DigiCert

Certification Practices Statement for Symantec Trust Network (STN)

Version 3.9
September 11, 2018

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

Table of Contents

Change History Table

Version	Changes made
3.1	

Version	Changes made
3.8.16	Added language to specifically include STN CAs managed by Symantec Japan Inc. in the definition of ‘Symantec’s Sub-domain’. Added reference to legacy certificates’ Organizational names. Incorporated the modification for Class 3 Organizational certificates recently approved for the Symantec Japan CPS (now merged with this CPS). Removed ‘Symantec-owned’ and added note regarding DRF for Symantec Japan

1. INTRODUCTION

This document is the DigiCert Certification Practices Statement for Symantec Trust Network (STN) (“CPS”). It states the practices that DigiCert certification authorities (“CAs”) employ in providing certification services that include, but are not limited to, issuing, managing, revoking, and renewing certificates in accordance with the specific requirements of the DigiCert Certificate Policy for Symantec Trust Network (“CP”).

The CP is the principal statement of policy governing the STN. It establishes the business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing, digital Certificates within the STN and providing associated trust services. These requirements, called the “STN Standards,” protect the security and integrity of the STN, apply to all STN Participants, and thereby provide assurances of uniform trust throughout the STN. More information concerning the STN and STN Standards is available in the CP.

DigiCert has authority over a portion of the STN called its “Sub-domain” of the STN. DigiCert’s Sub-domain includes entities subordinate to it such as its Customers, Subscribers, and Relying Parties.

While the CP sets forth requirements that STN Participants must meet, this CPS describes how DigiCert meets these requirements within DigiCert’s Sub-domain of the STN. More specifically, this CPS describes the practices that DigiCert employs for:

securely managing the core infrastructure that supports the STN, and
issuing, managing, revoking, and renewing STN Certificates

within DigiCert’s Sub-domain of the STN, in accordance with the requirements of the CP and its STN Standards.

This CPS conforms to the Internet Engineering Task Force (IETF) RFC 3647 for Certificate Policy and Certification Practice Statement construction. CAs within the Symantec Trust Network hierarchy 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 Requirements, those Requirements take precedence over this document.

At this time, DigiCert-issued, Symantec-branded Extended Validation (EV) SSL certificates, Extended Validation (EV) Code-Signing certificates and Domain-Validated (DV) and Organization-Validated (OV) SSL Certificates[1] issued by DigiCert CAs under this CP conform with the CABF Requirements. Such DV and OV certificates are issued containing the corresponding policy identifier(s) specified in section 1.2 of the CP indicating adherence to and conformance with these requirements. DigiCert CAs assert that all Certificates issued containing these policy identifier(s) are issued and managed in conformance with the CABF Requirements.

[1] Additionally, DigiCert issues organizational Client (non-SSL) certificates that are not subject to the CA Browser Forum Baseline Requirements. In addition to practices pertaining exclusively to the CA Browser Forum (ie, for OV SSL certificates), this CPS describes practices that pertain to any Class 2 or Class 3 certificate that is issued to an organization and contains organization information. Such certificates are r

Management may make exceptions to this policy on a case-by-case

STN Class of Certificate as listed in section 1.2 of the STN CP. Therefore, DigiCert has not assigned this CPS an object identifier value. Certificate Policy Object Identifiers are used in accordance with Section 7.1.6.

Domain-validated and organization-validated SSL Certificates contain the corresponding OID value in section 1.2 of the STN CP that indicates adherence to and compliance with the CA / Browser Forum Baseline Requirements.

1.3 PKI Participants

1.3.1 Certification Authorities

The term Certification Authority (CA) is an umbrella term that refers to all entities authorized to issue public key certificates within the STN. The CA term encompasses a subcategory of issuers called Primary Certification Authorities (PCA). PCAs act as roots of four domains[5], one for each class of Certificate. Each PCA is a DigiCert entity. Subordinate to the PCAs are Certification Authorities that issue Certificates to end-user Subscribers or other CAs.

DigiCert also operates the Symantec Class 3 Internal Administrator CA hierarchy that is limited to DigiCert internal administrative uses.

DigiCert also operates the “Symantec Universal Root Certification Authority” and the “Symantec ECC Universal Root Certification Authority”. The Universal Root CAs issue Class 3 and selected Class 2 Subordinate CAs.

DigiCert enterprise customers may operate their own CAs as subordinate CAs to a public STN PCA. Such a customer enters into a contractual relationship with DigiCert to abide by all the requirements of the STN CP and the STN CPS. These subordinate CAs may, however implement more restrictive practices based on their internal requirements.

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 certificates on behalf of a STN 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.

Third parties, who enter into a contractual relationship with DigiCert, may operate their own RA and authorize the issuance of certificates by a STN CA based on initial and periodically renewed validation by DigiCert compliant with CA/Browser Forum data reuse rules. Third party Ras must abide by all the requirements of the STN CP, the STN CPS and the terms of their enterprise services agreement with DigiCert. RAs may, however implement more restrictive practices based on their internal requirements.[6]

1.3.3 Subscribers

Subscribers under the STN include all end users (including entities) of certificates issued by a STN 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.

[5] Class 4 certificates are not currently issued by the STN.

[6] An example of a third party RA is a customer of Managed PKI services customer.

