DigiCert

Certificate Policy for Symantec Trust Network (STN)

Version 2.11
April 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

DigiCert Certificate Policy for Symantec Trust Network (STN)

Published date: April 18, 2019

Important – Acquisition Notice

On October 31, 2017, DigiCert, Inc. completed the acquisition of Symantec Corporation's Website Security business unit. As a result, DigiCert is now the registered owner of this Certificate Policy document and the PKI Services described within this document.

However, a hybrid of references to "VeriSign," "Symantec," and "DigiCert" shall be evident within this document for a period of time until it is operationally practical to complete the re-branding of the Certification Authorities and services. Any references to VeriSign or Symantec as a corporate entity should be strictly considered to be legacy language that solely reflects the history of ownership.

Trademark Notices

Table of Contents

Contents

Change History Table

Version	Description of Changes
2.2	Updated Relying Party responsibilities and recommendations for key recovery.
2.3	Added TLS as an appropriate use for organization certificates and editorial changes.
2.4	Added language and definition for EV Certificates.
2.5	Updated definition and details for the Netsure Protection Plan.
2.6	Updated legal jurisdiction language and made editorial changes.
2.7	Added two algorithms to section 7.1.3 and completed additional editorial changes.
2.8	Made minor editorial changes.
2.8.1	Replaced all references to RFC 3280 with RFC 5280, and made minor editorial changes.
2.8.2	Correction to ID Proofing of Class 3 Administrator (need not be employees). Remote Hosted KMS – provides option for customer to host the KMS & KMD on their own premises. Changes to describe CA transitions, Key Sizes & Universal Roots throughout the document.
2.8.3	Updated Trademarks Notices page & added Acquisition Notice. Changes to identify Symantec Corporation acquisition & ownership of the VTN CA services. Changes to Governing Law in accord with Symantec ownership. Removed VeriSign Roaming Services which is EOL. Removed reference to Certificate Interoperability Service (CIS) which is EOL. Clarification of TGV services. Clarified Symantec approval required for exceptions to certificate validity periods.
2.8.4	Exception for excluding email address in *subjAltName* for Public Lite accounts. Updated policy to delete all descriptions of the planned transition on or before 31 Dec 2010. Added individual exceptions identified in footnote. Changes made for Auto-Renew 6-year certificate lifetimes and 6-year certificate lifetimes for Enterprise & Client PKI.
2.8.5	Transition from VeriSign to Symantec including: naming, URLs, email addresses. Correction to URL for Managed PKI Lite CRLs. Elimination of the self-revoke webpage in the Magnum release. Clarified the conditions for revoking the recovered key. Individuals may be assigned to Trusted Roles from the QA & Sales teams solely for approved internal functions within Symantec Corp. RAs from the QA & Sales teams may operate without the physical & monitoring protections designated for RAs. Cert issuance is restricted to Class 2 certificates containing an OU value indicating the inherent lack of trust in the cert. Class 2 certs may be issued under certain approved internal uses without identity validation. Stipulate the period of usage of CL2 test & demo certificates issued for the Symantec internal accounts. Removed the statement on EAL-4 certification of the PC software. Correction to URL for Managed PKI Lite CRLs. Tables re Key Usage and EKU are removed because data is outdated and is not necessary to publish. Change to BasicConstraints setting for Subscriber certs. Section 8.4 & Appendix revision to reflect the AICPA change from SAS/70 to the SOC standard as documented in www.aicpa.org/soc.
2.8.6	Clarification of Universal Root – restricted to only Class 3 and selected Class 2 certificates. Document improvements suggested by auditor. Extend the validity period of s/w certs from 2 to 3 years before requiring renewal/rekey
2.8.7	All updates reflecting compliance with CABF Requirements for DV and OV certificates, Effective July 1, 2012.
2.8.8	All updates reflecting compliance with CABF Requirements for EV Code Signing Certificates, v1.4.. Routine maintenance.
2.8.9	Addition of Private Class 3 Admin hierarchy.
2.8.10	Updated references to policy requirements from CABF Guidelines: EV, EV Code Signing & Baseline Requirements.
2.8.11	Added Mozilla IDN Verification requirements
2.8.12	Included OID for certificates less than 2048 bit. Include IP address in common name field.
2.8.13	Change of NetSure Protection Plan liability caps.
2.8.14 - 2.8.24	Completed document-wide editorial changes.
2.9	Replaced with DigiCert where appropriate for 2017 acquisition. Various document-wide editorial and administrative changes.
2.10	Updates in section 3 for IP address validation required by CABF ballot SC7 to point back to the DigiCert CP and CPS. Multiple editorial changes for grammar. Modified section 4.10.2 to specify accurate SLA periods. Replaced “tier” in section 5, with “zone” to be more a more accurate description of physical security. Modified “Issuer CA” to “Issuing CA” to be in-line with the definition. Removed in the definitions section “Section 17.6 (Auditor Qualifications)” to “CP § 8.2.”

2.11	Edited sections 3.1.6, 3.2.1, and 6.1.3 to clarify naming and proof-of-possession practices.

1. INTRODUCTION

DigiCert's Symantec Trust Network (STN) is a global PKI that accommodates a large, public, and widely distributed community of users with diverse needs for communications and information security. DigiCert offers STN services together with a global network of affiliates ("Affiliates") throughout the world.

This document, "DigiCert Certificate Policy for Symantec Trust Network" (CP) is the principal statement of policy governing the STN. The CP sets forth the business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing, digital Certificates within the STN and providing associated trust services for all participants within the STN. These requirements protect the security and integrity of the STN and comprise a single set of rules that apply consistently STN-wide, thereby providing assurances of uniform trust throughout the STN. The CP is not a legal agreement between DigiCert and STN participants; rather, contractual obligations between DigiCert and STN participants are established by means of agreements with such participants.

This document is targeted at:

- STN PKI service providers who have to operate in terms of their own Certification Practices Statement (CPS) that complies with the requirements laid down by the CP
- STN certificate Subscribers who need to understand how they are authenticated and what their obligations are as STN subscribers and how they are protected under the STN
- Relying parties who need to understand how much trust to place in a STN certificate, or a digital signature using that certificate

The CP, however, does not govern any services outside the STN. For example, DigiCert and certain Affiliates offer private label services by which organizations create their own private hierarchies outside the STN, approve certificate applications, and outsource to DigiCert or an Affiliate the back-end functions of certificate issuance, management, revocation, and renewal. Because the CP applies only to the STN, it does not apply to these private hierarchies.[1]

This CP conforms to the Internet Engineering Task Force (IETF) RFC 3647 for Certificate Policy and Certification Practice Statement construction. STN Certificate Policy also adopts the current version of the CA/Browser Forum requirements as set forth in the following documents:

- 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 w*ww.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's Symantec-branded Extended Validation (EV) SSL certificates, Extended Validation (EV) Code-Signing certificates, and Domain-Validated (DV) and Organization-Validated (OV) SSL certificates[2] issued by Symantec-branded CAs under this CP, are governed by the CABF Requirements. Such DV and OV certificates are issued containing the

[1] Authenticated Content Signing Certificates (ACS) are issued by a non-STN CA. However, reference is made to these certificates in certain sections of this CP, for ACS customers to understand certain procedural differences used for these certificates

[2] Additionally, DigiCert issues Symantec-branded 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 CP 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 referred to throughout this CP as "organizational certificates".

corresponding policy identifier(s) specified in section 1.2 indicating adherence to and compliance with these requirements. DigiCert's Symantec-branded CAs shall also assert that all Certificates issued containing these policy identifier(s) are issued and managed in accordance with the CABF Requirements.

STN CAs shall not issue SSL inspection intermediate CAs from roots that are part of the Network. Only roots with no current or previous trust in Application Software Supplier products (private roots) may be used to create intermediate CAs used for SSL inspection.

Effective February 1, 2017 and after, the STN adopts the current version of the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates published at https://aka.ms/csbr. If there is any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

CAs shall disclose all Cross Certificates that identify the CA as the Subject in the established trust relationship.

1.1 Overview

At the top of the STN PKI hierarchy is this CP that sets out the policies under which STN participants must operate.

DigiCert and Affiliate Processing Centers operate as CAs under the STN CP, issuing end-user subscriber certificates.

Registration Authorities (RAs) are entities that authenticate certificate requests under the STN. DigiCert acts as RA for certificates it issues. DigiCert and Affiliates also enter into contractual relationships with Enterprises who wish to manage their own certificate requests. These enterprise customers act as RAs, authenticating certificate requests for themselves and their affiliated individuals. DigiCert or the Affiliate will then issue these authenticated certificate requests.

Depending on the class and type of certificate, Digital Certificates may be used by Subscribers to secure websites, digitally sign code or other content, digitally sign documents and/or e-mails. The person who ultimately receives a signed document or communication, or accesses a secured website is referred to as a relying party, i.e., he/she is relying on the certificate and has to make a decision on whether to trust it. A Relying Party must rely on a certificate in terms of the relevant Relying Party Agreement included in the Certificate.

1.2 Document Name and Identification

This document is the DigiCert Certificate Policy for Symantec Trust Network (STN) (CP). DigiCert, acting as the policy-defining authority, uses the assigned object identifier (OID) value extensions for each Class of Certificate issued under the Symantec Trust Network (STN). The object identifier values used for the Classes of end-user Subscriber Certificates are[3]:

- The Class 1 Certificate Policy: Symantec/pki/policies/stn-cp/class1 (2.16.840.1.113733.1.7.23.1).
- The Class 2 Certificate Policy: Symantec/pki/policies/stn-cp/class2 (2.16.840.1.113733.1.7.23.2).
- The Class 3 Certificate Policy: Symantec/pki/policies/stn-cp/class3 (2.16.840.1.113733.1.7.23.3)
- The Class 3 Certificate Policy for Symantec Private Hierarchy: Symantec/pki/policies/stn-cp/class3 (2.16.840.1.113733.1.7.23.3.2)
- The Class 3 EV Certificate Policy: Symantec/pki/stn-cp/Class3/Enhanced validation (2.16.840.1.113733.1.7.23.6)

[3] Certain certificates issued under the STN may contain legacy policy OIDS assigned under the STN.

The “Class 3 Certificate Policy for Symantec Private Hierarchy” adopts in its entirety the Class 3 policy defined by this CP with the exception that the hierarchy is limited to Internal CAs and the Primary Certification Authority (PCA) certificate shall not be added to public certificate trust lists.

Each OID above may be extended further to define additional policies covering a particular type of certificate. The extended OID shall be defined in the particular CPS for that product.

1.2.1 CABF Policy Identifiers

DigiCert uses a reserved OID value for asserting conformance with the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates. This OID value is reserved for use as a means of asserting compliance with these CABF Requirements and does not distinguish a particular brand or class of Certificate.

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

Most DV and OV certificates issued on or after March 5th, 2015 will include the applicable CABF policy OIDs:

- CABF OID for DV certificates: 2.23.140.1.2.1
- CABF OID for OV certificates: 2.23.140.1.2.2
- CABF OID for IV certificates: 2.23.140.1.2.3

All DV and OV certificates issued after May 2015 will include the applicable CABF policy OIDs. All individual validated certificates issued after December 1, 2016 will include the applicable CABF policy OID.

EV certificates use the applicable CABF policy OIDs:

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

1.2.2 Microsoft Policy Identifiers

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

1.3 PKI Participants

1.3.1 Certification Authorities

The term Certification Authority (CA) is 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[4], 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.

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

The Class 3 domain also allows for a DigiCert private hierarchy that is limited to DigiCert internal administrative uses.

Note: As of the dates indicated, the following root certificates are excluded from the scope of this document:

- As of December 1, 2015:
  VeriSign Class 3 Public Primary Certification Authority

Country = US
Organization = VeriSign, Inc.
Organizational Unit = Class 3 Public Primary Certification Authority

- As of March 27, 2015:
  VeriSign Class 3 Public Primary Certification Authority – G2
  Country = US
  Organization = VeriSign, Inc.
  Organizational Unit = Class 3 Public Primary Certification Authority - G2
  Organizational Unit = (c) 1998 VeriSign, Inc. - For authorized use only
  Organizational Unit = VeriSign Trust Network

Any references to PCAs or Class 3 PCAs in this CP no longer apply to these root certificates. These root certificates are only intended to be used for private purposes and should be disabled in browsers' trusted root lists. The CP and CPS for the Symantec Trust Network no longer govern the use of these root certificates and any of their subordinate services.

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.

Before a subordinate CA can issue STN Extended Validation Certificates in terms of the Guidelines for Extended Validation Certificates ("Guidelines"), it shall have to meet the requirements of the Guidelines.

DigiCert enterprise customers may operate their own CAs as a subordinate CA 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 and affiliates may act as RAs for certificates they issue. Affiliates do not perform domain or IP address validation.

Third parties, who enter into a contractual relationship with DigiCert or an affiliate, may operate their own RA and authorize the issuance of certificates by a STN CA. Third party RAs must abide by all the requirements of the STN CP, the relevant CPS and any Enterprise Service Agreement entered into with DigiCert. RAs may, however implement more restrictive practices based on their internal requirements. An example of a third party RA is a customer of Managed PKI services customer.

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.

In some cases certificates are issued directly to individuals or entities for their own use. However, there commonly exist other situations where the party requiring a certificate is different from the subject to whom the credential applies. For example, an organization may require certificates for its employees to allow them to represent the organization in electronic transactions/business. In such situations the entity subscribing for the issuance of certificates (i.e. paying for them, either through subscription to a specific service, or as the issuer itself) is different from the entity which is the subject of the certificate (generally, the holder of the credential). Two different terms are used in this CP to distinguish between these two roles: "Subscriber", is the entity which contracts with DigiCert for the issuance of credentials and "Subject", is the person to whom the credential is bound. The Subscriber bears ultimate responsibility for the use of the credential but the Subject is the individual that is authenticated when the credential is presented.

When ‘Subject’ is used, it is to indicate a distinction from the Subscriber. When “Subscriber” is used it may mean just the Subscriber as a distinct entity but may also use the term to embrace the two. The context of its use in this CP will invoke the correct understanding.

CAs are technically also subscribers of certificates within the STN, either as a PCA 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 CP, 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 under the STN. A Relying party may, or may not also be a Subscriber within the STN.

1.3.5 Other Participants

An Affiliate is a leading trusted third party, for example in the technology, telecommunications, or financial services industry that has entered into an agreement with DigiCert to operate a Certification Authority under the STN within a specific territory.

Processing Centers (i.e., DigiCert or certain Affiliates) are entities that create a secure facility housing, among other things, the cryptographic modules used for the issuance of Certificates. Processing Centers act as CAs within the STN and perform all Certificate lifecycle services of issuing, managing, revoking, and renewing Certificates. Affiliates who outsource the backend functionality to DigiCert but retain the RA responsibilities are called Service Centers.

