQDNs where the right-most domain name node is a gTLD granted directly to one owner by ICANN specifications, the gTLD itself may be used as the Base Domain Name.
Certificate	A message that, at least, states a name or identifies the CA, identifies the Subscriber, contains the Subscriber's public key, identifies the Certificate's Operational Period, contains a Certificate serial number, and is digitally signed by the CA.
Certificate Applicant	An individual or organization that requests the issuance of a Certificate by a CA.
Certificate Application	A request from a Certificate Applicant (or authorized agent of the Certificate Applicant) to a CA for the issuance of a Certificate.
Certificate Approver	A Certificate Approver is a natural person who is employed by the Applicant, or an authorized agent who has express authority to represent the Applicant of an EV Certificate to (i) act as a Certificate Requester and to authorize other employees or third parties to act as a Certificate Requester, and (ii) to approve EV Certificate Requests submitted by other Certificate Requesters.
Certificate Chain	An ordered list of Certificates containing an end-user Subscriber Certificate and CA Certificates, which terminates in a root Certificate.
Certificate Data	Certificate requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA's possession or control or to which the CA has access.

Term	Definition
Certificate Management Control Objectives	Criteria that an entity must meet in order to satisfy a Compliance Audit.
Certificate Management Process	Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.
Certificate Policy	A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.
Certificate Problem Report	Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates
Certificate Requester	A Certificate Requester is a natural person who is employed and authorized by the Applicant, or an authorized agent who has express authority to represent the Applicant or a third party (such as an ISP or hosting company) that completes and submits an EV Certificate Request on behalf of the Applicant.
Certificate Revocation List (CRL)	A periodically (or exigently) issued list, digitally signed by a CA, of identified Certificates that have been revoked prior to their expiration dates in accordance with CP § 3.4. The list generally indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the revoked Certificates' serial numbers, and the specific times and reasons for revocation.
Certificate Signing Request	A message conveying a request to have a Certificate issued.
Certification Authority (CA)	An entity authorized to issue, manage, revoke, and renew Certificates.
Certificate Practices Statement (CPS)	A statement of the practices that DigiCert or an Affiliate employs in approving or rejecting Certificate Applications and issuing, managing, and revoking Certificates.
Challenge Phrase	A secret phrase chosen by a Certificate Applicant during enrolment for a Certificate. When issued a Certificate, the Certificate Applicant becomes a Subscriber and a CA or RA can use the Challenge Phrase to authenticate the Subscriber when the Subscriber seeks to revoke or renew the Subscriber's Certificate.
Class	A specified level of assurances as defined within the CP. See CP § 1.1.1.
Code Confirmation Certificate	A Certificate issued by DigiCert in order for DigiCert to use the associated Private Key to digitally resign enrollment form code which has been digitally signed by a Publisher Certificate Private Key, upon request of code confirmation from the Publisher.
Compromise	A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred. With respect to private keys, a Compromise is a loss, theft, disclosure, modification, unauthorized use, or other compromise of the security of such private key.
Confidential/Private Information	Information required to be kept confidential and private pursuant to CP § 2.8.1.
Contract Signer	A Contract Signer is a natural person who is employed by the Applicant, or an authorized the Applicant to sign Subscriber Agreements on behalf of the Applicant for an EV Certificate.
Country	A Country shall mean a Sovereign state as defined in the Guidelines.
Cross Certificate	A certificate that is used to establish a trust relationship between two Root CAs.
CRL Usage Agreement	An agreement setting forth the terms and conditions under which a CRL or the information in it can be used.
Delegated Third Party	A natural person or Legal Entity that is not the CA but is authorized by the CA to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.
Demand Deposit Account	A deposit account held at a bank or other financial institution, the funds deposited in which are payable on demand. The primary purpose of demand accounts is to facilitate cashless payments by means of check, bank draft, direct debit, electronic funds transfer, etc. Usage varies among countries, but a demand deposit account is commonly known as: a checking account, a share draft account, a current account, or a checking account.