1.4.1.2 Certificates Issued to Organizations

Organizational Certificates are issued to organizations after authentication that the Organization legally exists and that other Organization attributes included in the certificate (excluding non-verified subscriber information) are authenticated e.g. ownership of an Internet or e-mail domain. It is not the intent of this CPS to limit the types of usages for Organizational Certificates. While the most common usages are included in Table 2 below, an Organizational Certificate may be used for other purposes, provided that a Relying Party is able to reasonably rely on that certificate and the usage is not otherwise prohibited by law, by the STN CP, by any CPS under which the certificate has been issued and any agreements with Subscribers.

High assurance with extended validation certificates are Class 3 certificates issued by DigiCert in conformance with the Guidelines for Extended Validation Certificates.

1.4.2 Prohibited Certificate Uses

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.

DigiCert 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. Also, Class 1 Certificates shall not be used as proof of identity or as support of non-repudiation of identity or authority. Client Certificates are intended for client applications and shall not be used as server or organizational Certificates.

CA Certificates may not be used for any functions except CA functions. In addition, end-user Subscriber Certificates shall not be used as CA Certificates.

The STN and its Participants do not issue any certificate that can be used for man-in-the-middle (MITM) or traffic management of domain names or IP addresses that the certificate holder does not legitimately own or control. Such certificate usage is expressly prohibited.

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. DigiCert recommends the use of PCA Roots 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

DigiCert's Public Primary Certification Authorities (PCAs) and DigiCert Infrastructure/Administrative CAs supporting the STN, and
DigiCert's CAs and Enterprise Customers' CAs that issue Certificates within DigiCert's Sub-domain of the STN.

DigiCert publishes the STN CP, this CPS, Subscriber Agreements, and Relying Party Agreements in the repository section of DigiCert's web site.

2.3 Time or Frequency of Publication

Updates to this CPS are published in accordance with Section 9.12. Updates to Subscriber Agreements and Relying Party Agreements are published as necessary. CA information is published promptly after it is made available to the CA. The STN offers CRLs showing the revocation of STN Certificates and offers status checking services through the DigiCert Repository and Affiliates' repositories. 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. CRLs for Authenticated Content Signing (ACS) Root CAs are published 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.

2.4 Access Controls on Repositories

Information published in the repository portion of the DigiCert web site is publicly-accessible information. Read-only access to such information is unrestricted. DigiCert requires persons to agree to a Relying Party Agreement as a condition to accessing Certificates, Certificate status information, or CRLs. DigiCert has implemented logical and physical security measures to prevent unauthorized persons from adding, deleting, or modifying repository entries. DigiCert and Affiliates make their repositories publicly available in a read-only manner, and specifically at the link stated in section 1.5.4 or specified in an Affiliate's CPS.

3. Identification and Authentication

3.1 Naming

Attribute	Value
Country (C) =	2-letter ISO country code or not used.
Organization (O) =	“DigiCert Inc”, “Symantec Corporation”, or <organization name>[8]

[redacted]

Attribute

3.1.1.1 CABF Naming Requirements

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the CA / Browser Forum requirements as set forth in the STN Supplemental Procedures, Appendix B1, Appendix C and Appendix D, respectively.

3.1.2 Need for Names to be Meaningful

Class 2 and 3 end-user Subscriber Certificates contain names with commonly understood semantics permitting the determination of the identity of the individual or organization that is the

3.2.2 Authentication of Organization Identity and Domain Control

Whenever a certificate contains an organization name, the identity of the organization and other enrollment information provided by Certificate Applicants (except for Non-verified Subscriber Information) is confirmed in accordance with the procedures set forth in set forth in section 3.2.2 of the DigiCert Certificate Policy and in the DigiCert Certification Practices Statement, version 4.14, or higher, available at https://www.digicert.com/CPS.

At a minimum DigiCert shall:

> Determine that the organization exists by using at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable government agency or competent authority that confirms the existence of the organization as per the requirements in the DigiCert CP section 3.2,

Certificate Class	Authentication of Identity
	information within the email, to then proceed with accessing a portal with the unique information sent in the email, to download and install the certificate.
Class 2	Authenticate identity by: ƒ Manual check performed by the enterprise administrator customer for each subscriber requesting a certificate, “in which the subscriber receives the certificate via an email sent to the address provided during enrollment” or ƒ Passcode-based authentic

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.

Whenever an individual's name is associated with an Organization name in a certificate in such a way to indicate the individual's affiliation or authorization to act on behalf of the Organization the DigiCert or a RA:

determines that the Organization exists by using at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable government that confirms the existence of the organization, and

Uses information contained in the business records or databases of business information (employee or customer directories) of an RA approving certificates to its own affiliated individuals or confirms by telephone, confirmatory postal mail, or comparable procedure to the organization, the employment with the Organization of the individual submitting the Certificate Application and, when appropriate, his/her authority to act on behalf of the Organization.

3.2.6 Criteria for Interoperation

No stipulation.

3.3 Identification and Authentication for Re-key Requests

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to obtain a new certificate to maintain continuity of Certificate usage. DigiCert generally requires that the Subscriber generate a new key pair to replace the expiring key pair (technically defined as "rekey") However, in certain cases (i.e., for web server certificates) Subscribers may request a new certificate for an existing key pair (technically defined as "renewal").