Processing Center and Service Center Affiliates do not perform domain or IP address validation. Processing Center Affiliates must comply with STN audit requirements. Service Center Affiliates must be included in the scope of DigiCert WebTrust for Certification Authorities audits.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Usages

1.4.1.1 Certificates Issued to Individuals

Individual Certificates are normally used by individuals to sign and encrypt e-mail and to authenticate to applications (client authentication). While the most common usages for individual certificates are included in the Table below, an individual 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 this CP, by any CPS under which the certificate has been issued and any agreements with Subscribers.

Certificate Class:	**Assurance Level**			**Usage**		
	Low assurance level	**Medium assurance level**	**High assurance Level**	**Signing**	**Encryption**	**Client Authentication**
Class 1 Certificates	✓			✓	✓	✓
Class 2 Certificates		✓		✓	✓	✓
Class 3 Certificates			✓	✓	✓	✓

Table 1. Individual Certificate Usage

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 CP to limit the types of usages for Organizational Certificates. While the most common usages are included in the Table 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 this CP, by any CPS under which the certificate has been issued and any agreements with Subscribers.

	Assurance Level				**Usage**			
Certificate Class	**Medium**	**High with Extended Validation**	**High with CABF OV Validation**	**High**	**Code/ Content Signing**	**Secure SSL/TLS-sessions**	**Authentication**	**Signing and Encryption**
Class 3 Certificates				✓	✓	✓	✓	✓
Class 3 EV SSL Certificates		✓		✓		✓	✓	✓
Class 3 EV Code Signing Certificates		✓		✓	✓		✓	✓
Class 3 OV Certificates			✓	✓		✓	✓	✓
Class 3 DV Certificates	✓					✓	✓ (domain only)	✓

Table 2. Organizational Certificate Usage[5]

[5] "In limited circumstances Class 2 certificates may be issued by a Managed MPKI customer to an affiliated organization (and not an individual within the organization). Such certificate may be used for organization authentication and application signing only. Except as expressly authorized by DigiCert through an Enterprise Service Agreement imposing authentication and practice requirements consistent with the security standards of this CP, Subscribers are prohibited

1.4.1.3 Assurance levels

Low assurance certificates are certificates that should not be used for authentication purposes or to support Non-repudiation. The digital signature provides modest assurances that the e-mail originated from a sender with a certain e-mail address. The Certificate, however, provides no proof of the identity of the Subscriber. The encryption application enables a Relying Party to use the Subscriber's Certificate to encrypt messages to the Subscriber, although the sending Relying Party cannot be sure that the recipient is in fact the person named in the Certificate.

Medium assurance certificates are certificates that are suitable for securing some inter- and intra-organizational, commercial, and personal e-mail requiring a medium level of assurances of the Subscriber identity, in relation to Class 1 and 3.

DigiCert Basic DV Certificates are issued to domains to provide encryption. Section 3.2.2 of the STN CPS explains how DigiCert validates that the person enrolling for the certificate has control of the domain. No organization authentication is performed on the owner of the domain listed in a DV certificate.

High assurance Certificates are individual and organizational Class 3 Certificates that provide a high level of assurance of the identity of the Subscriber in comparison with Class 1 and 2.

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.

STN 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 shall 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.

STN Participants periodically rekey 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.

from using this certificate for code and content signing, SSL encryption and S/mime signing and such key usage will be disabled for these certificates."

1.5 Policy Administration

1.5.1 Organization Administering the Document

This CP 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/

1.5.3 Person Determining CP Suitability for the Policy

The DCPA determines the suitability and applicability of this CP.

1.5.4 CP Approval Procedure

Approval of this CP and subsequent amendments shall be made by the DCPA. Amendments shall either be in the form of a document containing an amended form of the CP or an update notice. Amended versions or updates shall be linked to the Practices Updates and Notices section of the DigiCert Repository located at: *https://www.digicert.com/legal-repository* (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 CP. The DCPA shall determine whether changes to the CP require a change in the Certificate policy object identifiers of the Certificate Policies corresponding to each Class of Certificate.

1.6 Definitions and Acronyms

See Appendix A for a table of acronyms and definitions.

2. Publication and Repository Responsibilities

2.1 Repositories

For STN certificates, DigiCert and Affiliate Processing Centers are responsible for maintaining a publicly accessible online repository. Processing Centers, as part of their contracts with Service Centers, publish Certificates in the Service Center's repository based on Certificate Applications approved by the Service Centers or their RAs, as well as revocation information concerning such Certificates.

2.2 Publication of Certificate Information

For STN certificates, DigiCert and Affiliates maintain a web-based repository that permits Relying Parties to make online inquiries regarding revocation and other Certificate status information. Any exception to this shall be approved by the DCPA on a case by case basis and must be documented in the appropriate CPS. A Processing Center, as part of its contract with a Service Center, shall host such a repository on behalf of the Service Center. DigiCert and Affiliates provide Relying Parties with information on how to find the appropriate repository to check Certificate status and, if OCSP (Online Certificate Status Protocol) is available, how to find the right OCSP responder.

Processing Centers publish the Certificates they issue on behalf of their own CAs, and the CAs of Service Centers in their Sub-domain. Upon revocation of an end-user Subscriber's Certificate, the Processing Center that issued the Certificate shall publish notice of such revocation in the repository. In addition, Processing Centers shall issue Certificate Revocation Lists (CRLs) and, if available, provide OCSP services (Online Certificate Status Protocol) for their own CAs and the CAs of Service Centers within their respective Sub-domains.

DigiCert and Affiliates will at all times publish a current version of:

- This STN CP
- Its CPS,
- Subscriber Agreements,
- Relying Party Agreements

2.3 Time or Frequency of Publication

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 shall be issued at least once per day. CRLs for CAs that only issue CA Certificates shall be 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. If applicable based on the types of certificates they issue and the scope of the CA/Browser Forum Baseline Requirements, STN Participants shall develop, implement, enforce, and annually update a Certification Practices Statement that describes in detail how the CA implements the latest version of the CA/Browser Forum Baseline Requirements.

2.4 Access Controls on Repositories

DigiCert and Affiliates shall not intentionally use technical means of limiting access to this CP, their CPS, Certificates, Certificate status information, or CRLs. DigiCert and Affiliates shall, however, require persons to agree to a Relying Party Agreement or CRL Usage Agreement as a condition to accessing Certificates, Certificate status information, or CRLs. DigiCert and Affiliates shall implement controls to prevent unauthorized persons from adding, deleting, or modifying repository entries. DigiCert and Affiliates shall make their repositories publicly available in a read-only manner, either at the link stated in section 1.5.4 or specified in an Affiliate's CPS.

3. Identification and Authentication

3.1 Naming

Unless where indicated otherwise in this CP, the relevant CPS or the content of the digital certificate, names appearing in Certificates issued under STN are authenticated.

3.1.1 Type of Names

End-user Subscriber Certificates contain an X.501 Distinguished Name (DN) in the Subject name field and in the Issuer Name field.

The Subject DN of end-user Subscriber Certificates may include a common name (CN=) component. The authenticated common name value included in the Subject DN of organizational Certificates shall be a domain name, public IP address[6], Organizational e-mail address, the legal name of the organization, or name of the organizational representative authorized to use the organization's private key. The (O=) component shall be the legal name of the organization.

The common name value optionally included in the Subject DN of individual Certificates shall represent the individual's generally accepted personal name. Only for Class 1 Individual Certificates, the common name may be omitted. Class 1 Individual Certificates that omit the common name shall include an rfc822Name in the subject alternate name extension that contains the authenticated email address of the subject. Common names shall be authenticated in the case of Class 2-3 Certificates. STN Certificates may also contain a reference to the applicable Relying Party Agreement in their DNs.

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 domain names or public iPAddresses which will be authenticated in the same way as the Common Name value. 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.

3.1.1.1 CABF Naming Requirements

Naming values for EV SSL, EV Code Signing, and domain-validated and organization-validated SSL/TLS server Certificates shall be documented in a STN participant's CPS and shall comply with the applicable governing CA/Browser Forum Guidelines published at *www.cabforum.org*.

[6] The use of Certificates with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Name has been deprecated by the CA / Browser Forum and was terminated by October 2016. Any reference to IP address inclusion in Certificates are for legacy purposes or exceptional circumstances that are validated and controlled by DigiCert as per the DigiCert CPS section 3.2.2.

3.1.2 Need for Names to be Meaningful

Class 2 and 3 end-user Subscriber Certificates shall include meaningful names in the following sense: Class 2 and 3 end-user Subscriber Certificates shall contain names with commonly understood semantics permitting the determination of the identity of the individual or organization that is the Subject of the Certificate.

3.1.3 Anonymity or Pseudonymity of Subscribers

The identity of Class 1 individual Subscribers is not authenticated. Class 1 subscribers may use pseudonyms. Class 2 and 3 Subscribers are not permitted to use pseudonyms (names other than a Subscriber's true personal or organizational name).

When required by law or requested by a State or Government authority to protect the identity of certain end user subscribers (e.g., minors, or sensitive government employee information), a certificate may be issued indicating that identity has been authenticated but is protected. Each request for anonymity in a certificate will be evaluated on its merits by the DCPA.

3.1.4 Rules for Interpreting Various Name Forms

No stipulation

3.1.5 Uniqueness of Names

The names of Subscribers within the STN shall be unique within an Affiliate's and Customer's Sub-domain for a specific class 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 shall not use names in their Certificate Applications that infringe upon the Intellectual Property Rights of others. For EV SSL Certificates, DigiCert shall not include a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless DigiCert has verified this information in accordance with the EV Guidelines. For all other Certificate types, neither DigiCert nor any Affiliate shall be required to determine whether a Certificate Applicant has Intellectual Property Rights in the name appearing in a Certificate Application or to arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any domain name, trade name, trademark, or service mark, and DigiCert and any Affiliate shall be entitled, without liability to any Certificate Applicant, to reject or suspend any Certificate Application because of such dispute.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The certificate applicant may demonstrate that it rightfully holds the private key corresponding to the public key to be listed in the Certificate.

The method to prove possession of a private key shall be PKCS #10, another cryptographically equivalent demonstration, or another DigiCert-approved method. This process does not apply where a key pair is generated by a CA on behalf of a Subscriber, for example where pre-generated keys are placed on smart cards.

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

Where a domain name or e-mail address is included in the certificate DigiCert authenticates the Organization's right to use that domain name either as a fully qualified Domain name or an e-mail domain. For Organization Validated (OV) and Extended Validation (EV) Certificates domain validation is completed in all cases along with Organizational validation. Validation of domain ownership or control 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.

Additional checks necessary to satisfy United States export regulations and licenses issued by the United States Department of Commerce Bureau of Industry and Science ("BIS") are performed by DigiCert and Affiliates when required.

3.2.2.1 CABF Verification Requirements for Organization Applicants

Validation procedures for issuing EV SSL Certificates, EV Code Signing, and Domain-Validated and Organization-Validated SSL Certificates shall be documented in a STN participant's CPS and shall comply with the applicable governing CA/Browser Forum Guidelines published at *www.cabforum.org*.

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.

3.2.2.3 Domain Validation

DigiCert details the methods of vetting a domain name in the DigiCert CPS, section 3.2.2.

3.2.3 Authentication of Individual Identity

Authentication procedures for individual identity differ according to the Class of Certificate. The minimum authentication standard for each class of STN certificate is explained in Table 3 below.

Certificate Class	Authentication of Identity
Class 1	No identity authentication. Email address validation –

Certificate Class	Authentication of Identity
	Limited confirmation that the certificate subscriber has access to the email address. DigiCert performs a challenge-response type of procedure in which DigiCert sends email to the email address to be included in the certificate, containing unpredictable information such as a randomly generated PIN/Password unique to the owner of the email address. The owner of the email address (the subscriber of the certificate) demonstrates control over the email address by using the 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: • 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 • Passcode-based authentication where a randomly-generated passcode is delivered out-of-band by the enterprise administrator customer to the subscriber entitled to enroll for the certificate, and the subscriber provides this passcode at enrollment time or • Comparing information provided by the subscriber to information contained in business records or databases (customer directories such as Active Directory or LDAP.
Class 3	The authentication of Class 3 individual Certificates is based on the personal (physical) presence of the Certificate Applicant before an agent of the CA or RA, or before a notary public or other official with comparable authority within the Certificate Applicant's jurisdiction. The agent, notary or other official shall check the identity of the Certificate Applicant against a well-recognized form of government-issued photographic identification, such as a passport or driver's license and one other identification credential. Class 3 Administrator certificates shall also include authentication of the organization and a confirmation from the organization of the identity and authorization of the person to act as Administrator. DigiCert and Affiliates may also have occasion to approve Certificate Applications for their own Administrators. Administrators are "Trusted Persons" within an organization. In this case, authentication of their Certificate Applications shall be based on confirmation of their identity in connection with their employment or retention as an independent contractor and background checking procedures.[7] Email address validation –

[7] DigiCert and Affiliates may approve Administrator Certificates to be associated with a nonhuman recipient such as a device, or a server. Authentication of a Class 3 Administrator Certificate Applications for a non-human recipient shall include:
• Authentication of the existence and identity of the service named as the Administrator in the Certificate Application
• Authentication that the service has been securely implemented in a manner consistent with it performing an Administrative function
• Confirmation of the identity and authorization of the person enrolling for the Administrator certificate for the service named as Administrator in the Certificate Application.

Certificate Class	Authentication of Identity
	For Class 3 Organizational Email certificates, the CA or RA shall verify that the subscriber owns the base domain using methods from Section 3.2.2 of a CPS that implements this CP, and allows the subscriber to request any email address within that verified domain.

Table 3. Authentication of individual identity

3.2.4 Non-Verified Subscriber information

Non-verified subscriber information includes:

- Organization Unit (OU) with certain exceptions[8]
- Subscriber's name in Class 1 certificates
- Any other information designated as non-verified in the certificate.

3.2.5 Validation of Authority

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 CA or 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 agency or recognized authority that confirms the existence of the organization as per section 3.2 in the DigiCert CP, 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

The STN may provide interoperation services that allow a non-STN CA to be able to interoperate with the STN by unilaterally certifying that CA. CAs enabled to interoperate in this way will comply with this CP as supplemented by additional policies when required.

DigiCert shall only allow interoperation with the STN of a non-STN CA in circumstances where the CA shall at a minimum:

- Enters into a contractual agreement with DigiCert
- Operates under a CPS that meets STN requirements for the classes of certificates it will issue
- Passes a compliance assessment before being allowed to interoperate
- Passes an annual compliance assessment for ongoing eligibility to interoperate.

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. CAs and RAs generally require 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").

[8] Domain-validated and organization-validated certificates may contain Organizational Unit values that are validated.