Term	Definition
Domain Authorization	Correspondence or other documentation provided by a Domain Name Registrant attesting to the authority of an Applicant to request a Certificate for a specific Domain Namespace.
Domain Contact	The Domain Name Registrant, technical contact, or administrative "corporate" contact (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record.
Domain Name	The label assigned to a node in the Domain Name System.
Domain Namespace	The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.
Domain Name Registrant	Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.
Domain Name Registrar	A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).
Enterprise RA	An employee or agent of an organization unaffiliated with teh CA who authorizes issuance of Certificates to that organization.
Expiry Date	The "Not After" date in a Certificate that defines the end of a Certificate's validity period.
EV Certificate:	A digital certificate that contains information specified in the EV Guidelines and that has been validated in accordance with the Guidelines.
EV OID	An identifying number, called an "object identifier," that is included in the certificatePolicies field of an EV certificate that: (i) indicates which CA policy statement relates to that certificate, and which, (ii) by pre-agreement with one or more Application Software Vendor, marks the certificate as being an EV Certificate.
Exigent Audit/ Investigation	An audit or investigation by DigiCert where DigiCert has reason to believe that an entity's failure to meet DigiCert CA Standards, an incident or Compromise relating to the entity, or an actual or potential threat to the security of the DigiCert CA posed by the entity has occurred.
Extended Validation	Validation Procedures defined by the Guidelines for Extended Validation Certificates published by a forum consisting of major certification authorities and browser vendors.
Fully-Qualified Domain Name	A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.
Government Entity	A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).
Intellectual Property Rights	Rights under one or more of the following: any copyright, patent, trade secret, trademark, and any other intellectual property rights.
Intermediate Certification Authority (Intermediate CA)	A Certification Authority whose Certificate is located within a Certificate Chain between the A Certification Authority whose Certificate is located within a Certificate Chain between the end-user Subscriber's Certificate.
International Organization	An International Organization is an organization founded by a constituent document, e.g., charter, treaty, convention, or similar document, signed by, or on behalf of, a minimum of two or more Sovereign State governments.
Internal Server Name	A Server Name (which may or may not include an Unregistered Domain Name) that is not resolvable using the public DNS.
Issuing CA	In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.
Key Compromise	A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, an unauthorized person has had access to it, or there exists a practical technique by which an unauthorized person may discover its value.
Key Generation Ceremony	A procedure whereby a CA's or RA's key pair is generated, its private key is transferred into a cryptographic module, its private key is backed up, and/or its public key is certified.
Key Generation Script	A documented plan of procedures for the generation of a CA Key Pair.

Term	Definition
Key Pair	The Private Key and its associated Public Key.
Legal Entity	An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.
Nonverified Subscriber Information	Information submitted by a Certificate Applicant to a CA or RA, and included within a Certificate, that has not been confirmed by the CA or RA and for which the applicable CA and RA provide no assurances other than that the information was submitted by the Certificate Applicant.
Non-repudiation	An attribute of a communication that provides protection against a party to a communication falsely denying its origin, denying that it was submitted, or denying its delivery. Denial of origin includes the denial that a communication originated from the same source as a sequence of one or more prior messages, even if the identity associated with the sender is unknown. Note: only an adjudication by a court, arbitration panel, or other tribunal can ultimately prevent repudiation. For example, a digital signature verified with reference to a DigiCert Certificate may provide proof in support of a determination of Non-repudiation by a tribunal, but does not by itself constitute Non-repudiation.
Object Identifier	A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.
OCSP (Online Certificate Status Protocol)	An online Certificate-checking protocol for providing Relying Parties with real-time Certificate status information.
OCSP Responder	An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.
Offline CA	DigiCert PCAs, Issuing Root CAs and other designated intermediate CAs that are maintained offline for security reasons in order to protect them from possible attacks by intruders by way of the network. These CAs do not directly sign end user Subscriber Certificates.
Online CA	CAs that sign end user Subscriber Certificates are maintained online so as to provide continuous signing services.
Online Certificate Status Protocol (OCSP)	A protocol for providing Relying Parties with real-time Certificate status information.
Operational Period	The period starting with the date and time a Certificate is issued (or on a later date and time certain if stated in the Certificate) and ending with the date and time on which the Certificate expires or is earlier revoked.
Parent Company	A parent company is defined as a company that owns a majority of the Subsidiary Company and this can be verified by referencing a QIIS or from financial statement supplied by a registered Chartered Professional Accountant (CPA) or equivalent outside of the USA.
PKCS #10	Public-Key Cryptography Standard #10, developed by RSA Security Inc., which defines a structure for a Certificate Signing Request.
PKCS #12	Public-Key Cryptography Standard #12, developed by RSA Security Inc., which defines a secure means for the transfer of private keys.
Primary Certification Authority (PCA)	A CA that acts as a root CA for a specific Class of Certificates, and issues Certificates to CAs subordinate to it.
Principal Individual(s)	Individuals of a Private Organization, Government Entity or Business Entity that are either owners, partners, managing members, directors or officers, as identified by their title of employment, or an employee, contractor or agent authorized by such entity or organization to conduct business related to the request, issuance and use of EV Certificates.
Private Key	The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.
Public Key	The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