Generally speaking, both "Rekey" and "Renewal" are commonly described as "Certificate Renewal", focusing on the fact that the old Certificate is being replaced with a new Certificate and not emphasizing whether or not a new key pair is generated. For all Classes and Types of STN Certificates, except for Class 3 Server Certificates, this distinction is not important as a new key pair is always generated as part of DigiCert's end-user Subscriber Certificate replacement process. However, for Class 3 Server Certificates, because the Subscriber key pair is generated on the web server and most web server key generation tools permit the creation of a new Certificate Request for an existing key pair, there is a distinction between "rekey" and "renewal."

3.3.1 Identification and Authentication for Routine Re-key

Re-key procedures ensure that te) ‘
t h e N
o !

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.2.2 Approval or Rejection of Certificate Applications

DigiCert or an RA will approve an application for a certificate

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

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Conduct constituting Acceptance of a 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

Certificate rekey is the application for the issuance of a new certificate that certifies the new public key. Certificate rekey is supported for all certificate Classes.

The affiliation between an organization that is a Subscriber of a Class 3 Organizational ASB Certificate and the organizational representative controlling the Subscriber’s private key is terminated or has otherwise ended,

DigiCert or a Customer has reason to believe that the Certificate was issued in a manner not materially in accordance with the procedures required by the applicable CPS, the Certificate (other than a Class 1 Certificate) was issued to a person other than the one named as the Subject of the Certificate, or the Certificate (other than a Class 1 Certificate) was issued without the authorization of the person named as the Subject of such Certificate,

DigiCert or a Customer has reason to believe that a material fact in the Certificate Application is false,

DigiCert or a Customer determines that a material prerequisite to Certificate Issuance was neither satisfied nor waived,

In the case of Class 3 organizational Certificates, the Subscriber’s organization name changes,

The information within the Certificate, other than Non-verified Subscriber Information, is incorrect or has changed,

The Subscriber identity has not been successfully re-verified in accordance with section 6.3.2,

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 the STN participant indicating that the certificate was used to sign malware

The Subscriber has not submitted payment when due, or

The continued use of that certificate is harmful to the STN.

When considering whether certificate usage is harmful to the ST ¶ ofThe Subr ɲ ro s ✕ l M ɔ l D T 7 0

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 CA / Browser Forum requirements as set forth in the STN Supplemental Procedures, Appendix B1, Appendix C and Appendix D, respectively.

4.9.2 Who Can Request Revocation

Individual Subscribers can request the revocation of their own individual Certificates through an authorized representative of DigiCert or an RA. In the case of organizational Certificates, a duly authorized representative of the organization shall be entitled to request the revocation of Certificates issued to the organization. A duly authorized representative of DigiCert or a RA shall be entitled to request the revocation of an RA Administrator’s Certificate. The entity that approved a Subscriber’s Certificate Application shall also be entitled to revoke or request the revocation of the Subscriber’s Certificate.

Regarding code signing certificates, DigiCert and Affiliates that issue code signing certificates provide Anti-Malware Organizations, Subscribers, Relying Parties, Application Software Suppliers, and other third parties with clear instructions on how they can report suspected Private Key ! ¾struc#_
₴oest t th l Mᴱ er ӽ ing had p ^ t ÿ anṃ ᴀ ɓ ɔ M

Where an Enterprise Customer initiates revocation of an end-use

4.9.7 CRL Issuance Frequency

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

DigiCert uses commercially reasonable efforts to notify potential Relying Parties if it discovers, or have reason to believe, that there has been a Compromise of the private key of one of their own CAs or one of the CAs within their sub-domains.

4.9.13 Circumstances for Suspension

Not applicable.

4.9.14 Who Can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The Status of public certificates is available via CRL at DigiCert’s website and via an OCSP responder (where available).

4.10.2 Service Availability

Certificate Status Services are available 24 U7 without scheduled interruption.

Certificate status services for EV SSL Certificates, EV Code Signing, and Organization-validated ©er Fqrum reqÈireyents as s¾ m M

OCSP is a3 oN® ʊ ᴀ ɿ ꝑ ꝁ M T m ꝑ m ᴀ ¡ servif

4.11 End of Subscription

Not disclose or allow to be disclosed escrowed keys or escrowed key-related information to any third party unless required by the law, government rule, or regulation; by the enterprise's organization policy; or by order of a court of competent jurisdiction.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Private keys are stored in the Key Manager database in encrypted form. Each Subscriber's private key is individually encrypted with its own triple-DES symmetric key. A Key Escrow Record (KER) is generated then the triple-DES key is combined with a r biometrics. Online CSUs are protected through the use of locked cabinets. Offline CSUs are protected through the use of locked safes, cabinets and containers. Access to CSUs and keying material is restricted in accordance with DigiCert's segregation of duties requirements. The opening and closing of cabinets or containers in these tiers is logged for audit purposes.

5.1.3 Power and Air Conditioning

DigiCert's secure facilities are equipped with primary and backup:

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

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 within DigiCert facilities or in a secure off-site storage facility with appropriate physical and logical access controls designed to limit access to authorized personnel and protect such media from accidental damage (e.g., water

Trusted Persons include, but are not limited to:

- customer service personnel, with the exception of technical support analysts in some facilities,
- cryptographic business operations personnel,
- security personnel,
- system administration personnel,
- designated engineering personnel with production system access, and
- executives that are designated to manage infrastructural trustworthiness.