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 DigiCert-issued Symantec-branded 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

The entity approving a Certificate Application for the Subscriber of an end-user Subscriber Certificate shall be responsible for authenticating a request for re-key or renewal. Re-key procedures ensure that the person or organization seeking to renew/rekey an end-user Subscriber Certificate is in fact the Subscriber of the Certificate.

One acceptable procedure is through the use of a Challenge Phrase (or the equivalent thereof), or proof of possession of the private key. Subscribers choose and submit with their enrollment information a Challenge Phrase. Upon renewal of a Certificate, if a Subscriber correctly submits the Subscriber’s Challenge Phrase (or the equivalent thereof) with the Subscriber’s reenrollment information, and the enrollment information (including contact information[9]) has not changed, and the previous validations were performed within the allowable data reuse limits specified in the CA/Browser Forum Baseline Requirements and EV Guidelines, a renewal Certificate is automatically issued.

3.3.2 Identification and Authentication for Re-key After Revocation

Re-key/renewal after revocation is not permitted if the revocation occurred because:

- 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 or entity named as the Subject of such Certificate, or
- the entity approving the Subscriber’s Certificate Application discovers or has reason to believe that a material fact in the Certificate Application is false
- the certificate was deemed harmful to the STN.

Subject to the foregoing paragraph, renewal of an Organizational or CA Certificate following revocation of the Certificate is permissible as long as renewal procedures ensure that the organization or CA seeking renewal is in fact the Subscriber of the Certificate. Renewed Organizational Certificates shall contain the same Subject DN as the Subject DN of the Organizational Certificate being renewed.

Renewal of an individual Certificate following revocation must ensure that the person seeking renewal is, in fact, the Subscriber. One acceptable procedure is the use of a Challenge Phrase (or the equivalent thereof). Other than this procedure or another DigiCert-approved procedure, the requirements for the identification and authentication of an original Certificate Application shall be used for renewing a Certificate following revocation.

[9] If contact information has changed via an approved formal contact change procedure the certificate shall still qualify for automated renewal.

3.4 Identification and Authentication for Revocation Request

Revocation procedures ensure prior to any revocation of any Certificate that the revocation has in fact been requested by the Certificate's Subscriber, the entity that approved the Certificate Application, or the applicable Processing Center.

Acceptable procedures for authenticating the revocation requests of a Subscriber include:

- Having the Subscriber for certain certificate types submit the Subscriber's Challenge Phrase (or the equivalent thereof), and revoking the Certificate automatically if it matches the Challenge Phrase (or the equivalent thereof) on record. (Note that this option may not be available to all customers.)
- Receiving a message from the Subscriber that requests revocation and contains a digital signature verifiable with reference to the Certificate to be revoked,
- Communication with the Subscriber providing reasonable assurances in light of the Class of Certificate that the person or organization requesting revocation is, in fact the Subscriber. Such communication, depending on the circumstances, may include one or more of the following: telephone, facsimile, e-mail, postal mail, or courier service.

CA/RA Administrators are entitled to request the revocation of end-user Subscriber Certificates within the CA's/RA's Sub domain. DigiCert and Affiliates authenticate the identity of Administrators via access control using SSL and client authentication before permitting them to perform revocation functions, or another STN-approved procedure.

RAs using an Automated Administration Software Module may submit bulk revocation requests to a Processing Center. Such requests shall be authenticated via a digitally signed request signed with the private key in the RA's Automated Administration hardware token.

The requests to revoke a CA Certificate shall be authenticated by the requesting entity's Superior entity to ensure that the revocation has in fact been requested by the CA.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application?

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

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

4.1.2 Enrollment Process and Responsibilities

4.1.2.1 End-User Certificate Subscribers

All end-user Certificate Subscribers shall manifest assent to the relevant Subscriber Agreement that contains representations and warranties described in Section 9.6.3 and undergo an enrollment process consisting of:

- completing a Certificate Application and providing true and correct information,
- generating, or arranging to have generated, a key pair,
- delivering his, her, or its public key, directly or through an RA, to the processing Center,
- demonstrating possession and/or exclusive control of the private key corresponding to the public key delivered to the Processing Center.

4.1.2.2 CABF Certificate Application Requirements

Practices for Certificate enrollment for EV SSL Certificates, EV Code Signing, and Domain-Validated and Organization-Validated SSL Certificates shall be documented in a STN participant's CPS and shall comply with the applicable governing CA/Browser Forum Guidelines published at *www.cabforum.org*.

4.1.2.3 CA and RA Certificates

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

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

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

4.2.2 Approval or Rejection of Certificate Applications

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

- Successful identification and authentication of all required Subscriber information in terms of Section 3.2
- Payment (if applicable) has been received

An RA will reject a certificate application if:

- identification and authentication of all required Subscriber information in terms of Section 3.2 cannot be completed, or
- The Subscriber fails to furnish supporting documentation upon request, or
- The Subscriber fails to respond to notices within a specified time, or
- Payment (if applicable) has not been received, or
- The RA believes that issuing a certificate to the Subscriber may bring the STN into disrepute

4.2.3 Time to Process Certificate Applications

CAs and RAs begin processing certificate applications within a reasonable time of receipt. There is no time stipulation to complete the processing of an application unless otherwise indicated in the relevant Subscriber Agreement, CPS or other Agreement between STN participants.

A certificate application remains active until rejected.

4.2.4 Certificate Authority Authorization (CAA)

As of September 8, 2017, CAA issue and issuewild records must be 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 can be treated as permission to issue when the failure is proven to be outside DigiCert infrastructure, was retried at least once, and the domain zone does not have a DNSSEC validation chain to the ICANN root.

STN CAs must log actions taken based on CAA records, and document issuance prevented by CAA for feedback to the CA/Browser Forum.

The Symantec Trust Network and all its brands recognize any and all of the following Issuer Domain Names as permission to issue: digicert.com, symantec.com, thawte.com, geotrust.com, rapidssl.com, and FQDNs terminating in the base domain name digitalcertvalidation.com with reseller-specific licensed prefixes.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

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

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

CAs issuing Certificates to end-user Subscribers shall, either directly or through an RA, notify Subscribers that they have created such Certificates, and provide Subscribers with access to the Certificates by notifying them that their Certificates are available and the means for obtaining them. Certificates shall be made available to end-user Subscribers, either by allowing them to download them from a web site or via a message sent to the Subscriber containing the Certificate.

4.3.3 CABF Requirement for Certificate Issuance by a Root CA

Practices for Certificate Issuance by a Root CA as applicable to EV SSL Certificates, EV Code Signing, and Domain-Validated and Organization-Validated SSL Certificates shall be documented in a STN participant's CPS and shall comply with the applicable governing CA/Browser Forum Guidelines published at *www.cabforum.org*.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The following conduct constitutes certificate acceptance:

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

4.4.2 Publication of the Certificate by the CA

Processing Centers publish the Certificates they issue in a publicly accessible repository.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

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

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

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

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

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties shall assent to the terms of the applicable Relying Party Agreement as a condition of relying on the 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 CP. DigiCert, CAs, and RAs are not responsible for assessing the appropriateness of the use of a Certificate.
- That the certificate is being used in accordance with the *KeyUsage* field extensions included in the certificate (e.g., if Digital Signature is not enabled then the certificate may not be relied upon for validating a Subscriber's signature).
- The status of the certificate and all the CAs in the chain that issued the certificate. If any of the Certificates in the Certificate Chain have been revoked, the Relying Party is solely responsible to investigate whether reliance on a digital signature performed by an end-user Subscriber Certificate prior to revocation of a Certificate in the Certificate chain is reasonable. Any such reliance is made solely at the risk of the Relying party.

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

4.6 Certificate Renewal

Certificate renewal is the issuance of a new certificate to the subscriber without changing the public key or any other information in the certificate. Certificate renewal is supported for Class 3 certificates where the key pair is generated on a web server as most web server key generation tools permit the creation of a new Certificate Request for an existing key pair.

4.6.1 Circumstances for Certificate Renewal

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to renew the expiring certificate to maintain continuity of Certificate usage. A certificate may also be renewed after expiration.

4.6.2 Who May Request Renewal

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

4.6.3 Processing Certificate Renewal Requests

Renewal procedures ensure that the person or organization seeking to renew an end-user Subscriber Certificate is in fact the Subscriber (or authorized by the Subscriber) of the Certificate.

One acceptable procedure is through the use of a Challenge Phrase (or the equivalent thereof), or proof of possession of the private key. Subscribers choose and submit with their enrollment information a Challenge Phrase (or the equivalent thereof). Upon renewal of a Certificate, if a Subscriber correctly submits the Subscriber's Challenge Phrase (or the equivalent thereof) with the Subscriber's reenrollment information, and the enrollment information (including contact information[10]) has not changed, and the relevant validation data has not expired as defined by the guidelines of the CA/Browser Forum, a renewal Certificate is automatically issued.

Other than this procedure or another DigiCert-approved procedure, the requirements for the authentication of an original Certificate Application shall be used for renewing an end-user Subscriber Certificate.

4.6.4 Notification of New Certificate Issuance to Subscriber

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

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

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

4.6.6 Publication of the Renewal Certificate by the CA

The renewed certificate is published in the issuing Processing Center's publicly accessible repository.

[10] If contact information has changed via an approved formal contact change procedure the certificate shall still qualify for automated renewal.

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.

4.7.1 Circumstances for Certificate Re-Key

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to re-key the certificate to maintain continuity of Certificate usage. A certificate may also be re-keyed after expiration.

4.7.2 Who May Request Certification of a New Public Key

Only the subscriber for an individual certificate or an authorized representative for an Organizational certificate may request certificate re-key.

4.7.3 Processing Certificate Re-Keying Requests

Re-key procedures ensure that the person or organization seeking to renew an end-user Subscriber Certificate is in fact the Subscriber (or authorized by the Subscriber) of the Certificate.

One acceptable procedure is through the use of a Challenge Phrase (or the equivalent thereof), or proof of possession of the private key. Subscribers choose and submit with their enrollment information a Challenge Phrase (or the equivalent thereof). Upon renewal of a Certificate, if a Subscriber correctly submits the Subscriber's Challenge Phrase (or the equivalent thereof) with the Subscriber's reenrollment information, and if the enrollment information (including contact information[11]) has not changed, a renewal Certificate is automatically issued. After re-keying in this fashion, and on at least alternative instances of subsequent re-keying thereafter, the CA or RA shall reconfirm the identity of the Subscriber in accordance with the requirements specified in this CP for the authentication of an original Certificate Application.

Other than this procedure or another DigiCert-approved procedure, the requirements for the authentication of an original Certificate Application shall be used for re-keying an end-user Subscriber Certificate.

4.7.4 Notification of New Certificate Issuance to Subscriber

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

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

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

4.7.6 Publication of the Re-Keyed Certificate by the CA

The re-keyed certificate is published in the issuing Processing Center's publicly accessible repository.

[11] If contact information has changed via an approved formal contact change procedure the certificate shall still qualify for automated renewal.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

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

4.8 Certificate Modification

4.8.1 Circumstances for Certificate Modification

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

Certificate modification is considered a Certificate Application in terms of Section 4.1.

4.8.2 Who May Request Certificate Modification

See Section 4.1.1

4.8.3 Processing Certificate Modification Requests

An RA shall perform identification and authentication of all required Subscriber information in terms of Section 3.2

4.8.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2

4.8.5 Conduct Constituting Acceptance of Modified Certificate

See Section 4.4.1

4.8.6 Publication of the Modified Certificate by the CA

See Section 4.4.2

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3

4.9 Certificate Revocation and Suspension

Practices for revocation and status checking of EV SSL Certificates, EV Code Signing, and Domain-Validated and Organization-Validated SSL Certificates shall be documented in a STN participant's CPS and shall comply with the applicable governing CA/Browser Forum Guidelines published at *www.cabforum.org*.

If an STN Participant (Affiliate, Processing Center, Service Center) issues code signing certificates and has independent authority to revoke certificates, practices for revocation and status checking of Code Signing Certificates shall be documented in an STN participant's CPS and shall comply with section 13 of the applicable governing Microsoft Minimum Requirements published at *aka.ms/csbr*.

4.9.1 Circumstances for Revocation

Only in the circumstances listed below, will an end-user Subscriber certificate be revoked by a Processing Center (or by the Subscriber) and published on a CRL. Upon request from a Subscriber who can no longer use (or no longer wishes to use) a certificate for a reason other than one mentioned below, DigiCert will flag the certificate as inactive in its database but will not publish the certificate on a CRL.

An end-user Subscriber Certificate is revoked if:

- A Processing Center, a Customer, or a Subscriber has reason to believe or strongly suspects that there has been a Compromise of a Subscriber's private key,
- A Processing Center or a Customer has reason to believe that the Subscriber has materially breached a material obligation, representation, or warranty under the applicable Subscriber Agreement,
- The Subscriber Agreement with the Subscriber has been terminated,
- The affiliation between an Enterprise Customer with a Subscriber is terminated or has otherwise ended,
- A Processing Center 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,
- A Processing Center or a Customer has reason to believe that a material fact in the Certificate Application is false,
- A Processing Center 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 STN, a CA and/or RA considers, among other things, the following:

- The nature and number of complaints received
- The identity of the complainant(s)
- Relevant legislation in force
- Responses to the alleged harmful use from the Subscriber

When considering whether the use of a Code Signing Certificate is harmful to the STN, a CA and/or RA additionally considers among other things, the following:

- The name of the code being signed
- The behavior of the code
- Methods of distributing the code

- Disclosures made to recipients of the code
- Any additional allegations made about the code

DigiCert may also revoke an Administrator Certificate if the Administrator's authority to act as Administrator has been terminated or otherwise has ended.

DigiCert Subscriber Agreements require end-user Subscribers to immediately notify DigiCert of a known or suspected compromise of its private key.

A Processing Center may also revoke an Administrator Certificate if the Administrator's authority to act as Administrator has been terminated or otherwise has ended.

Subscriber Agreements require end-user Subscribers to immediately notify a Processing Center of a known or suspected compromise of its private key.

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, an Affiliate, 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.

Only DigiCert is entitled to request or initiate the revocation of the Certificates issued to its own CAs. Non-DigiCert Processing Centers, Service Centers and RAs are entitled, through their duly authorized representatives, to request the revocation of their own Certificates, and their Superior Entities shall be entitled to request or initiate the revocation of their Certificates.

Regarding code signing certificates, DigiCert and those Affiliates that issue code signing certificates must 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 Compromise, Certificate misuse, Certificates used to sign Suspect Code, Takeover Attacks, or other types of possible fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates. DigiCert and Affiliates MUST publicly disclose the instructions on its website.

