DigiCert

Certification Practice s Statement for GeoTrust and RapidSSL

Version 1. 4

Effective Date: March 18, 2019

DigiCert, Inc.
2801 N. Thanksgiving Way
Suite 500
Lehi, UT 84043
USA
Tel: 1-801-877-2100
Fax: 1-801-705-0481
www.digicert.com

Revision date: March 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 address size to 64 bits.

appropriate repository to check Certificate status a

1. INTRODUCTION

This document is the DigiCert Certification Practices Statement for GeoTrust and RapidSSL ("CPS"). It states the practices that DigiCert's

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

1.4.2 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 Informati on

DigiCert

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 Authenti cation

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 Subscribe rs

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).

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. DigiCert, however, 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 must 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 requirement 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

Certificate Type	*Additional Procedures*
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 DnTc 0.001 Tw 9.311 0 Tdd [(3)-0.9 tnamatt9.305 0-0.9 ( )06 (1 T2.Tj EMC /P <</a)5.1 (t9.3

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,

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

4.6 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 Reques6.8 (y)11.1 ( )4)(he)0.5 l y 4g 4 (uan1y)11.l-2.1 (ho3p22)]TJ 0drer5. Td ( )TjT 1 Tf 0.0.6 (C)-1.

4.7.2 Who May Request Certification of a New Public Key

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

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

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 CPSCr6 (S)3.3 w (-)Tj 0.001 Tc1-1.9 (ma)- -0.00- 0 Td [(f)0329 (ma)-

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 R equest 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 U7.

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 ren.3 [Trno or

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.

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.

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

5.5.2 Retention Period for Archive

Records shall be retained for at least 7 y

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 e event tubscrectedR2 (s)1.4 0.5 (ng)2ice to ba8dresiarIn t7dR2

- 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,

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

6.2.10 Method of Destroying Private Key

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

6.6.3 Life Cycle Security Controls

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-

7.1.6 Certificate Policy O bject 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 Polic y 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)

N i o . 6 1 7

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

8.4 Topics Covered by Assessment

The scope of DigiCert

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

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 Propert y 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-ьser Subscribers that are the respective Subjects o5fon5.3 and su Tc 03.230 Tc 0 (ehnd)0.6pe(o4)1.7 (s

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

• 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

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 Notifio onpudure marocnrgodTw 12.581 06.6 [(r)-1.MC /P <</MCID 3 >>BDC5 /TT2 1 Tf 0.002 Tc -0.003 Tw 0.

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 La w

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

Appendi ces

Appendix A :

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,

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.

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

Term

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 (e t)-5.1 (ha07 (e C7 (n,w [(c)-3 (om)-32 490.4)-1 a533.3 (i

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 orSHA-512
RSA	2048
ECC	256 or384

2. Subordinate CA Certificates

	Key Sizes
Digest algorithm	SHA1*, SHA-256, SHA-384 or SHA512
RSA	2048
ECC	256 or384

3. Subscriber Certificates

	Key Sizes
Digest algorithm	SHA1*, SHA-256, SHA-384 orSHA-512
RSA	2048
ECC	256 or384

*

Appendix B2:

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 (7 (ar)-7 (zat)-1.7 (S r)2.7 (eF)(

- 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.