DigiCert considers the categorie

the validation of information in Certificate Applications;
the acceptance, rejection, or other processing of Certificate Applications, revocation requests, key recovery requests or renewal requests, or enrollment information;
the issuance of Certificates, including personnel having access to restricted portions of the repository;
the handling of Subscriber information or requests
the generation, issuing or destruction of a CA certificate
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, qu] 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

DigiCert provides its personnel with training upon hire as well as the requisite on-the-job training needed for them to perform their job responsibilities competently and satisfactorily. DigiCert maintains records of such training. DigiCert periodically reviews and enhances its training programs as necessary.

DigiCert's training programs are tailored to the individual's responsibilities and include the following as relevant:

Basic PKI concepts,
Job responsibilities,
DigiCert security and operational policies and procedures,
Use and operation of deployed hardware and software,
Incident and Compromise reporting and handling, and
Disaster recovery and business continuity procedures.

5.3.3.1 CABF Requirements for Training and Skill Level

For EV SSL Certificates, EV Code Signing, and Organization-validated and Domain-validated SSL Certificates, personnel training is provided as set forth in the STN Supplemental Procedures, Appendix B1, Appendix C and Appendix D, respectively.

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

No stipulation

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 § 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 manually or automatically logs the following significant events:

5.4.2 Frequency of Processing Log

The CA system is continuously monitored to provide real time alerts of significant security and operational events for review by designated system security personnel. Monthly reviews of the audit logs include verifying that the logs have not been tampered with and thoroughly investigating any alerts or irregularities detected in the logs. Actions taken based on audit log reviews are also documented.

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 with an electronic audit log system that includes mechanisms to protect the log files from unauthorized viewing, modification, deletion, or other tampering.

5.4.5 Audit Log Backup Procedures

5.5.2 Retention Period for Archive

Records shall be retained for at least the time periods set forth below following the date the Certificate expires or is revoked.

Five (5) years for Class 1 Certificates,
Ten (10) years and six (6) months for Class 2 and Class 3 Certificates

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

DigiCert incrementally backs up electronic archives of its issued Certificate information on a daily basis. Copies of paper-based records shall be maintained in an off-site secure facility.

The Superior CA continues to issue CRLs signed with the original Superior CA private key until the expiration date of the last Certificate issued using the original key pair has been reached

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

Backups of the following CA information shall be kept in off-site storage and made available in the event of a Compromise or disaster: Certificate Application data, audit data, and database records for all Certificates issued. Back-ups of CA private keys shall be generated and maintained in accordance with CP § 6.2.4. DigiCert maintains backups of the foregoing CA information for their own CAs, as well as the CAs of Enterprise Customers within its Sub-domain.

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 and DigiCert's incident handling procedures are enacted. Such procedures require appropriate escalation, incident investigation, and incident response. If necessary, DigiCert's key compromise or disaster recovery procedures will be enacted.

5.7.3 Entity Private Key Compromise Procedures

Upon the suspected or known Compromise of a STN CA, DigiCert infrastructure or Customer CA private key, DigiCert's Key Compromise Response procedures are enacted by the Incident Response Team. This team assesses the situation, develops an action plan, and implements the action plan with approval from DigiCert executive management.

If CA Certificate revocation is required, the following procedures are performed:

> The Certificate's revoked status is communicated to Relying Parties through the DigiCert Repository in accordan

forth in the STN Supplemental Procedures, Appendix B1, Appendix C and Appendix D, respectively.

The target recovery time for restoring critical Production service functionality is no greater than 24 hours.

DigiCert conducts at least one disaster recovery test per calendar year to ensure functionality of services at the DRF. Formal Business Continuity Exercises are also conducted yearly where procedures for additional types of scenarios (e.g. pandemic, earthquake, flood, power outage) are tested and evaluated.

DigiCert takes significant steps to develop, maintain, and test sound business recovery plans, and DigiCert's planning for a disaster or significant business disruption is consistent with many of the best practices established within the industry.

DigiCert maintains redundant hardware and backups of its CA and infrastructure system software at its disaster recovery facility. In addition, CA private keys are backed up and maintained for disaster recovery purposes in accordance with CPS § 6.2.4.

DigiCert maintains offsite backups of important CA information for STN CAs as well as the CAs of Service Centers, and Enterprise Customers, within DigiCert's Sub-domain. Such information includes, but is not limited to: Certificate Application data, audit data (per Section 4.5), and database records for all Certificates issued.

5.8 CA or RA Termination

In the event that it is necessary for a STN CA, or Enterprise Customer CA 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 and, in the case of a Customer CA, the applicable Customer, will develop a termination plan to minimize disruption to Customers, 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, Relying Parties, and Customers, 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 or the maintenance of online status checking services,

The revocation of unexpired unrevoked Certificates of end-user Subscribers and subordinate CAs, if necessary,

Refunding (if necessary) 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 CA / Browser Forum requirements for Data Security as set forth in the STN Supplemental Procedures, Appendix B1, Appendix C and Appendix D, respectively.