Term	Definition
Public Key Infrastructure	The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based public key cryptographic system.
Publicly-Trusted Certificate	A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software.
Qualified Auditor	A natural person or Legal Entity that meets the requirements of Section 17.6 (Auditor Qualifications).
Random Value	A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy.
Registered Domain Name	A Domain Name that has been registered with a Domain Name Registrar.
Registration Agency	A Governmental Agency that registers business information in connection with an entity's business formation or authorization to conduct business under a license, charter or other certification. A Registration Agency MAY include, but is not limited (i) a State Department of Corporations or a Secretary of State; (ii) a licensing agency, such as a State Department of Insurance; or (iii) a chartering agency, such as a state office or department of financial regulation, banking or finance, or a federal agency such as the Comptroller of Currency (OCC) or Office of Thrift Supervision (OTC).
Registration Authority (RA)	An entity approved by a CA to assist Certificate Applicants in applying for Certificates, and to approve or reject Certificate Applications, revoke Certificates, or renew Certificates.
Regulated Financial Institution	A financial institution that is regulated, supervised, and examined by governmental, national, state or provincial, or local authorities having regulatory authority over such financial institution based on the governmental, national, state or provincial, or local laws under which such financial institution was organized and/or licensed.
Reliable Method of Communication	A method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative.
Relying Party	An individual or organization that acts in reliance on a certificate and/or a digital signature.
Relying Party Agreement	An agreement used by a CA setting forth the terms and conditions under which an individual or organization acts as a Relying Party.
Repository	An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.
Request Token	A value derived in a method specified by the CA which binds this demonstration of control to the certificate request. The Request Token incorporates the key used in the certificate request. A Request Token may include a timestamp to indicate when it was created. A Request Token may include other information to ensure its uniqueness. A Request Token that includes a timestamp remains valid for no more than 30 days from the time of creation. A Request Token that includes a timestamp is treated as invalid if its timestamp is in the future. A Request Token that does not include a timestamp is valid for a single use and DigiCert does not re-use it for a subsequent validation. The binding uses a digital signature algorithm or a cryptographic hash algorithm at least as strong as that to be used in signing the certificate request.
Reseller	An entity marketing services on behalf of DigiCert or an Affiliate to specific markets.
Reserved IP Address	An IPv4 or IPv6 address that the IANA has marked as reserved: http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml
Root CA	The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.
Root Certificate	The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.
RSA	A public key cryptographic system invented by Rivest, Shamir, and Adelman.
RSA Secure Server Certification Authority (RSA Secure Server CA)	The Certification Authority that issues Secure Server IDs.
RSA Secure Server Hierarchy	The PKI hierarchy comprised of the RSA Secure Server Certification Authority.