DigiCert and those Affiliates that issue code signing certificates MUST revoke a Code Signing Certificate in any of these four circumstances: (1) the Application Software Supplier requests revocation and DigiCert or its Affiliate does not intend to pursue an alternative course of action, (2) the authenticated subscriber requests revocation, (3) a third party provides information that leads the CA to believe that the certificate is compromised or is being used for Suspect Code, or (4) the CA otherwise decides that the certificate should be revoked. DigiCert and Affiliates shall follow the process for handling revocation requests detailed at section 13.1.5 of the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates. Where applicable due to restricted revocation privilege, Affiliates will request revocation to be performed by DigiCert.

4.9.3 Procedure for Revocation Request

4.9.3.1 Procedure for Requesting the Revocation of an End-User Subscriber Certificate
Prior to the revocation of a Certificate, the CA verifies that the revocation has been requested by the Certificate's Subscriber, or the entity that approved the Certificate Application, or that the revocation request relates to a code signing certificate subject to other revocation requestors specified in section 4.9.2. Acceptable procedures for authenticating Subscriber revocation requests include:

- Having the Subscriber for certain certificate types submit the Subscriber's Challenge Phrase (or an equivalent thereof) and revoking the Certificate automatically if it matches the Challenge Phrase (or an equivalent thereof) on record,
- Receiving a message purporting to be from the Subscriber that requests revocation and contains a digital signature verifiable with reference to the Certificate to be revoked, and
- Communication with the Subscriber providing reasonable assurances in light of the Class of Certificate that the person or organization requesting revocation is, in fact the Subscriber. Depending on the circumstances, such communication may include one or more of the following: telephone, facsimile, e-mail, postal mail, or courier service.

CA/RA Administrators are entitled to request the revocation of end-user Subscriber Certificates within the CA's/RA's Subdomain. DigiCert and Affiliates shall authenticate the identity of Administrators via access control using SSL and client authentication before permitting them to perform revocation functions.

RAs using the Automated Administration Software Module may submit bulk revocation requests to DigiCert. Such requests are authenticated via a request digitally signed with the private key in the RA's Automated Administration hardware token.

The requests from CAs to revoke a CA Certificate shall be authenticated by their Superior Entities to ensure that the revocation has in fact been requested by the CA.

4.9.4 Revocation Request Grace Period

Revocation requests shall be submitted as promptly as possible within a commercially reasonable time.

4.9.5 Time within Which CA Must Process the Revocation Request

Commercially reasonable steps are taken to process revocation requests without delay. STN participants that issue code signing certificates shall comply with the revocation timeframes specified for malware in the Minimum Requirements for Issuance and Management of Publicly-Trusted Code Signing Certificates in section 13.1.5.3 for code signing certificates. In the case of Affiliates that both issue code signing certificates and rely on DigiCert to perform revocation due to limited privileges, DigiCert shall comply with the timeframes.

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. Alternatively, Relying Parties may meet this requirement either by checking Certificate status using the applicable web-based repository or by using OCSP (if available). CAs shall provide Relying Parties with information on how to find the appropriate CRL, web-based repository, or OCSP responder (where available) to check for revocation status.

Due to the numerous and varying locations for CRL repositories, relying parties are advised to access CRLs using the URL(s) embedded in a certificate's CRL Distribution Points extension. The proper OCSP responder for a given certificate is placed in its Authority Information Access extension.

4.9.7 CRL Issuance Frequency

CRLs for end-user Subscriber Certificates are issued at least once per day. CRLs for CA Certificates shall be issued at least annually, but 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.

Any deviation from this general policy must get approval from the DCPA and be published in the appropriate CPS.

4.9.7.1 CABF Requirements for CRL Issuance

Frequency of CRL issuance for EV SSL Certificates, EV Code Signing, and Domain-Validated and Organization-Validated SSL Certificates shall be documented in a STN participant's CPS and shall comply with the applicable governing CA/Browser Forum Guidelines published at *www.cabforum.org*.

4.9.7.2 Microsoft Requirements for CRL Issuance

Frequency of CRL issuance for code signing and timestamp certificates shall be documented in a STN participant's CPS if they issue code signing and/or timestamp certificates and shall comply with section 13.2.2 of the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates published at https://aka.ms/csbr.

4.9.8 Maximum Latency for CRLs

CRLs are posted to the DigiCert Repository within a commercially reasonable time after generation. This is generally done automatically within minutes of generation.

4.9.9 On-Line Revocation/Status Checking Availability

Online revocation and other Certificate status information are available via a web-based repository and, where offered, OCSP. Processing Centers shall have a web-based repository that permits Relying Parties to make online inquiries regarding revocation and other Certificate status information. A Processing Center, as part of its contract with a Service Center, shall host such a repository on behalf of the Service Center. Processing Centers provide Relying Parties with information on how to find the appropriate repository to check Certificate status and, if OCSP is available, how to find the correct OCSP responder.

STN Participants that issue code signing and/or timestamp certificates MUST provide OCSP responses for Code Signing Certificates and Timestamp Certificates for the time period specified in their CPS, which MUST be at least 10 years after the expiration of the certificate. If a CA issues CRLs, the serial number of a revoked certificate MUST remain on the CRL for at least 10 years after the expiration of the certificate.

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 shall be documented in a STN participant's CPS and shall comply with the applicable governing CA/Browser Forum Guidelines published at *www.cabforum.org*.

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

STN Participants shall be notified of an actual or suspected CA private key Compromise using commercially reasonable efforts. Processing Centers shall use commercially reasonable efforts to notify potential Relying Parties if they discover, 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-domain.

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, through a Processing Center's website (at a URL specified in that Processing Center's CPS), LDAP directory and via an OCSP responder (where available).

4.10.2 Service Availability

Certificate Status Services shall be available 24×7.

For EV SSL Certificates, EV Code Signing, and Domain-Validated and Organization-Validated SSL Certificates, availability of certificate status services shall be documented in a STN participant's CPS and shall comply with the applicable governing CA/Browser Forum Guidelines published at *www.cabforum.org*.

4.10.3 Optional Features

OCSP is an optional status service feature that is not available for all products and must be specifically enabled for other products

4.11 End of Subscription

A subscriber may end a subscription for a STN certificate by:

- Allowing his/her/its certificate to expire without renewing or re-keying that certificate
- Revoking of his/her/its certificate before certificate expiration without replacing the certificate.

4.12 Key Escrow and Recovery

With the exception of enterprises deploying Managed PKI Key Management Services no STN participant may escrow CA, RA or end-user Subscriber private keys.

Enterprise customers using the Key Escrow option within the Symantec Managed PKI Service can escrow copies of the private keys of Subscribers whose Certificate Applications they approve. The enterprise customer may escrow keys either within the enterprise's premises or DigiCert's secure data center. If operated out of the enterprise's premises, DigiCert does not store copies of Subscriber private keys but nevertheless plays an important role in the Subscriber key recovery process.

4.12.1 Key Escrow and Recovery Policy and Practices

Enterprise customers using the Key Escrow option within the Symantec Managed PKI Service (or an equivalent service approved by DigiCert) are permitted to escrow end-user Subscribers' private key. Escrowed private keys shall be stored in encrypted form using the Managed PKI Key Manager software. Except for enterprise customers using the Managed PKI Key Manager Service (or an equivalent service approved by DigiCert), the private keys of CAs or end-user Subscribers shall not be escrowed.

End-user Subscriber private keys shall only be recovered under the circumstances permitted within the Managed PKI Key Management Service Administrator's Guide, under which:

- Enterprise customers using Managed PKI Key Manager shall confirm the identity of any person purporting to be the Subscriber to ensure that a purported Subscriber request for the Subscriber's private key is, in fact, from the Subscriber and not an imposter,
- Enterprise customers shall recover a Subscriber's private key without the Subscriber's authorization only for their legitimate and lawful purposes, such as to comply with judicial or administrative process or a search warrant, and not for any illegal, fraudulent, or other wrongful purpose, and
- Such Enterprise customers shall have personnel controls in place to prevent Key Management Service Administrators and other persons from obtaining unauthorized access to private keys.

It is recommended that an Enterprise Customer using the Key Escrow option within the Symantec Managed PKI Service:

- Notify the subscribers that their private keys are escrowed

- Protect subscribers' escrowed keys from unauthorized disclosure,
- Protect all information, including the administrator's own key(s) that could be used to recover subscribers' escrowed keys.
- Release subscribers' escrowed keys only for properly authenticated and authorized requests for recovery.
- Revoke the Subscriber's Key pair prior to recovering the encryption key under certain circumstances such as to discontinue the use of a lost certificate.
- Not be required to communicate any information concerning a key recovery to the subscriber except when the subscriber him/herself has requested recovery.
- 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, 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 random session key to form a session key mask (MSK). The resulting MSK together with the certificate request information is securely sent and stored in the Managed PKI database at DigiCert. The KER (containing the end user's private key) and the individual session key are stored in the Key Manager database.

The Managed PKI database is operated out of DigiCert's secure data center. The enterprise customer may choose to operate the Key Manager database either on the enterprise's premises or out of DigiCert's secure data center.

Recovery of a private key and digital certificate requires the Managed PKI administrator to securely log on to the Managed PKI Control Center, select the appropriate key pair to recover and click a "recover" hyperlink. Only after an approved administrator clicks the "recover" link is the MSK for that key pair returned from the Managed PKI database. The Key Manager retrieves the session key from the KMD and combines it with the MSK to regenerate the triple-DES key which was used to originally encrypt the private key, allowing recovery of the end user's private key. As a final step, an encrypted PKCS#12 file is returned to the administrator and ultimately distributed to the end user.

5. Facility, Management, and Operational Controls

5.1 Physical Controls

The STN has documented detailed physical control and security policies for CAs and RAs to adhere to. Compliance with these policies is included in the STN independent audit requirements described in Section 8. These documents contain sensitive security information and are only available upon agreement with DigiCert. An overview of the requirements is described in the subsections following.

5.1.1 Site Location and Construction

All STN CA and RA operations shall be conducted within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information and systems.

Such requirements are based in part on the establishment of physical security zone. A zone, such as a locked door or gate, provides mandatory access control for individuals and requires a positive response (e.g., door or gate unlocks or opens) for each individual to proceed to the next area. Each successive zone provides more restricted access and greater physical security against intrusion or unauthorized access.

The minimum level of physical security required by the CA or RA is determined by the highest Class of certificates they process. For example, DigiCert processes and issues Class1, 2 and 3 Certificates and therefore operates at the highest level of security required under the STN. CAs or RAs processing or issuing Class 1 or Class 2 certificates are required to implement a level of security appropriate to the specific class of certificate. CAs and RAs shall describe their Site Location and Construction in more detail in their CPS, a redacted CPS, or in separate confidential documents.

5.1.2 Physical Access

Access to each zone of physical security shall be auditable and controlled so that each zone can be accessed only by authorized personnel.

5.1.3 Power and Air Conditioning

The secure facilities of CAs and RAs shall be equipped with primary and backup power systems to ensure continuous, uninterrupted access to electric power. Also, these secure facilities shall be equipped with primary and backup heating/ventilation/air conditioning systems to control temperature and relative humidity.

5.1.4 Water Exposures

The secure facilities of CAs and RAs shall be constructed and equipped, and procedures shall be implemented, to minimize floods or other damaging exposure to water.

5.1.5 Fire Prevention and Protection

The secure facilities of CAs and RAs shall be constructed and equipped, and procedures shall be implemented, to prevent and extinguish fires or other damaging exposure to flame or smoke. These measures shall meet all local applicable safety regulations.

5.1.6 Media Storage

CAs and RAs shall protect the magnetic media holding back ups of critical system data or any other sensitive information from water, fire, or other environmental hazards, and shall use protective measures to deter, detect, and prevent the unauthorized use of, access to, or disclosure of such media.

5.1.7 Waste Disposal

CAs and RAs shall implement procedures for the disposal of waste (paper, media, or any other waste) to prevent the unauthorized use of, access to, or disclosure of waste containing Confidential/Private Information.

5.1.8 Off-Site Backup

CAs and RAs shall maintain backups of critical system data or any other sensitive information, including audit data, in a secure off-site facility.

5.2 Procedural Controls

5.2.1 Trusted Roles

Employees, contractors, and consultants that are designated to manage infrastructural trustworthiness shall be considered to be “Trusted Persons” serving in a “Trusted Position.” Persons seeking to become Trusted Persons by obtaining a Trusted Position shall meet the screening requirements of this CP.

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, or renewal requests, or enrollment information;
- the issuance, or revocation of Certificates, including (in the case of Processing Centers) personnel having access to restricted portions of its repository or the handling of Subscriber information or requests.

Trusted Persons include, but are not limited to:

- customer service personnel, with the exception of technical support analysts,
- system administration personnel,
- designated engineering personnel, and
- executives that are designated to manage infrastructural trustworthiness.

5.2.2 Number of Persons Required per Task

CAs and RAs shall establish, maintain, and enforce rigorous control procedures to ensure the segregation of duties based on job responsibility and to ensure that multiple Trusted Persons are required to perform sensitive tasks.

Policy and control procedures must be in place to ensure segregation of duties based on job responsibilities. The most sensitive tasks, such as access to and management of CA cryptographic hardware (cryptographic signing unit or CSU) and associated key material, shall require multiple Trusted Persons.

These internal control procedures must be designed to ensure that at a minimum, two trusted personnel are required to have either physical or logical access to the device. Access to CA cryptographic hardware must be strictly enforced by multiple Trusted Persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction. Once a module is activated with operational keys, further access controls must be invoked to maintain split control over both physical and logical access to the device. Persons with physical access to modules shall not hold “Secret Shares” and vice versa.

Other manual operations such as the validation and issuance of Class 3 Certificates, not issued by an automated validation and issuance system, shall require the participation of at least 2 Trusted Persons, or a combination of at least one trusted person and an automated validation and issuance process. Manual operations for Key Recovery may optionally require the validation of two (2) authorized Administrators.

5.2.3 Identification and Authentication for Each Role

CAs and RAs shall confirm the identity and authorization of all personnel seeking to become Trusted before such personnel are:

- issued with their access devices and granted access to the required facilities;

- given electronic credentials to access and perform specific functions on Information Systems and CA or RA systems.

Authentication of identity shall include the personal (physical) presence of such personnel before Trusted Persons performing HR or security functions within an entity, and a check of well-recognized forms of identification, such as passports and driver's licenses. Identity shall be further confirmed through background checking procedures specified in this CP.

5.2.4 Roles Requiring Separation of Duties

Roles requiring Separation of duties include (but are not limited to)

- customer service personnel, with the exception of technical support analysts,
  - 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 handling of Subscriber information or requests
- system administration personnel,
  - the issuance of Certificates, including personnel having access to restricted portions of the repository;
  - generation, issuing or destruction of a CA certificate
- designated engineering personnel,
  - the loading of a CA to a Production environment;
- executives,
  - exclusive to those designated to manage infrastructural trustworthiness.