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 pre-selected, trained and trusted individuals using Trustworthy Systems and processes that provide for the security and required cryptographic strength for the generated keys. For PCA and Issuing Root CAs, the cryptographic modules used for key generation meet the requirements of FIPS 140-2 level 3. For other CAs (including STN CAs and Managed PKI Customer CAs), the cryptographic modules used meet the requirements of at least FIPS 140-2 level 2.

communicated to the RA or end-user Subscriber using an out of band process. The distribution of such devices is logged by DigiCert.

Where end-user Subscriber key pairs are pre-generated by Enterprise Customers on hardware tokens or smart cards, such devices are distributed to the end-user Subscriber using a commercial delivery service and tamper evident packaging. The required activation data required to activate the device is communicated to the RA or end-user Subscriber using an out of band process. The distribution of such devices is logged by the Enterprise Customer.

For Enterprise Customers using Managed PKI Key Manager for key recovery services, the Customer may generate encryption key pairs (on behalf of Subscribers whose Certificate Applications they approve) and transmit such key pairs to Subscribers via a password protected PKCS #12 file.

SSL/TLS and S/MIME email signature certificates are not distributed as PKCS#12 packages. S/MIME encryption certificates may be distributed as PKCS#12 packages using secure channels and sufficiently secure passwords sent out of band from the package.

6.1.3 Public Key Delivery to Certificate Issuer

End-user Subscribers and RAs submit their public key to DigiCert for certification electronically through the use of a PKCS#10 Certificate Signing Request (CSR) or other digitally signed package in a session secured by Secure Sockets Layer (SSL). 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 Certificates for its PCAs and root CAs available to Subscribers and Relying Parties through their inclusion in web browser software. As new PCA and root CA Certificates are generated, DigiCert provides such new Certific ¾ ertificateb" dβac ! w Cæy p® ḫ Ă 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 CA /Browser Forum requirements as set forth in the STN Supplemental Procedures, Appendix B1, Appendix C and Appendix D, respectively[15].

DigiCert 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 9 – Algorithms and key sizes for Root CA Certificates

DigiCert 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)	2048	2048
ECC curve	NIST P-256, P-384 or P-521	NIST P-256, P-384 or P-521

Table 10 – Algorithms and key sizes for Subordinate CA Certificates

DigiCert 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 11 – Algorithms and key sizes for Subscriber Certificates

[15] STN certificates that have a non-standard key pair and key length size of less than 2048bit are authorized to be used within a selected group or closed eco system.

* 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.

DigiCert CAs reserve the right to reject a certificate request if the requested Public Key does not 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 DigiCert and Enterprise Customer CA private keys. Subscribers are required by contract to take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of private keys.

6.2.1 Cryptographic Module Standards and Controls

For PCA and Issuing Root CA key pair generation and CA private key storage, DigiCert uses hardware cryptographic modules that are certified at or meet the requirements of FIPS 140-2 Level 3. DigiCert recommends that enterprise RA Customers perform all Automated Administration RA cryptographic operations on a cryptographic module rated at least FIPS 140-2 level 2.

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

DigiCert has implemented technical and procedural mechanisms that require the participation of multiple trusted individuals to perform sensitive CA cryptographic operations. DigiCert uses

6.2.4 Private Key Backup

DigiCert creates backup copies of CA private keys for routine recovery and disaster recovery

6.2.8.2 Class 2 Certificates

The Standard for Class 2 Private Key protection is for Subscribers to:

Use a password in accordance with Section 6.4.1 or security of equivalent strength to authenticate the Subscriber before the activation of the private key, which includes, for instance, a password to operate the private key, or a Windows logon or screen saver password; and

Take commercially reasonable measures for the physical protection of the Subscriber's workstation to prevent use of the workstation and its associated private key without the Subscriber's authorization.

When deactivated, private keys shall be kept in encrypted form only.

6.2.8.3 Class 3 Certificates other than Administrator Certificates

The Standard for Class 3 private key protection (other than Administrators) requires Subscribers to:

Use a smart card, biometric access device or security of equivalent strength to authenticate the Subscriber before the activation of the private key; and

Take commercially reasonable measures for the physical protection of the Subscriber's workstation to prevent use of the workstation and its associated private key without the Subscriber's authorization.

Use of a password along with a smart card or biometric access device in accordance with Section 6.4.1 is recommended. When deactivated, private keys shall be kept in encrypted form only.

DigiCert obtains a representation from the Subscriber that the Subscriber will use one of the following options to generate and protect their Code Signing Certificate private keys:

1. A Trusted Platform Module (TPM) that generates and secures a key pair and that can document the Subscriber's private key protection through a TPM key attestation.
2. A hardware crypto module with a unit design form factor certified as conforming to at least FIPS 140 Level 2, Common Criteria EAL 4+, or equivalent.
3. Another type of hardware storage token with a unit design form factor of SD Card or USB token (not necessarily certified as conformant with FIPS 140 Level 2 or Common Criteria EAL 4+). The Subscriber MUST also warrant that it will keep the token physically separate from the device that hosts the code signing function until a signing session is begun.

DigiCert recommends that the Subscriber protect Private Keys using the method described in (1) or (2) over the method described in (3) and obligates the Subscriber to protect Private Keys in accordance with Section 10.3.2(2) in the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates

Symantec Secure App Service (SAS) ensures that a Subscriber's private key is generated, stored, and used in a secure environment that has controls to prevent theft or misuse. SAS enforces multi-factor authentication to access and authorize Code Signing and obtain a representation from the Subscriber that they will securely store the tokens required for multi-factor access. SAS systems used to host a Signing Service are not used for web browsing, run a
regu Ď

iv ^ te

means to ensure the complete destruction of CA private keys. When performed, CA key destruction activities are witnessed. The private key associated with an ACS Application ID is deleted immediately after it has been used for code signing.