Term	Definition
Secret Share	A portion of a CA private key or a portion of the activation data needed to operate a CA private key under a Secret Sharing arrangement.
Secret Sharing	The practice of splitting a CA private key or the activation data to operate a CA private key in order to enforce multi-person control over CA private key operations under CP § 6.2.2.
Secure Server ID	A Class 3 organizational Certificate used to support SSL sessions between web browsers and web servers.
Secure Sockets Layer (SSL)	The industry-standard method for protecting Web communications developed by Netscape Communications Corporation. The SSL security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a Transmission Control Protocol/Internet Protocol connection.
Sovereign State	A Sovereign state is a state, or country, that administers its own government, and is not dependent upon, or subject to, another power.
Subject	The holder of a private key corresponding to a public key. The term "Subject" can, in the case of an organizational Certificate, refer to the equipment or device that holds a private key. A Subject is assigned an unambiguous name, which is bound to the public key contained in the Subject's Certificate.
Subject Identity Information	Information that identifies the Certificate Subject. Subject Identity Information does not include a domain name listed in the *subjectAltName* extension or the Subject *commonName* field.
Subordinate CA	A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.
Subscriber	In the case of an individual Certificate, a person who is the Subject of, and has been issued, a Certificate. In the case of an organizational Certificate, an organization that owns the equipment or device that is the Subject of, and that has been issued, a Certificate. A Subscriber is capable of using, and is authorized to use, the private key that corresponds to the public key listed in the Certificate.
Subscriber Agreement	An agreement used by a CA or RA setting forth the terms and conditions under which an individual or organization acts as a Subscriber.
Subsidiary Company	A subsidiary company is defined as a company that is majority owned by Applicant as verified by referencing a QIIS or from financial statement supplied by a registered Chartered Professional Accountant (CPA) or equivalent outside of the USA.
Terms of Use	Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with these Requirements when the Applicant/Subscriber is an Affiliate of the CA.
Test Certificate	A Certificate with a maximum validity period of 30 days and which: (i) includes a critical extension with the specified Test Certificate CABF OID, or (ii) is issued under a CA where there are no certificate paths/chains to a root certificate subject to these Requirements.
Trusted Person	An employee, contractor, or consultant of an entity within DigiCert responsible for managing infrastructural trustworthiness of the entity, its products, its services, its facilities, and/or its practices as further defined in CP § 5.2.1.
Trusted Position	The positions within DigiCert that must be held by a Trusted Person.
Trustworthy System	Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy. A trustworthy system is not necessarily a "trusted system" as recognized in classified government nomenclature.
Unregistered Domain Name	A Domain Name that is not a Registered Domain Name.
Valid Certificate	A Certificate that passes the validation procedure specified in RFC 5280.
Validation Specialists	Someone who performs the information verification duties specified by these Requirements.
Validity Period	The period of time measured from the date when the Certificate is issued until the Expiry Date.
Wildcard Certificate	A Certificate containing an asterisk (*) in the left-most position of any of the Subject Fully-Qualified Domain Names contained in the Certificate.

Appendix B1: Minimum Cryptographic Algorithm and Key Sizes for EV Certificates

Minimum Cryptographic Algorithm and Key Sizes for EV Certificates

1. **Root CA Certificates**

	Key Sizes
Digest algorithm	SHA1*, SHA-256, SHA-384 or SHA-512
RSA	2048
ECC	256 or 384

2. **Subordinate CA Certificates**

	Key Sizes
Digest algorithm	SHA1*, SHA-256, SHA-384 or SHA-512
RSA	2048
ECC	256 or 384

3. **Subscriber Certificates**

	Key Sizes
Digest algorithm	SHA1*, SHA-256, SHA-384 or SHA-512
RSA	2048
ECC	256 or 384

* SHA-1 MAY be used with RSA keys in accordance with the criteria defined in Section 7.1.3 of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.

Appendix B2:
EV Certificates Required Certificate Extensions

EV Certificates Required Certificate Extensions

1. Root CA Certificate

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

(a) basicConstraints

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

(b) keyUsage

If the certificate is v3 and is created after October 2006, this extension MUST be present and MUST be marked critical. Bit positions for CertSign and cRLSign MUST be set. If the Root CA Private Key is used for signing OCSP responses, then the digitalSignature bit MUST be set.

(c) certificatePolicies

This extension SHOULD NOT be present.

(d) extendedKeyUsage

This extension is not present.

All other fields and extensions are set in accordance to RFC *5280*.

2. Subordinate CA Certificate

(a) certificatePolicies

MUST be present and SHOULD NOT be marked critical. The set of policy identifiers MUST include the identifier for the CA's EV policy.

certificatePolicies:policyIdentifier (Required)
- the ***anyPolicy*** if subordinate CA is controlled by DigiCert

(b) cRLDistributionPoint

is always present and NOT marked critical. It contains the HTTP URL of the CA's CRL service.