5.3 Personnel Controls

The STN has documented detailed personnel control and security policies for CAs and RAs to adhere to and be audited against. Compliance with these policies is included in the independent audit requirements described in Section 8. These documents contain sensitive security information and are only available by STN participants under agreement with DigiCert. An overview of the requirements is described in the subsections following.

Personnel controls for the issuance of EV SSL Certificates, EV Code Signing, and Domain-Validated and Organization-Validated SSL Certificates shall be documented in a STN participant's CPS and shall comply with the applicable governing CA/Browser Forum Guidelines published at *www.cabforum.org*.

5.3.1 Qualifications, Experience, and Clearance Requirements

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

5.3.2 Background Check Procedures

CAs and RAs shall conduct background checks for personnel seeking to become Trusted Persons. Background checks shall be repeated for personnel holding Trusted Positions at least every ten (10) years. These procedures shall be subject to any limitations on background checks imposed by local law. To the extent one of the requirements imposed by this section cannot be met due to a prohibition or limitation in local law, the investigating entity shall utilize a substitute investigative technique permitted by law that provides substantially similar information, including but not limited to obtaining a background check performed by the applicable governmental agency.

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

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

Reports containing such information shall be evaluated by human resources and security personnel, and such personnel shall take actions that are reasonable in light of the type, magnitude, and frequency of the behavior uncovered by the background check. Such actions may include measures up to and including the cancellation of offers of employment made to candidates for Trusted Positions or the termination of existing Trusted Persons. The use of information revealed in a background check to take such actions shall be subject to applicable law.

Background investigation of persons seeking to become a Trusted Person includes:

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

Processing Centers and Affiliate Service Centers shall perform the following additional investigations:

- a search of driver’s license records, and
- a search of government social insurance records (analogous to Social Security Administration records in the United States or comparable system outside the United States).

5.3.3 Training Requirements

CAs and RAs shall provide their personnel with the requisite training needed for their personnel to perform their job responsibilities relating to CA or RA operations competently and satisfactorily. They shall also periodically review their training programs, and their training shall address the elements relevant to functions performed by their personnel. Affiliate customer service personnel shall meet DigiCert training requirements, as a condition of the Affiliate beginning operations.

Training programs must address the elements relevant to the particular environment of the person being trained, including:

- Security principles and mechanisms of the STN,
- Hardware and software versions in use,
- All duties the person is expected to perform,
- Incident and Compromise reporting and handling, and
- Disaster recovery and business continuity procedures.

5.3.4 Retraining Frequency and Requirements

CAs and RAs shall provide 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

CAs and RAs shall establish, maintain, and enforce employment policies for the discipline of personnel following unauthorized actions. Disciplinary actions may include measures up to and including termination and shall be commensurate with the frequency and severity of the unauthorized actions.

5.3.7 Independent Contractor Requirements

CAs and RAs may permit independent contractors or consultants to become Trusted Persons only to the extent necessary to accommodate clearly-defined outsourcing relationships and only under the following conditions:

- the entity using the independent contractors or consultants as Trusted Persons does not have suitable employees available to fill the roles of Trusted Persons, and
- the contractors or consultants are trusted by the entity to the same extent as if they were employees.

Otherwise, independent contractors and consultants shall have access to DigiCert's, an Affiliate's, or an Enterprise Customer's secure facility only to the extent they are escorted and directly supervised by Trusted Persons.

5.3.8 Documentation Supplied to Personnel

DigiCert, Affiliates, and Enterprise Customers shall provide their personnel with (including Trusted Persons) the requisite training and access to other documentation needed to perform their job responsibilities competently and satisfactorily.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

The types of auditable events that must be recorded by CAs and RAs are set forth below. All logs, whether electronic or manual, shall contain the date and time of the event, and the identity of the entity that caused the event. CAs shall state in their CPS the logs and types of events they record.

Types of auditable events include:

- Operational events (including but not limited to (1) the generation of a CA's own keys and the keys of subordinate CAs, (2) start-up and shutdown of systems and applications, (3) changes to CA details or keys, (4) cryptographic module lifecycle management-related events (*e.g.*, receipt, use, de-installation, and retirement), (5) possession of activation data for CA private key operations, physical access logs, (6) system configuration changes and maintenance, (7) Records of the destruction of media containing key material, activation data, or personal Subscriber information)
- Certificate lifecycle events (including but not limited to initial issuance, re-key, renew, revocation, suspension)
- Trusted employee events (including but not limited to (1) logon and logoff attempts, (2) attempts to create, remove, set passwords or change the system privileges of the privileged users, (3) personnel changes)

- Discrepancy and compromise reports (including but not limited to unauthorized system and network logon attempts)
- Failed read and write operations on the Certificate and repository
- Changes to Certificate creation policies e.g., validity period

5.4.2 Frequency of Processing Log

Audit logs shall be reviewed in response to alerts based on irregularities and incidents within their CA/RA systems. Processing Centers shall compare their audit logs with the supporting manual and electronic logs from their RA Customers and Service Centers when any action is deemed suspicious.

Audit log processing shall consist of a monthly review of the audit logs and documenting the reason for all significant events in an audit log summary. Audit log reviews shall include a verification that the log has not been tampered with, an inspection of all log entries, and an investigation of any alerts or irregularities in the logs. Actions taken based on audit log reviews shall be 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

Incremental backups of audit logs are created daily and full backups are performed weekly.

5.4.6 Audit Collection System (Internal vs. External)

No stipulation

5.4.7 Notification to Event-Causing Subject

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

5.4.8 Vulnerability Assessments

Events in the audit process are logged, in part, to monitor system vulnerabilities. Logical security vulnerability assessments (“LSVAs”) are performed, reviewed, and revised following an examination of these monitored events. LSVAs are based on real-time automated logging data and are performed on a daily, monthly, and annual basis. An annual LSVA will be an input into an entity’s annual Compliance Audit.

5.5 Records Archival

5.5.1 Types of Records Archived

RAs and CAs archive:

- All audit data collected in terms of Section 5.4
- Certificate application information
- Documentation supporting certificate applications, including CAA results
- Certificate lifecycle information e.g., revocation, rekey and renewal application information

5.5.2 Retention Period for Archive

Records shall be retained for at least 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
- Twenty (20) years and six (6) months for Class 4 Certificates

5.5.3 Protection of Archive

An entity maintaining an archive of records shall protect the archive so that only the entity's 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 CP.

5.5.4 Archive Backup Procedures

Entities compiling electronic information shall incrementally back up system archives of such information on a daily basis and perform full backups on a weekly basis. Copies of paper-based records shall be maintained in an off-site secure facility.

5.5.5 Requirements for Time-Stamping of Records

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

5.5.6 Archive Collection System (Internal or External)

Archive collection systems for entities within the STN shall be internal, except for enterprise RA Customers. Processing Centers shall assist their enterprise RAs in preserving an audit trail. Such an archive collection system therefore is external to that enterprise RA. Otherwise, entities within the STN shall utilize internal archive collection systems.

5.5.7 Procedures to Obtain and Verify Archive Information

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

5.6 Key Changeover

A CA Certificate may be renewed if the CA's Superior Entity reconfirms the identity of the CA. Following such reconfirmation, the Superior Entity shall either approve or reject the renewal application.

Following an approval of a renewal request, the Superior Entity shall conduct a Key Generation Ceremony in order to generate a new key pair for the CA. During such Key Generation

Ceremony, the Superior Entity shall sign and issue the CA a new Certificate. Such Key Generation Ceremony shall meet the Key Ceremony requirements documented in the STN's confidential security policies. New CA Certificates containing the new CA public keys generated during such Key Generation Ceremony shall be made available to Relying Parties.

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. Processing Centers shall maintain backups of the foregoing CA information for their own CAs, as well as the CAs of Service Centers and Enterprise Customers within their Sub-domains.

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

Following corruption of computing resources, software, and/or data, a report of the incident and a response to the event, shall be promptly made by the affected CA or RA in accordance with the DigiCert's documented incident and Compromise reporting and handling procedures in the applicable CPS and the STN's documented confidential security policies.

5.7.3 Entity Private Key Compromise Procedures

In the event of a CA private key compromise that CA will be revoked. Processing Centers use commercially reasonable efforts to notify potential Relying Parties if they discover, or have reason to believe, that there has been a Compromise of the private key of a CA within their sub-domain of the STN.

5.7.4 Business Continuity Capabilities after a Disaster

STN entities operating secure facilities for CA and RA operations develop, test, maintain and, if necessary, implement a Disaster Recovery Plan (DRP) designed to mitigate the effects of any kind of natural or man-made disaster. The DRP shall identify conditions for activating the plan and what constitutes an acceptable system outage and recovery time for the restoration of information systems services and key business functions within a defined recovery time objective (RTO). Additionally, the DRP shall include:

- Frequency for taking backup copies of essential business information and software,
- Requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location,
- Separation distance of the Disaster recovery site to the CA's main site,
- 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.

The DRP shall include administrative requirements including:

- maintenance schedule for the plan;
- Awareness and education requirements;
- Responsibilities of the individuals; and
- Regular testing of contingency plans.

Disaster recovery sites have the equivalent physical security protections specified by the STN.

Processing Centers have the capability of restoring or recovering essential operations within twenty-four (24) hours following a disaster with, at a minimum, support for the following functions: Certificate issuance, Certificate revocation, publication of revocation information, and providing key recovery information for Enterprise Customers using Managed PKI Key Manager. A Processing Center's disaster recovery database shall be synchronized with the production database within the time limits set forth in the Security and Audit Requirements Guide. A Processing Center's disaster recovery equipment shall have the physical security protections documented in the STN's confidential security policies, which includes the enforcement of physical security zone.

Service Centers have the capability of declaring a disaster on their web sites in their local languages and English, and of directing Subscribers, Relying Parties, and other interested persons to a Processing Center supporting their lifecycle services.

A Service Center or Processing Center disaster recovery plan makes provision for full recovery within one week following disaster occurring at the Service Center's or Processing Center's primary site. Each Service Center and Processing Center shall install and test equipment at its primary site to support CA/RA functions following all but a major disaster that would render the entire facility inoperable. Such equipment ensures redundancy and fault tolerance.

For the issuance of EV SSL Certificates, EV Code Signing, and Domain-Validated and Organization-Validated SSL Certificates, practices for Business Continuity shall be documented in a STN participant's CPS and shall comply with section 16 of the applicable governing CA/Browser Forum Guidelines published at *www.cabforum.org*.

5.8 CA or RA Termination

The termination of a non-DigiCert CA or RA (Affiliate, enterprise Customer) shall be subject to the agreement entered into between the CA to be terminated and its Superior Entity. Both parties shall, in good faith, use commercially reasonable effort to agree on a termination plan that minimizes disruption to Customers, Subscribers, and Relying Parties. The termination plan may cover issues such as:

- Providing notice to parties affected by the termination, such as Subscribers, Relying Parties, and Customers,
- handling of the cost of such notice,
- The revocation of the Certificate issued to the CA by the Superior Entity,
- The preservation of the CA's archives and records for the time periods required in this CP
- 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,
- The refund (if necessary) to Subscribers whose unexpired, unrevoked Certificates are revoked under the termination plan or provision, for the issuance of substitute Certificates by a successor CA,
- Disposition of the CA's private key and the hardware token containing such private key,
- 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 Domain-Validated and Organization-Validated SSL Certificates, Data Security practices shall be documented in a STN participant's CPS and shall comply with section 16 of the applicable CA/Browser Forum Guidelines published at *www.cabforum.org*.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Key pair generation shall be performed using Trustworthy Systems and processes that provide the required cryptographic strength of the generated keys and prevent the loss, disclosure, modification, or unauthorized use of private keys. This requirement applies to end-user Subscribers, Enterprise Customers using Managed PKI Key Manager, CAs pre-generating key pairs on end-user Subscriber hardware tokens and Processing Centers. Processing Centers generate the CA key pairs of the Client Service Centers, and Enterprise Customers in their Sub-domains.

CA keys are generated in a Key Generation Ceremony. All Key Generation Ceremonies conform to the requirements documented in the STN's confidential security policies.

6.1.2 Private Key Delivery to Subscriber

End-user Subscribers' private keys are generally generated by the end-user Subscribers themselves, and therefore private key delivery to a Subscriber is unnecessary. Private keys shall be delivered to end-user Subscribers only when:

- Their Certificate Applications are approved by an Enterprise Customer using Managed PKI Key Manager, or
- Their key pairs are pre-generated on hardware tokens, which are distributed to Certificate Applicants in connection with the enrollment process.

Enterprise Customers using Managed PKI Key Manager (or an equivalent service approved by DigiCert) shall use the Managed PKI Key Manager Software (or equivalent software approved by DigiCert) and Trustworthy Systems to deliver private keys to Subscribers and shall secure such delivery through the use of a PKCS#12 package or any other comparably equivalent means (e.g., encryption) in order to prevent the loss, disclosure, modification, or unauthorized use of such private keys. Where key pairs are pre-generated on hardware tokens, the entities distributing such tokens shall take commercially reasonable efforts to provide physical security of the tokens to prevent the loss, disclosure, modification, or unauthorized use of the private keys on them. SSL/TLS and S/MIME email signature certificates shall not be distributed as PKCS#12 packages. S/MIME encryption certificates can 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

When a public key is transferred to the issuing CA to be certified, it shall be delivered through a mechanism ensuring that the public key has not been altered during transit. It may include a process of proving the Certificate Applicant possesses the private key corresponding to the transferred public key. The acceptable mechanism within the STN for public key delivery is a PKCS#10 Certificate signing request package or an equivalent method checking that:

- The public key has not been altered during transit; and
- May verify the Certificate Applicant possesses the private key corresponding to the transferred public key.

Processing Centers performing Key Generation Ceremonies transfer the public key from the cryptographic module where it was created to the cryptographic module of the superior CA (same cryptographic module if a PCA) by wrapping it in a PKCS#10 Certificate signing request.

6.1.4 CA Public Key Delivery to Relying Parties

The public keys of the PCAs are included in Root Certificates that are already embedded within many popular software applications, making special root distribution mechanisms unnecessary.[12] Also, in many instances, a Relying Party using the S/MIME protocol will automatically receive, in addition to the Subscriber's Certificate, the Certificates (and therefore the public keys) of all CAs subordinate to the relevant PCA.

6.1.5 Key Sizes

Key pairs shall be of sufficient length to prevent others from determining the key pair's private key using cryptanalysis during the period of expected utilization of such key pairs. The STN Standard for minimum key sizes is the use of key pairs equivalent in strength to 2048-bit RSA for PCAs and CAs.[13]

DigiCert issues a minimum key size equivalent in strength to 2048-bit RSA for RAs and end entity certificates key pairs.

DigiCert recommends the use of a minimum key size equivalent in strength to 256-bit ECC for PCA, CA, Registration Authority and end entity certificate key pairs.