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

STN CA, RA and end-user Subscriber Certificates are backed up and archived as part of DigiCert's routine backup procedures.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The Operational Period of a Certificate ends upon its expiration or revocation. 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. The maximum Operational Periods for DigiCert Certificates for Certificates issued on or after the effective date of this CPS are set forth in Table 12 below[16]. End user Subscriber Certificates that are renewals of existing subscriber certificates may have a longer validity period (up to 3 months).

In addition, STN CAs stop issuing new Certificates at an appropriate date (60 days plus maximum validity period of issu

Except as noted in this section, DigiCert sub-domain participants shall cease all use of their key pairs after their usage periods have expired.

Certificates issued by CAs to end-user Subscribers may have Operational Periods longer than three years, up to six years, if the following requirements are met:

RAs are required to store their Administrator/RA private keys in encrypted form using password protection and their browser’

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 CA /Browser Forum requirements as set forth in the STN Supplemental Procedures, Appendix B1, Appendix C and Appendix D, respectively.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

Applications are developed and implemented by DigiCert in accordance with DigiCert systems development and change management standards. DigiCert also provides software to its Enterprise Customers for performing RA and certain CA functions. Such software is developed in accordance with DigiCert system development standards.

DigiCert developed software, when first loaded, provides a method to verify that the software on the system originated from DigiCert, has not been modified prior to installation, and is the version intended for use.

6.6.2 Security Management Controls

DigiCert has mechanisms and/or policies in place to control and monitor the configuration of its CA systems. DigiCert creates a hash of all software packages and DigiCert software updates. This hash is used to verify the integrity of such software manually. Upon installation and daily thereafter, DigiCert validates the integrity of its CA systems.

6.6.3 Life Cycle Security Controls

No stipulation

6.7 Network Security Controls

DigiCert protects its communications of sensitive information through the use of encryption and digital signatures.

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

DigiCert 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”)[21]. As applicable to the Certificate type, STN 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 consensus emerges, the non-Repudiation bit might not be meaningful for potential Relying Parties. Moreover, the most commonly used applications do not always respect the non-Repudiation bit. Therefore, setting the bit might not help Relying Parties make a trust decision. Consequently, this CPS does not require that the non-Repudiation bit be set. It may be set in the case of dual key pair signature Certificates issued through Managed PKI Key Manager, or as otherwise requested. Any dispute relating to non-repudiation arising from the use of a digital certificate is a matter solely between the Subscriber and the Relying Party(s). DigiCert shall incur no liability in relation thereto.

7.1.2.2 Certificate Policies Extension

The *CertificatePolicies* extension of X.509 Version 3 Certificates are populated with the object identifier for the STN CP in accordance with CP Section 7.1.6 and with policy qualifiers set forth in CP Section 7.1.8. The criticality field of this extension shall be set to FALSE.

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 CA / Browser Forum requirements as set forth in the STN Supplemental Procedures, Appendix B1, Appendix C, and Appendix D, respectively.

7.1.2.3 Subject Alternative Names

The *subjectAltName* extension of X.509 Version 3 Certificates are populated in accordance with RFC 5280 with the exception of those issued under Public Lite accounts which may optionally exclude the email address in *SubjectAltName*. The criticality field of this extension shall be set to FALSE.

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
cer S ʊ Ӥ̈́é " e ᴘ ɇ ! a matem- cer ᵀ ʝ M l ℶ ɣ M

7.1.2.5 Extended Key Usage

By default, *ExtendedKeyUsage* is set as a non-critical extension. STN CA Certificates may include the *ExtendedKeyUsage* extension as a form of technical constraint on the usage of certificates that they issue. DigiCert Certificates may contain the *ExtendedKeyUsage* extension, aligning to Application Software Supplier granted trust bits and private PKI use cases. For certificates issued after Febr

7.1.4 Name Forms

DigiCert populates STN Certificates with an Issuer Name and Subject Distinguished Name 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 Issuer CA.

In addition, DigiCert may include within end-user Subscriber Certificates an additional Organizational Unit field that contains a notice stating that the terms of use of the Certificate are set forth in a URL which is a pointer to the applicable Relying Party Agreement. This OU must appear if a pointer to the applicable Relying Party Agreement is not included in the policy extension of the certificate.

7.1.5 Name Constraints

No stipulation

7.1.6 Certificate Policy Object Identifier

Where the Certificate Policies extension is used, Certificates contain the object identifier for the Certificate Policy corresponding to the appropriate Class of Certificate as set forth in the STN CP Section 1.2. For legacy Certificates issued prior to the publication of the STN CP which include the Certificate Policies extension, Certificates refer to the STN CPS.

7.1.6.1 CABF Requirements for Certificate Policy Object Identifier

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the CA / Browser Forum requirements as set forth in the STN Supplemental Procedures, Appendix B1, Appendix C and Appendix D, respectively.