(c) authorityInformationAccess

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

(d) basicConstraints

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

(e) keyUsage
This extension MUST be present and MUST be marked critical. Bit positions for *CertSign* and *cRLSign* MUST be set. If the Subordinate CA Private Key is used for signing OCSP responses, then the digitalSignature bit MUST be set.

All other fields and extensions MUST BE set in accordance to RFC *5280*.

3. Subscriber Certificate

(a) certificate Policies
MUST be present and SHOULD NOT be marked critical. The set of policyIdentifiers MUST include the identifier for DigiCert's or GeoTrust's EV policy.

certificatePolicies:policyIdentifier (Required)
- EV policy OID

certificatePolicies:policyQualifiers:policyQualifierId (Required)
- id-qt 2 [RFC *5280*]

certificatePolicies:policyQualifiers:qualifier (Required)
- URI to the Certificate Practice Statement

(b) cRLDistributionPoint
is always present and NOT marked critical. It contains the HTTP URL of the applicable GeoTrust / DigiCert CRL service.

(c) authorityInformationAccess
is always present and NOT marked critical. SHALL contain the HTTP URL of the OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1).

An HTTP accessMethod MAY be included for the CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2).

(d) basicConstraints (optional)
If present, the CA field MUST be set false.

(e) keyUsage (optional)
If present, bit positions for *CertSign* and *cRLSign* MUST NOT be set.

(f) extKeyUsage
Either the *value id-kp-serverAuth* [RFC5280] or *id-kp-clientAuth* [RFC5280] or both values MUST be present. Other values SHOULD NOT be present.

(g) SubjectAltName (optional)
If present is populated in accordance with RFC5280 and criticality is set to FALSE.

All other fields and extensions set in accordance to RFC *5280*.

Appendix B3:
Foreign Organization Name Guidelines

Foreign Organization Name Guidelines

NOTE: This appendix is only relevant to EV applications from countries that do not have Latin character organization name registrations. More specific information for particular countries may be added to this appendix in the future.

Where an EV Applicant's organization name is not registered with a QGIS in Latin characters and the applicant's foreign character organization name and registration have been verified with a QGIS in accordance with these Guidelines, DigiCert MAY include a Latin character organization name in the EV certificate. In such a case, DigiCert will follow the procedures laid down in this appendix.

Romanized Names
In order to include a transliteration/Romanization of the registered name, the Romanization will be verified by DigiCert using a system officially recognized by the Government in the Applicant's jurisdiction of incorporation.

If DigiCert cannot rely on a transliteration/Romanization of the registered name using a system officially recognized by the Government in the Applicant's jurisdiction of incorporation, then it MUST rely on one of the options below, in order of preference:

- A system recognized by the International Standards Organization (ISO),
- A system recognized by the United Nations or
- A Lawyer's Opinion confirming the Romanization of the registered name.

English Name
In order to include a Latin character name that is not a Romanization of the registered name in the EV certificate, DigiCert will verify that the Latin character name is:

- Included in the Articles of Incorporation (or equivalent document) filed as part of the organization registration, or
- Recognized by a QGTIS in the Applicant's Jurisdiction of Incorporation as the applicant's recognized name for tax filings, or
- Confirmed with a QIIS to be the name associated with the registered organization, or
- Confirmed by a lawyer's opinion letter to be the trading name associated with the registered organization.

Country Specific Procedures
F-1. Japan
In addition to the procedures set out above:

- The Hepburn method of Romanization is acceptable for Japanese Romanizations.
- DigiCert MAY verify the Romanized transliteration of Applicant's formal legal name with either a QIIS or a lawyer's opinion letter.
- DigiCert MAY use the Financial Services Agency to verify an English Name. When used, DigiCert will verify that the English name is recorded in the audited Financial Statements filed with the Financial Services Agency.

- When relying on Articles of Incorporation to verify an English Name, the Articles of Incorporation MUST be accompanied either: by a document, signed with the original Japanese Corporate Stamp, that proves that the Articles of Incorporation are authentic and current, or by a lawyer's opinion letter. DigiCert will verify the authenticity of the Corporate Stamp.