The STN Standard for digital signature hash algorithm is SHA-2. SHA-1 may be used to support legacy applications provided that such usage does not violate procedures and policies set forth by the CA/Browser Forum and related Application Software Suppliers. Individual Certification Practice Statements subordinate to this CP and covering specific sub-trees of the STN hierarchy may further restrict or prohibit the use of SHA1 for those certificates governed by them.

6.1.5.1 CABF Requirements for Key Sizes

Key Sizes for EV SSL Certificates, EV Code Signing, and Domain-Validated and Organization-Validated SSL Certificates, shall be documented in a STN participant's CPS and shall comply with section 6.1.5 of the applicable governing CA/Browser Forum Guidelines published at *www.cabforum.org*.

6.1.6 Public Key Parameters Generation and Quality Checking

STN Participants using the Digital Signature Standard shall generate the required Key Parameters in accordance with FIPS 186-2 or a DCPA-approved equivalent standard.

When STN Participants use the Digital Signature Standard, the quality of the generated Key Parameters shall be verified in accordance with FIPS 186-2 or a DCPA-approved equivalent standard.

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

Refer to Section 7.1.2.1.

[12] The Class 1 PCA used to support rudimentary non-federal SSP certificates is not generally distributed and is only made available to legacy Symantec Non-Federal SSP customers

[13] DigiCert may retain legacy Trusted Roots with 1024-bit RSA key pairs for support of customer legacy platforms for issuance of 1024-bit RSA end-entity certificates for a limited period.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

Private keys within the STN shall be protected using a Trustworthy System and private key holders shall take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of such Private Keys in accordance with this CP, contractual obligations and requirements documented in the STN's confidential security policies. End-user Subscribers have the option of protecting their private keys in a smart card or other hardware token. DigiCert and enterprise RA customers shall protect private key segments on these servers using a Trustworthy System.

Processing Centers shall perform all CA cryptographic operations on cryptographic modules rated at a minimum of FIPS 140-2 level 3. Service Centers shall perform all RA cryptographic operations on a cryptographic module rated at FIPS 140-2 level 2. 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. The requirements for ratings in this section are subject to any applicable local requirements for higher ratings.

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

Multi-person controls are enforced to protect the activation data needed to activate CA private keys held by Processing Centers in accordance with the standards documented in the STN's confidential security policies. Processing Centers use "Secret Sharing" to split the private key or activation data needed to operate the private key into separate parts called "Secret Shares" held by individuals called "Shareholders." Some threshold number of Secret Shares (m) out of the total number of Secret Shares (n) shall be required to operate the private key.

Processing Centers utilize Secret Sharing to protect the activation data needed to activate their own private keys and other CAs within their respective Subdomains in accordance with the standards documented in the STN's confidential security policies. Processing Centers also use Secret Sharing to protect the activation data needed to activate private keys located at their respective disaster recovery sites.

The threshold number of shares needed to sign a CA certificate is 3. It should be noted that the number of shares distributed for disaster recovery tokens may be less than the number distributed for operational tokens, while the threshold number of required shares remains the same.

6.2.3 Private Key Escrow

CA private keys are not escrowed. Escrow of private keys for end user subscribers is explained in more detail in Section 4.12.

6.2.4 Private Key Backup

CAs shall back up their own private keys so as to be able to recover from disasters and equipment malfunction in accordance with the standards documented in the STN's confidential security policies. Processing Centers shall also back up the private keys of CAs within their Subdomains. Backups shall be made in accordance with these documented policies. Back-ups shall be made by copying such private keys and entering them onto back-up cryptographic modules in accordance with Section 6.2.6 and 6.2.7.

Private keys that are backed up are to be protected from unauthorized modification or disclosure through physical or cryptographic means. Backups are protected with a level of physical and cryptographic protection equal to or exceeding that for cryptographic modules within the CA site, such as at a disaster recovery site or at another secure off-site facility, such as a bank safe.

The backup of end-user Subscriber private keys subject to the Managed PKI Key Manager service, is governed by Section 4.12. DigiCert recommends that Enterprise Customers having Automated Administration tokens and Class 3 end-user Subscribers who are not subject to the Managed PKI Key Manager service back up their private keys and protect them from unauthorized modification or disclosure by physical or cryptographic means.

6.2.5 Private Key Archival

Except for CA certificates that are signed by the US Federal Bridge CA, upon expiration of a STN CA Certificate, the key pair associated with the certificate will be securely retained for a period of at least 5 years using hardware cryptographic modules that meet the requirements of this CP. These CA key pairs shall not be used for any signing events after the expiration date of the corresponding CA Certificate, unless the CA Certificate has been renewed in terms of this CP. For CA certificates that chain to the Federal Bridge CA, DigiCert will destroy such CA keys when a Shared Service Provider customer terminates their service agreement with DigiCert.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

Entry of a private key into a cryptographic module shall use mechanisms to prevent loss, theft, modification, unauthorized disclosure, or unauthorized use of such private key.

Processing Centers generating CA or RA private keys on one hardware cryptographic module and transferring them into another shall securely transfer such private keys into the second cryptographic module to the extent necessary to prevent loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys. Such transfers shall be limited to making backup copies of the private keys on tokens in accordance with the standards documented in the STN's confidential security policies. Private keys shall be encrypted during such transfer.

STN Participants pre-generating private keys and transferring them into a hardware token, for example transferring generated end-user Subscriber private keys into a smart card, shall securely transfer such private keys into the token to the extent necessary to prevent loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys.

6.2.7 Private Key Storage on Cryptographic Module

CA or RA private keys held on hardware cryptographic modules shall be stored in encrypted form.

6.2.8 Method of Activating Private Key

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

6.2.8.1 Class 1 Certificates

The STN Standard for Class 1 private key protection is for Subscribers to 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. In addition, DigiCert recommends that Subscribers 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, a Windows logon or screen saver password, or a network logon password.

6.2.8.2 Class 2 Certificates

The STN 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 STN Standard for Class 3 private key protection (other than Administrators) is for 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.

6.2.8.4 Administrators' Private Keys (Class 3)

The STN Standard for Administrators' private key protection requires them to:

- Use a smart card, biometric access device, password in accordance with Section 6.4.1, or security of equivalent strength to authenticate the Administrator before the activation of the private key, which includes, for instance, a password to operate the private key, a Windows logon or screen saver password, or a network logon password; and
- Take commercially reasonable measures for the physical protection of the Administrator's workstation to prevent use of the workstation and its associated private key without the Administrator's authorization.

DigiCert recommends that Administrators use a smart card, biometric access device, or security of equivalent strength along with the use of a password in accordance with Section 6.4.1 to authenticate the Administrator before the activation of the private key.

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

6.2.8.5 Enterprise RAs using a Cryptographic Module (with Automated Administration or with Managed PKI Key Manager Service)

The STN Standard for private key protection for Administrators using such a cryptographic module requires them to:

- Use the cryptographic module along with a password in accordance with Section 6.4.1 to authenticate the Administrator before the activation of the private key; and

- Take commercially reasonable measures for the physical protection of the workstation housing the cryptographic module reader to prevent use of the workstation and the private key associated with the cryptographic module without the Administrator'sauthorization.

6.2.8.6 Private Keys Held by Processing Centers (Class 1-3)

An online CA's private key shall be activated by a threshold number of Shareholders, as defined in Section 6.2.2, supplying their activation data (stored on secure media). Once the private key is activated, the private key may be active for an indefinite period until it is deactivated when the CA goes offline. Similarly, a threshold number of Shareholders shall be required to supply their activation data in order to activate an offline CA's private key. Once the private key is activated, it shall be active only for one time.

6.2.9 Method of Deactivating Private Key

Class 3 End-user Subscribers have an obligation to protect their private keys. Such obligations extend to protection of the private key after a private key operation has taken place. The private key may be deactivated after each operation, upon logging off their system, or upon removal of a smart card from the smart card reader depending upon the authentication mechanism employed by the user.

When an online CA is taken offline by a Processing Center, the Processing Center's personnel shall remove the token containing such CA's private key from the reader in order to deactivate it. With respect to the private keys of offline CAs, after the completion of a Key Generation Ceremony, in which such private keys are used for private key operations, the Processing Center's personnel shall remove the token containing such CAs' private keys from the reader in order to deactivate them. Once removed from the reader, tokens shall be protected in accordance to the Security and Audit Requirements Guide.

6.2.10 Method of Destroying Private Key

Where required, CA private keys are destroyed in a manner that reasonably ensures that there are no residuals remains of the key that could lead to the reconstruction of the key. Processing Center personnel decommission the CA's private key by deleting it using functionality of the token containing such CA's private key so as to prevent its recovery following deletion, while not adversely affecting the private keys of other CAs contained on the token. This process shall be witnessed in accordance with the standards documented in the STN's confidential security policies.

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

CAs shall archive their own public keys, as well as the public keys of all CAs within their Sub-domains, in accordance Section 5.5.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The Operational Period for Certificates shall be set according to the time limits set forth in Table 5 below[14]. End user Subscriber Certificates that are renewals of existing subscriber certificates may have a longer validity period (up to 3 months).

The usage period for end-user Subscriber key pairs is the same as the Operational Period for their Certificates, except that private keys may continue to be used after the Operational Period for decryption and signature verification. The Operational Period of a Certificate ends upon its expiration or revocation. A CA shall not issue Certificates if their Operational Periods would extend beyond the usage period of the key pair of the CA. Therefore, the CA key pair usage period is necessarily shorter than the operational period of the CA Certificate. Specifically, the usage period is the Operational Period of the CA Certificate minus the Operational Period of the Certificates that the CA issues. Upon the end of the usage period for a Subscriber or CA key pair, the Subscriber or CA shall thereafter cease all use of the key pair, except to the extent a CA needs to sign revocation information until the end of the Operational Period of the last Certificate it has issued.

Certificate Issued By:	*Validity Period*
PCA self-signed (2048 bit RSA)	Up to 25 years
PCA self-signed (256 bit ECC)	Up to 25 years
PCA self-signed (384 bit ECC)	Up to 25 years
PCA to Offline intermediate CA	Generally 10 years but up to 15 years after renewal
PCA to online CA	Generally 5 years but up to 10 years after renewal
Offline intermediate CA to online CA	Generally 5 years but up to 10 years after renewal[15]
Online CA to End-user individual Subscriber	Normally up to 3 years, but under the conditions described below, up to 6 years[16] with no option to renew or re-key. After 6 years new enrollment is required.
Online CA to End-Entity Organizational Subscriber	Normally up to 3 years.[17] NOTE: SSL certificates may be valid for up to 825 days as per section 6.3.2.1.

Table 5 – Certificate Operational Periods

Except as noted in this section, STN 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:

- Protection of the Subscriber key pairs in relation to its operational environment for Organization Certificates, operation with the enhanced protection of a data center and for Individual Certificates, the Subscribers' key pairs reside on a hardware token, such as a smart card,
- Subscribers are required to undergo re-authentication procedures at least every 3 years under Section 3.2.3,

[14] Individual exceptions must be approved by DigiCert for certificate validity periods beyond the limits set in Section 6.3.2 and are strictly limited to certificates using stronger encryption algorithms or longer key lengths, e.g. the use of SHA 2 or ECC algorithms and/or the use of 4096 bit or larger keys. In consideration of approval, additional requirements for protection of the private key may be imposed, such as generation and storage on a Hardware device.

[15] If 6-year end-user subscriber certificates are issued, the online CA certificate's operational period will be 10 years with no option to renew. CA re-key will be required after 5 years.

[16] If 6-year end-user subscriber certificates are issued, the online CA certificate's operational period will be 10 years with no option to renew. CA re-key will be required after 5 years.

[17] Organizational end-entity certificates used solely to support the operation of a portion of the STN may be issued with a validity period of 6 years and up to a maximum of 10 years after renewal.

- If a Subscriber is unable to complete re-authentication procedures under Section 3.2.3 successfully or is unable to prove possession of such private key when required by the foregoing, the CA shall automatically revoke the Subscriber's Certificate.

Certificates issued to individual Subscribers of the legacy Symantec Non-Federal Shared Services Provider PKI may have a 3-year validity.

Any exception to this procedure requires approval from the DCPA and must be documented in the relevant CPS.

6.3.2.1 CABF Validity Period and Validation Data Reuse Requirements

Validity periods for EV SSL Certificates, EV Code Signing, and Domain-Validated and Organization-Validated SSL Certificates, shall be documented in a STN participant's CPS and shall comply with the applicable governing CA/Browser Forum Guidelines published at *www.cabforum.org*.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

STN Participants generating and installing activation data for their private keys shall use methods that protect the activation data to the extent necessary to prevent the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys.

To the extent passwords are used as activation data, Subscribers shall generate passwords that cannot easily be guessed or cracked by dictionary attacks. Class 3 end-user Subscribers may not need to generate activation data, for example if they use biometric access devices.

Processing Centers generate activation data for their own CAs' private keys, and for the private keys of CAs and RAs within their Sub-domains, in accordance with the Secret Sharing requirements of this CP and the standards documented in the STN's confidential security policies.

6.4.2 Activation Data Protection

STN Participants shall protect the activation data for their private keys using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys.

End-user Subscribers shall protect the activation data for their private keys, if any, to the extent necessary to prevent the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys

Processing Centers utilize Secret Sharing in accordance with this CP and the standards documented in the STN's confidential security policies. Processing Centers provide the procedures and means to enable Shareholders to take the precautions necessary to prevent the loss, theft, modification, unauthorized disclosure, or unauthorized use of the Secret Shares that they possess. Shareholders shall not:

- Copy, disclose, or make the Secret Share available to a third party, or make any unauthorized use of it whatsoever; or
- disclose his, her, or any other person's status as a Shareholder to any third party.

The Secret Shares and any information disclosed to the Shareholder in connection with his or her duties as a Shareholder constitute Confidential/Private Information.

Processing Centers include in their disaster recovery plans provisions for Shareholders making their Secret Shares available at a disaster recovery site after a disaster. Each Processing Center maintains an audit trail of Secret Shares, and Shareholders shall participate in the maintenance of an audit trail.

6.4.3 Other Aspects of Activation Data

6.4.3.1 Activation Data Transmission

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

6.4.3.2 Activation Data Destruction

Activation data for CA private keys shall be decommissioned using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of the private keys protected by such activation data. After the record retention periods in Section 5.5.2 lapses, Processing Centers shall decommission activation data by overwriting and/or physical destruction.

6.5 Computer Security Controls

CA and RA functions take place on Trustworthy Systems in accordance with the standards documented in the STN's confidential security policies (in the case of DigiCert and Affiliates).

6.5.1 Specific Computer Security Technical Requirements

Processing Centers shall ensure that the systems maintaining CA software and data files are Trustworthy Systems secure from unauthorized access, which can be demonstrated by compliance with audit criteria applicable under Section 5.4.1. In addition, Processing Centers limit access to production servers to those individuals with a valid business reason for access. General application users shall not have accounts on the production servers.