7.1.7 Usage of Policy Constraints Extension

No stipulation

7.1.8 Policy Qualifiers Syntax and Semantics

DigiCert generally populates X.509 Version 3 STN Certificates with a policy qualifier within the Certificate Policies extension. Generally, such Certificates contain a CPS pointer qualifier that points to the applicable Relying Party Agreement or the STN CPS. In addition, some Certificates

Field	Value or Value constraint
Version	See Section 7.2.1.
Signature Algorithm	Algorithm used to sign the CRL in accordance with RFC 3279. (See CPS § 7.1.3)
Issuer	Entity who has signed and issued the CRL.
Effective Date	Issue date of the CRL. CRLs are effective upon issuance.
Next Update	Date by which the next CRL will be issued. CRL issuance frequency is in

Criteria for Certification Authorities - Extended Validation Code Signing examination is performed for DigiCert's data center operations and key management operations supporting DigiCert's public and Managed PKI CA services including the STN Root CAs, Class 3 Organizational CAs, Class 2 Organizational and Individual CAs, and Class 1 Individual CAs specified in Section 1.3.1. The external audit scheme of DigiCert Japan's public CAs is ISAE3402/SSAE16 instead of WebTrust for Certification Authorities. DigiCert shall be entitled to require that Enterprise Customers undergo a compliance audit under this CPS and audit programs for these types of Customers.

In addition to compliance audits, DigiCert shall be entitled to perform other reviews and investigations to ensure the trustworthiness of DigiCert's Sub-domain of the STN, which include, but are not limited to:

A "Security and Practices Review" of an Affiliate before it is permitted to begin operations. A Security and Practices Review consists of a review of an Affiliate's secure facility, security documents, CPS, STN-related agreements, privacy policy, and validation plans to ensure that the Affiliate meets STN Standards. DigiCert does not delegate domain or IP address validation to Affiliates or any delegated third parties.

DigiCert shall be entitled, within its sole and exclusive discretion, to perform at any time an "Exigent Audit/Investigation" on itself, an Affiliate, or an Enterprise Customer in the event DigiCert has reason to believe that the audited entity ha

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 Assessor's 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 (or equivalent) audit includes CA environmental controls, key management operations and Infrastructure/Administrative CA controls, certificate life cycle management and CA business practices disclosure.

Audits of RAs (Class 1-2)

Enterprise customers approving Class 1 and 2 certificates may undergo an annual compliance audit. Upon request from DigiCert and/or a Superior Entity (if the Superior Entity is not DigiCert), Enterprise customers may undergo an audit noting any exceptions or irregularities to STN policies and the steps taken to remedy the irregularities.

Audit of an RA (Class 3)

Enterprise Customers authorizing the issuance of Class 3 certificates undergo an annual compliance audit of their obligations under the STN.[24] Upon request from DigiCert and/or a Superior Entity (if the Superior Entity is not DigiCert) Enterprise Customers undergo an audit noting any exceptions or irregularities to STN policies and the steps taken to remedy the irregularities.

Audit of DigiCert or an Affiliate (Class 1-3)

DigiCert and each Affiliate is audited pursuant to the guidelines provided in the American Institute of Certificate Public Accounts' Statement on Service Organizations Control (SOC) Reports on the risks associated with Service Organizations. Their Compliance Audits are the WebTrust for Certification Authorities audit or an equivalent audit standard approved by DigiCert which includes: A Report of Policies and Procedures in Operation and Test of Operational Effectiveness.

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 STN, a corrective action plan will be developed within 30 days and implemented

[24] DigiCert performs identification and authentication of Class 3 SSL certificates authorized for issuance by Enterprise Customers.

the certificate. To request a refund, please call customer service at +1 801-701-9600. This refund policy is not an exclusive remedy and does not limit other remedies that may be available to subscribers.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

Enterprise Customers are encouraged to maintain a commercially reasonable level of insurance coverage for errors and omissions, either through an errors and omissions insurance program with an insurance carrier or a self-insured retention. DigiCert maintains such errors and omissions insurance coverage.

9.2.2 Other Assets

Enterprise Customers shall hav

9.3.3 Responsibility to Protect Confidential Information

Symantec 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 Policy, which is located at: *https://www.digicert.com/digicert-privacy-policy/*, in compliance with CP § 9.4.1.

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

DigiCert and Affiliates secure private information from compromise and disclosure to third parties and complies 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 Policy 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 DigiCert Sub-domain Participants other than Subscribers and Relying Parties is governed by the applicable agreements among such DigiCert Sub-domain 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 and that use of Certificates is subject to the Relying Party Agreement referenced in the Certificate. DigiCert and Customers shall grant permission to use revocation information to perform Relying Party functions subject to the applicable CRL Usag

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 CA / Browser Forum requirements as set forth in the STN Supplemental Procedures, Appendix B1, Appendix C, and Appendix D, respectively.

9.6.2 RA Representations and Warranties

RAs warrant that:

> There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate,
>
> There are no errors in the info

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 Party Agreements shall require Relying Parties to 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.

The applicable Relying Party Agreement may include additional indemnity obligations.