Processing Centers shall have production networks logically separated from other components. This separation prevents network access except through defined application processes. Processing Centers shall use firewalls to protect the production network from internal and external intrusion and limit the nature and source of network activities that may access production systems.

Processing Centers shall require the use of passwords with a minimum character length and a combination of alphanumeric and special characters, and shall require that passwords be changed on a periodic basis and whenever necessary. Direct access to a Processing Center's database maintaining the Processing Center's repository shall be limited to Trusted Persons in the Processing Center's operations group having a valid business reason for such access.[18]

[18] Gateway servers shall include the following functionality: access control to CA services, identification and authentication for launching of CA services, object re-use for CA random access memory, use of cryptography for session communication and database security, archival of CA and end-user Subscriber history and audit data, audit of security related events, self-test of security related CA services, and Trusted path for identification of PKI roles and associated identities

RAs shall ensure that the systems maintaining RA software and data files are Trustworthy Systems secure from unauthorized access, which can be demonstrated by compliance with audit criteria applicable under Section 5.4.1.

RAs shall logically separate access to these systems and this information from other components. This separation prevents access except through defined processes. RAs shall use firewalls to protect the network from internal and external intrusion and limit the nature and source of activities that may access such systems and information. RAs shall require the use of passwords with a minimum character length and a combination of alphanumeric and special characters, and shall require that passwords be changed on a periodic basis and asnecessary. Direct access to the RA's database maintaining Subscriber information shall be limited to Trusted Persons in the RA's operations group having a valid business reason for such access.

6.5.1.1 CABF Requirements for System Security

For the issuance of EV SSL, EV Code Signing and Domain-Validated and Organization-Validated SSL Certificates, system security shall be documented in a STN participant's CPS and shall comply with the applicable governing CA/Browser Forum Guidelines published at *www.cabforum.org* .

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

DigiCert provides software for CA and RA functions to Processing Centers, Service Centers, and RAs. Such software, to the extent used to manage Class 2 or 3 Certificates, shall be developed within a systems development environments that meet DigiCert's development assurance requirements. DigiCert shall use a design and development process that enforces quality assurance and process correctness.

The software provided by DigiCert, when first loaded, shall provide a method for the entity 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

Software for CA and RA functions designed to manage Class 2 or 3 Certificates shall be subject to checks to verify its integrity. DigiCert provides a hash of all software packages or software updates it provides. This hash can be used to verify the integrity of such software manually. Processing Centers shall also have mechanisms and/or policies in place to control and monitor the configuration of their CA systems. Upon installation, and at least once a day, Processing Centers shall validate the integrity of the CA system.

6.6.3 Life Cycle Security Controls

No stipulation

6.7 Network Security Controls

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

6.8 Time-Stamping

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

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

STN 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")[19]. 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.

At a minimum, X.509 STN Certificates shall contain the basic fields and indicated prescribed values or value constraints in Table 6 below:

Field	*Value or Value constraint*
Serial Number	Unique value per Issuer DN that contains at least 64 bits of entropy output from a CSPRNG.
Signature Algorithm	Object identifier of the algorithm used to sign the certificate (See CP § 7.1.3)
Issuer DN	See Section 7.1.4
Valid From	Universal Coordinated Time base. Synchronized to Master Clock of U.S. Naval Observatory. Encoded in accordance with RFC 5280.
Valid To	Universal Coordinated Time base. Synchronized to Master Clock of U.S. Naval Observatory. Encoded in accordance with RFC 5280.
Subject DN	See CP § 7.1.4
Subject Public Key	Encoded in accordance with RFC 5280
Signature	Generated and encoded in accordance with RFC 5280

Table 6 – Certificate Profile Basic Fields

7.1.1 Version Number(s)

STN Certificates shall be X.509 Version 3 Certificates although certain Root Certificates are permitted to be X.509 Version 1 Certificates to support legacy systems. CA certificates shall be X.509 Version 1 or Version 3 CA Certificates. End-user Subscriber Certificates shall be X.509 Version 3.

[19] While STN certificates generally conform to RFC 5280, certain limited provisions may not be supported.

7.1.2 Certificate Extensions

Processing Centers shall populate X.509 Version 3 STN Certificates with the extensions required by Section 7.1.2.1-7.1.2.8. Private extensions are permissible, but the use of a private extension(s) is not warranted under this CP and the applicable CPS unless specifically included by reference.

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.

Note: The non-Repudiation bit[20] is not required to be set in these Certificates because the PKI industry has not yet reached a consensus as to what the non-Repudiation bit means. Until such a 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 CP 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

CertificatePolicies extension of X.509 Version 3 Certificates are populated with the object identifier of this CP in accordance with Section 7.1.6 and with policy qualifiers set forth in 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

The Certificate Policies extension for EV SSL, EV Code Signing and Domain-Validated and Organization-Validated SSL Certificates, shall be documented in a STN participant's CPS and shall comply with the applicable governing CA/Browser Forum Guidelines published at *www.cabforum.org* .

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 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.

[20] The non-Repudiation bit may also be referred to as ContentCommitment in Digital Certificates in accordance with the X.509 standard

7.1.2.4 Basic Constraints

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.

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. CA Certificates issued to an online Enterprise Customer issuing end-user Subscriber Certificates shall have a "*pathLenConstraint*" field set to a value of "0" indicating that only an end-user Subscriber Certificate may follow in the certification path. End-user Subscriber certificates shall not contain the path length constraint attribute.

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

7.1.2.6 CRL Distribution Points

X.509 Version 3 STN Certificates are populated with a *cRLDistributionPoints* extension containing the URL of the location where a Relying Party can obtain a CRL to check the Certificate's status. The criticality field of this extension shall be set to FALSE. URLs shall comply with Mozilla requirements to exclude the LDAP protocol, and may appear multiple times within a *cRLDistributionPoints* extension.

7.1.2.7 Authority Key Identifier

X.509 Version 3 STN Certificates are generally populated with an *authorityKeyIdentifier* extension The method for generating the *keyIdentifier* based on the public key of the CA issuing the Certificate shall be calculated in accordance with one of the methods described in RFC 5280. The criticality field of this extension shall be set to FALSE.

7.1.2.8 Subject Key Identifier

If present in X.509 Version 3 STN Certificates, the criticality field of this extension shall be set to FALSE and the method for generating the *keyIdentifier* based on the public key of the Subject of the Certificate shall be calculated in accordance with one of the methods described in RFC 5280.

7.1.3 Algorithm Object Identifiers

STN Certificates are signed using one of following algorithms.

- ***sha256withRSAEncryption*** OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
- ***ecdsa-with-Sha256*** OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840)ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 2}
- ***ecdsa-with-Sha384*** OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840)ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 3}

- ***sha-1WithRSAEncryption*** OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}

Certificate signatures produced using these algorithms shall comply with RFC 3279. *sha-256WithRSAEncryption* is used over sha-1*WithRSAEncryption*[21].

Certain versions of Processing Center support the use of SHA-256, SHA-384 and SHA-512 encryption algorithms in end-entity Subscriber Certificates.

7.1.4 Name Forms

STN Certificates are populated with the Issuer Name and Subject Distinguished Name required under Section 3.1.1. The Issuer Name shall be populated in each Certificate issued containing the Country, Organization Name and the Common Name of the Issuing CA.

In addition, end-user Subscriber Certificates may include an additional Organizational Unit field that contains a notice stating that the terms of use of the Certificate are set forth in a URL, and the URL shall be a pointer to the applicable Relying Party Agreement. Exceptions to the foregoing requirement shall be permitted when space, formatting, or interoperability limitations within Certificates make such an Organizational Unit impossible to use in conjunction with the application for which the Certificates are intended, or if a pointer to the applicable Relying Party Agreement is included in the policy extension of the certificate.

7.1.5 Name Constraints

No stipulation

7.1.6 Certificate Policy Object Identifier

The object identifier for the Certificate policy corresponding to each Class of Certificate is set forth in Section 1.2. The *CertificatePolicies* extension in each X.509 Version 3 STN Certificate is populated in accordance with Section 1.2.[22]

7.1.6.1 CABF Requirements for Certificate Policy Object Identifier

Certificate Policy OIDs for EV SSL Certificates, EV Code Signing, and Domain-Validated and Organization-Validated SSL Certificates, shall be documented in a STN participant's CP or CPS and shall comply with the applicable governing CA/Browser Forum Guidelines published at *www.cabforum.org* .

7.1.7 Usage of Policy Constraints Extension

No stipulation

7.1.8 Policy Qualifiers Syntax and Semantics

X.509 Version 3 STN Certificates may contain 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 applicable CPS. In addition, some Certificates contain a User Notice Qualifier which points to the applicable Relying Party Agreement.

[21] sha-1*WithRSAEncryption* is used only with prior approval to preserve business continuity of legacy applications.

[22] Certain certificates issued under the STN may contain legacy policy OIDS assigned under the STN.

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.

Version 2 CRLs conform to RFC 5280 and contain the basic fields and contents specified in Table 8 below:

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 CP § 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 accordance with the requirements of Section 4.9.7.
Revoked Certificates	Listing of revoked certificates, including the Serial Number of the revoked Certificate and the Revocation Date.

Table 8 – CRL Profile Basic Fields

7.2.1 Version Number(s)

The STN supports both X.509 Version1 and Version 2 CRLs.

7.2.2 CRL and CRL Entry Extensions

No stipulation

7.3 OCSP Profile

OCSP (Online Certificate Status Protocol) is a way to obtain timely information about the revocation status of a particular certificate. DigiCert validates:

- Class 2 Enterprise certificates using the Enterprise OCSP which conforms to RFC 2560, and
- Class 2 Enterprise certificates and Class 3 organization certificates using the DigiCert Trusted Global Validation (TGV) service which conforms to RFC 6960, excluding client requested cipher support.

CABF Requirement for OCSP Signing

For EV SSL Certificates, EV Code Signing, and Domain-Validated and Organization-Validated SSL Certificates, the OCSP signing requirements shall be documented in a STN participant's CPS and shall comply with the applicable governing CA/Browser Forum Guidelines published at *www.cabforum.org*.

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

DigiCert TGV Service uses secure timestamp and validity period to establish the current freshness of each OCSP response. DigiCert does not use a nonce to establish the current freshness of each OCSP response and clients should not expect a nonce in the response to a request that contains a nonce. Instead, clients should use the local clock to check for response freshness.

8. Compliance Audit and Other Assessments

DigiCert and Affiliates undergo a periodic compliance audit ("Compliance Audit") to ensure compliance with STN Standards after they begin operations. These audits test and report compliance against WebTrust "Principles and Criteria for Certification Authorities - Version 2.0" or later, and where applicable, WebTrust "Principles and Criteria for Certification Authorities – SSL Baseline with Network Security - Version 2.2" or later, WebTrust "Principles and Criteria for Certification Authorities - Extended Validation SSL 1.4.5" or later and/or WebTrust Principles and Criteria for Certification Authorities - Extended Validation Code Signing.

In addition to these compliance audits, DigiCert and Affiliates shall be entitled to perform other reviews and investigations to ensure the trustworthiness 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 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 or the Superior Entity of the entity to be audited has reason to believe that the audited entity has failed to meet STN Standards, has experienced an incident or compromise, or has acted or failed to act, such that the audited entity's failure, the incident or compromise, or the act or failure to act poses an actual or potential threat to the security or integrity of the STN.
- DigiCert shall be entitled to perform "Supplemental Risk Management Reviews" on itself, an Affiliate, or a Customer following incomplete or exceptional findings in a Compliance Audit or as part of the overall risk management process in the ordinary course of business.

DigiCert shall be entitled to delegate the performance of these audits, reviews, and investigations to the Superior Entity of the entity being audited, reviewed, or investigated or to a third party audit firm. Entities that are subject to an audit, review, or investigation shall provide reasonable cooperation with DigiCert and the personnel performing the audit, review, or investigation.

CABF Audit Requirement

For the issuance of EV SSL Certificates, EV Code Signing, and Domain-Validated and Organization-Validated SSL Certificates, Audit practices including self-audits shall be documented in a STN participant's CPS and shall comply with the applicable governing CA/Browser Forum Guidelines published at *www.cabforum.org*.

8.1 Frequency and Circumstances of Assessment

Compliance Audits are conducted at least annually at the sole expense of the audited entity. Audits shall be conducted over unbroken sequences of audit periods with each period no longer than one year duration. In a period-of-time audit, an audit period is the period between the first day (start) and the last day of operations (end) covered by the auditors in their engagement.

8.2 Identity/Qualifications of Assessor

A third party auditing firm shall perform the Compliance Audits of DigiCert and Affiliates.

Reviews and audits performed by an independent third party audit firm shall be performed by a certified public accounting firm with demonstrated expertise in computer security or by accredited computer security professionals employed by a competent security consultancy. Such firm shall also have demonstrated expertise in the performance of IT security and PKI compliance audits and the selected Audit Scheme.

The qualified auditor shall be bound by law, government regulation, or professional code of ethics; and, except in the case of an Internal Government Auditing Agency, shall maintain Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage. The qualified auditor shall be licensed by WebTrust to perform audits in the jurisdiction of primary CA operations.

8.3 Assessor's Relationship to Assessed Entity

Compliance Audits performed by third-party audit firms shall be conducted by firms independent of the audited entity. Such firms shall not have a conflict of interest that hinders their ability to perform auditing services.

8.4 Topics Covered by Assessment

Audit topics for each category of entity are set forth below. The audited entity may make a Compliance Audit a module that is part of an overall annual audit of the entity’s information systems.

Audits of RAs (Class 1-2)

It is recommended that Enterprise customers approving Class 1 and 2 certificates undergo an annual compliance audit. Upon request from DigiCert and/or a Superior Entity (if the Superior Entity is not DigiCert), Enterprise customers shall 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)

It is recommended that Enterprise Customers authorizing the issuance of Class 3 SSL certificates undergo an annual compliance audit of their obligations under the STN.[23] Upon request from DigiCert and/or a Superior Entity (if the Superior Entity is not DigiCert) Enterprise Customers shall undergo an audit noting any exceptions or irregularities to STN policies and the steps taken to remedy the irregularities.

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

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

DigiCert and each Affiliate shall be 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 shall be a WebTrust for Certification Authorities 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

After receiving a Compliance Audit report, the audited entity's Superior Entity shall contact the audited party to discuss any exceptions or deficiencies shown by the Compliance Audit. DigiCert shall also be entitled to discuss such exceptions or deficiencies with the audited party. The audited entity and the Superior Entity shall, in good faith, use commercially reasonable efforts to agree on a corrective action plan for correcting the problems causing the exceptions or deficiencies and to implement the plan.