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 DigiCert 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 sua ̦ ꞵ ꞇ ꓫ ꞁ b b direcŎM ξ ӿ Ɛ ı c ! ˁ
Ɣ e]̦ ꞇ ᵐ ı N l] at ` tir]ꞇ ¶ ed to a Cb i]ꞇ γ ꞵ ᵐ Ӛ ξ ᴀ R edamah

9.11 Individual Notices and Communications with Participants

Unless otherwise specified by agreement between the parties, DigiCert Sub-domain 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

Amendments to this CPS may be made by the DigiCert Policy Authority (DCPA). Amendments shall either be in the form of a document containing an amended form of the CPS or an update. Amended versions or updates shall be linked to the Policies and Agreements section of the DigiCert Repository located at: *https://www.digicert.com/legal-repository/* and for an interim period, available at *https://www.websecurity.symantec.com/legal/repository#PoliciesAndAgreements*. Updates supersede any designated or conflicting provisions of the referenced version of the CPS. The DCPA shall determine whether changes to the CPS require a change in the Certificate policy object identifiers of the Certificate policies corresponding to each Class of Certificate.

9.12.2 Notification Mechanism and Period

DigiCert and the DCPA reserve the right to amend the CPS without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URLs, and changes to contact information. The DCPA's decision to designate amendments as material or non-material shall be within the DCPA's sole discretion

The DCPA solicits proposed amendments to the CPS from other DigiCert Sub-domain participants. If the DCPA considers such an amendment desirable and proposes to implement the amendment, the DCPA shall provi

Repository. Unless proposed amendments are amended or withdrawn, they shall become effective upon the expiration of the comment period.

9.12.3 Circumstances under Which OID Must be Changed

If the DCPA determines that a change is necessary in the object identifier corresponding to a Certificate policy, the amendment shall contain new object identifiers for the Certificate policies corresponding to each Class of Certificate. Otherwise, amendments shall not require a change in Certificate policy object identifier.

9.13 Dispute Resolution Provisions

9.13.1 Disputes among DigiCert, Affiliates, and Customers

Disputes among DigiCert Sub-domain 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

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall contain a dispute resolution clause. Disputes involving DigiCert require an initial negotiation period of sixty (60) days followed by litigation in the federal or state court encompassing Utah County, Utah, in the case of claimants who are U.S. residents, or, in the case of all other claimants, arbitration administered by the International Chamber of Commerce (“ICC”) in accordance with the ICC Rules of Conciliation and Arbitration, unless otherwise approved by DigiCert.

9.14 Governing Law

Subject to any limits appearing in applicable law, the laws of the State of Utah, U.S.A., shall govern the enforceability, construction, interpretation, and validity of this CPS, irrespective of contract or other choice of law provisions and without the requirement to establish a commercial nexus in Utah, USA. This choice of law is made to ensure uniform procedures and interpretation for all STN Participants, no matter where they are located.

This governing law provision applies only to this CPS. Agreements incorporating the CPS by reference may have their own governing law provisions, provided that this Section 9.14 governs the enforceability, construction, interpretation, and validity of the terms of the CPS separate and apart from the remaining provisions of any such agreements, subject to any limitations appearing in 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.

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

In the event that a clause or provision of this CPS is held to be unenforceable by a court of law or other tribunal having authority, the remainder of the CPS shall remain valid.

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

Not applicable

9.16.5 Force Majeure

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall include a force majeure clause protecting DigiCert.

9.17 Other Provisions

Not applicable

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	Certification Authority.
ccTLD	Country Code Top-Level Domain
CICA	Canadian Instituted of Chartered Accountants
CP	Certificate Policy.
CPS	Certification Practice Statement.
CRL	Certificate Revocation List.
CSPRNG	Cryptographically Secure Pseudo-Random Number Generator
DBA	Doing Business As
DCPA	DigiCert Policy Authority
DNS	Domain Name System
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

Definitions

Term	Definition
Administrator	A Trusted Person within the organization of a Processing Center, Service Center, Managed PKI Customer, or Gateway Customer that performs validation and other CA or RA functions.

Term	Definition
	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.
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 Policies (CP)	The “DigiCert Certificate Policy for Symantec Trust Network” and is the principal statement of policy governing the STN.
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.

Term	Definition
Key Pair	The Private Key and its associated Public Key.
Key Recovery Block (KRB)	

Term	Definition
Principal Individual(s)	Individuals of a Private Organization, Government E

Term	Definition
Root Certificate	

Appendix B3: 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. All other bit positions SHOULD NOT 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.

certificatePolicies:policyIdentifier (Required)

- o the anyPolicy identifier if subordinate CA is controlled by DigiCert

(b) cRLDistributionPoint

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

(c) authorityInformationAccess

MUST be present and MUST NOT be marked critical.
SHALL contain the HTTP URL of the Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1). An HTTP accessMethod SHOULD be included for DigiCert's certificate (accessMethod = 1.3.6.1.basicConstraintesr ! tbخي χ r M(d)

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

3. Subscriber Certificate

(a) certificatePolicies

MUST be present and SHOULD NOT be marked critical.

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 DigiCert’s CRL service.

(c) authorityInformationAccess

is always present and NOT marked critical. SHALL contain the HTTP URL of DigiCert’s OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1). An HTTP accessMethod MAY be included for DigiCert’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.

(f) SubjectAltName

populated in accordance with RFC5280 and criticality is set to FALSE.

Appendix B4: 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 Lawyers 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

Appendix C: Supplemental Validation Procedures for Extended Validation (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/. Because the CA/Browser Forum frequently updates the EVCS Guidelines our CPS