In the event of the audited entity's failure to develop such a corrective action plan or implement it, or if the report reveals exceptions or deficiencies that DigiCert and the audited entity's Superior Entity reasonably believe pose an immediate threat to the security or integrity of the STN, then:

(a) DigiCert and/or the Superior Entity shall determine whether revocation and compromise reporting are necessary,
(b) DigiCert and the Superior Entity shall be entitled to suspend services to the audited entity, and
(c) If necessary, DigiCert and the Superior Entity may terminate such services subject to this CP and the terms of the audited entity's contract with its Superior Entity

8.6 Communications of Results

Following any Compliance Audit, the audited entity shall provide DigiCert and its Superior Entity (if the Superior Entity is not DigiCert) with the annual report and attestations based on its audit or self-audit within fourteen (14) days after the completion of the audit and no later than forty-five (45) days after the anniversary date of commencement of operations.

CAs shall make its annual Audit Report publicly available no later than three (3) months after the end of the audit period. In the event of a delay greater than three months, the CA shall provide an explanatory letter signed by the Qualified Auditor.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

DigiCert, Affiliates, and RA Customers are entitled to charge end-user Subscribers for the issuance, management, and renewal of Certificates.

9.1.2 Certificate Access Fees

DigiCert, Affiliates, and RA Customers shall not charge a fee as a condition of making a Certificate available in a repository or otherwise making Certificates available to Relying Parties.

9.1.3 Revocation or Status Information Access Fees

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

9.1.4 Fees for Other Services

DigiCert and Affiliates do not charge a fee for access to this CP or their respective 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

To the extent permitted by applicable law, DigiCert, Affiliates, and Resellers shall implement a refund policy. They shall place their refund policies within their web sites (including a listing in their repositories), in their Subscriber Agreements, and, in the case of DigiCert and Affiliates, in their CPSs.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

DigiCert, Affiliates and Enterprise Customers (when required) shall 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. This insurance requirement does not apply to governmental entities.

9.2.2 Other Assets

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

9.2.3 Extended Warranty Coverage

Some STN participants offer extended warranty programs that provides SSL and code signing certificate subscribers with protection against loss or damage that is due to a defect in the participant's issuance of the certificate or other malfeasance caused by participant's negligence or breach of its contractual obligations, provided that the subscriber of the certificate has fulfilled its obligations under the applicable service agreement. STN participants offering extended warranty programs are required to include program information in their CPS.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The following records of Subscribers shall, subject to Section 9.3.2, be kept confidential and private ("Confidential/Private Information"):

- CA application records, whether approved or disapproved,
- Certificate Application records,
- Private keys held by enterprise RA Customers using Managed PKI Key Manager and information needed to recover such Private Keys,
- Transactional records (both full records and the audit trail of transactions),
- STN audit trail records created or retained by DigiCert, an Affiliate, or a Customer,
- STN audit reports created by DigiCert, an Affiliate, or a Customer (to the extent such reports are maintained), or their respective auditors (whether internal or public),
- Contingency planning and disaster recovery plans, and
- Security measures controlling the operations of DigiCert or Affiliate hardware and software and the administration of Certificate services and designated enrollment services.

9.3.2 Information Not Within the Scope of Confidential Information

STN Participants acknowledge that Certificates, Certificate revocation and other status information, repositories of STN Participants, and information contained within them are not considered Confidential/Private Information. Information not expressly deemed Confidential/Private Information under Section 9.3.1 shall be considered neither confidential nor private. This section is subject to applicable privacy laws.

9.3.3 Responsibility to Protect Confidential Information

STN participants receiving private information shall secure it from compromise and disclosure to third parties.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

DigiCert and Affiliates shall implement a privacy policy in accordance with requirements of the DCPA. Such privacy policies shall conform to applicable local privacy laws. DigiCert and Affiliates shall not disclose or sell the names of Certificate Applicants or other identifying information about them, subject to Section 9.3.2 and to the right of a terminating CA to transfer such information to a successor CA under Section 5.8.

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

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

9.4.5 Notice and Consent to Use Private Information

Unless where otherwise stated in this CP, 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

STN Participants acknowledge that DigiCert and the Affiliate shall be entitled to disclose Confidential/Private Information if, in good faith, DigiCert or the Affiliate 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

Privacy policies shall contain provisions relating to the disclosure of Confidential/Private Information to the person disclosing it to DigiCert or the Affiliate. This section is subject to applicable privacy laws.

9.5 Intellectual Property Rights

The allocation of Intellectual Property Rights among STN Participants other than Subscribers and Relying Parties shall be governed by the applicable agreements between such STN 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, Affiliates, and Customers shall 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, Affiliates, and Customers shall grant permission to use revocation information to perform Relying Party functions subject to the applicable CRL Usage Agreement, Relying Party Agreement, or any other applicable agreements.

9.5.2 Property Rights in the CP

STN Participants acknowledge that DigiCert retains all Intellectual Property Rights in and to this CP.

9.5.3 Property Rights in Names

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

9.5.4 Property Rights in Keys and Key Material

Key pairs corresponding to Certificates of CAs and end-user Subscribers are the property of the CAs and end-user Subscribers that are the respective Subjects of these Certificates, subject to the rights of enterprise Customers using Managed PKI Key Manager, regardless of the physical medium within which they are stored and protected, and such persons retain all Intellectual Property Rights in and to these key pairs. Without limiting the generality of the foregoing, DigiCert's root public keys and the root Certificates containing them, including all PCA public keys and self-signed Certificates, are the property of DigiCert. DigiCert licenses software and hardware manufacturers to reproduce such root Certificates to place copies in trustworthy hardware devices or software. Finally, Secret Shares of a CA's private key are the property of the CA, and the CA retains all Intellectual Property Right in and to such Secret Shares even though they cannot obtain physical possession of the those shares or the CA from DigiCert.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

STN CAs 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 information in the Certificate that were introduced by the entities approving the Certificate Application or issuing the Certificate as a result of a failure to exercise reasonable care in managing the Certificate Application or creating the Certificate,
- Their Certificates meet all material requirements of this CP and the applicable CPS, and
- Revocation services and use of a repository conform to all material requirements of this CP and the applicable CPS in all material aspects.

Subscriber Agreements may include additional representations and warranties.

9.6.1.1 CABF Warranties and Obligations

For the issuance of EV SSL Certificates, EV Code Signing, and Domain-Validated and Organization-Validated SSL Certificates, CA warranties and obligations shall be documented in a STN participant's CPS and shall comply with the applicable governing CA/Browser Forum Guidelines published at *www.cabforum.org* .

9.6.2 RA Representations and Warranties

STN 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 information in the Certificate that were introduced by the entities approving the Certificate Application as a result of a failure to exercise reasonable care in managing the Certificate Application,
- Their Certificates meet all material requirements of this CP and the applicable CPS, and
- Revocation services (when applicable) and use of a repository conform to all material requirements of this CP and 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,
- 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 all material requirements of this CP and the applicable 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 Party Agreements require Relying Parties to acknowledge that they have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a Certificate, that they are solely responsible for deciding whether or not to rely on such information, and that they shall bear the legal consequences of their failure to perform the Relying Party obligations in terms of this CP.

Relying Party Agreements may include additional representations and warranties.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

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

9.8 Limitations of Liability

To the extent DigiCert has issued and managed the Certificate(s) at issue in compliance with its Certificate Policy and its Certification Practice Statement, DigiCert shall have no liability to the Subscriber, any Relying Party, or any other third parties for any damages or losses suffered as a result of the use or reliance on such Certificate(s). To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall limit DigiCert's and the applicable Affiliates' liability outside the context of the Extended Warranty Protection Program. Limitations of liability shall include an exclusion of indirect, special, incidental, and consequential damages. They shall also include the following liability caps limiting DigiCert's and the Affiliate's damages concerning a specific Certificate:

Class	Liability Caps
Class 1	One Hundred U.S. Dollars ($ 100.00 US)
Class 2	Five Thousand U.S. Dollars ($ 5,000.00 US)
Class 3	One Hundred Thousand U.S. Dollars ($ 100,000.00 US)

Table 9 – Liability Caps

The liability caps in Table 5 limit damages recoverable outside the context of the Extended Warranty Protection Program. Amounts paid under the Extended Warranty Protection Program are subject to their own liability caps. The liability caps under the Extended Warranty Protection Program for different kinds of Certificates range from $10,000 US to $1,750,000 US. *See* the Extended Warranty Protection Program for more detail at https://www.digicert.com/legal-repository/ (for an interim period, available at https://www.websecurity.symantec.com/legal/repository#PoliciesAndAgreements).

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

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

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

9.9 Indemnities

9.9.1 Indemnification by Subscribers

To the extent permitted by applicable law, Subscribers are required to indemnify CAs or RAs (both STN and non-STN) for:

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

The applicable Subscriber Agreement may include additional indemnity obligations

9.9.2 Indemnification by Relying Parties

To the extent permitted by applicable law, Relying Party Agreements shall require Relying Parties to indemnify CAs or RAs (both STN and non-STN) 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 such Application Software Supplier's software displaying as not trustworthy a Certificate that is still valid, or displaying as trustworthy: (1) a Certificate that has expired, or (2) a Certificate that has been revoked (but only in cases where the revocation status is currently available from the CA online, and the application software either failed to check such status or ignored an indication of revoked status).

9.10 Term and Termination

9.10.1 Term

The CP becomes effective upon publication in the DigiCert Repository. Amendments to this CP become effective upon publication in the DigiCert Repository.

9.10.2 Termination

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

9.10.3 Effect of Termination and Survival

Upon termination of this CP, STN participants are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

9.11 Individual Notices and Communications with Participants

Unless otherwise specified by agreement between the parties, STN 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 CP 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 CP 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/* (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 CP. The DCPA shall determine whether changes to the CP 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 CP 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 shall send Affiliates notice of material amendments to the CP proposed by the DCPA. The notice shall state the text of the proposed amendments and the comment period. Proposed amendments to the CP shall also appear in the Practices Updates and Notices section of the DigiCert Repository, which is located at: https://www.digicert.com/legal-repository/ (for an interim period, available at https://www.websecurity.symantec.com/legal/repository#PoliciesAndAgreements. Affiliates shall publish or provide a link to the proposed amendments on their own web-based repositories within a reasonable time after receiving notice of such amendments.

The DCPA solicits proposed amendments to the CP from other STN Participants. If the DCPA considers such an amendment desirable and proposes to implement the amendment, the DCPA shall provide notice of such amendment in accordance with this section.

Notwithstanding anything in the CP to the contrary, if the DCPA believes that material amendments to the CP are necessary immediately to stop or prevent a breach of the security of the STN or any portion of it, DigiCert and the DCPA shall be entitled to make such amendments by publication in the DigiCert Repository. Such amendments will be effective immediately upon publication. Within a reasonable time after publication, DigiCert shall provide notice to Affiliates of such amendments.

9.12.2.1 Comment Period

Except as otherwise stated, the comment period for any material amendments to the CP shall be fifteen (15) days, starting on the date on which the amendments are posted on the DigiCert Repository. Any STN Participant shall be entitled to file comments with the DCPA up until the end of the comment period.

9.12.2.2 Mechanism to Handle Comments

The DCPA shall consider any comments on the proposed amendments. The DCPA shall either (a) allow the proposed amendments to become effective without amendment, (b) amend the proposed amendments and republish them as a new amendment when required, or (c) withdraw the proposed amendments. The DCPA is entitled to withdraw proposed amendments by notifying Affiliates and providing notice in the Practices Updates and Notices section of the DigiCert 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 one or more of any of DigiCert, Affiliates, and/or Customers 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. The procedures in the Affiliate Practices Legal Requirements Guidebook to resolve 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 CP, 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 CP. Agreements incorporating the CP 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 CP separate and apart from the remaining provisions of any such agreements, subject to any limitations appearing in applicable law.

This CP 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 CP 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. CAs shall be licensed in each jurisdiction where 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 CP is held to be unenforceable by a court of law or other tribunal having authority, the remainder of the CP 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 and the applicable Affiliate.

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	*(US Government) 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*
KRB	*Key Recovery Block.*
LSVA	*Logical security vulnerability assessment.*
NIST	*(US Government) National Institute of Standards and Technology*
OCSP	*Online Certificate Status Protocol.*
OID	*Object Identifier*
PCA	*Primary Certification Authority.*
PIN	*Personal identification number.*
PKCS	*Public-Key Cryptography Standard.*
PKI	*Public Key Infrastructure.*
RA	*Registration Authority.*
RFC	*Request for comment.*
SAR	*Security Audit Requirements*
S/MIME	*Secure multipurpose Internet mail extensions.*
SOC	*Service Organization Control standard (promulgated by the American Institute of Certified Public Accountants).*
SSL	*Secure Sockets Layer.*
STN	*Symantec Trust Network.*
TLD	*Top-Level Domain*
TLS	*Transport Layer Security*

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.*
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 to be a STN 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.
Affiliated Individual	A natural person that is related to a Managed PKI Customer, Managed PKI Lite Customer, or Gateway Customer entity (i) as an officer, director, employee, partner, contractor, intern, or other person within the entity, (ii) as a member of a DigiCert registered community of interest, or (iii) as a person maintaining a relationship with the entity where the entity has business or other records providing appropriate assurances of the identity of such person.
Applicant	The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual certificate request.
Applicant Representative	A natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: (i) who signs and submits, or approves a certificate request on behalf of the Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or (iii) who acknowledges and agrees to the Certificate Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA.
Application Software Supplier	A supplier of Internet browser software or other relying-party application software that displays or uses Certificates and incorporates Root Certificates.
Attestation Letter	A letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information.
Audit Report	A report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the mandatory provisions of these Requirements.
Automated Administration	A procedure whereby Certificate Applications are approved automatically if enrollment information matches information contained in a database.
Automated Administration Software Module	Software provided by DigiCert that performs Automated Administration.
Certificate	A message that, at least, states a name or identifies the CA, identifies the Subscriber, contains the Subscriber's public key, identifies the Certificate's Operational Period, contains a Certificate serial number, and is digitally signed by the CA.
Certificate Applicant	An individual or organization that requests the issuance of a Certificate by a CA.
Certificate Application	A request from a Certificate Applicant (or authorized agent of the Certificate Applicant) to a CA for the issuance of a Certificate.
Certificate 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)	This document, which is entitled "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 Revocation List (CRL)	A periodically (or exigently) issued list, digitally signed by a CA, of identified Certificates that have been revoked prior to their expiration dates in accordance with CP § 3.4. The list generally indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the revoked Certificates' serial numbers, and the specific times and reasons for revocation.
Certificate Signing Request	A message conveying a request to have a Certificate issued.
Certification Authority (CA)	An entity authorized to issue, manage, revoke, and renew Certificates in the STN.

Term	Definition
Certification Practice Statement (CPS)	A statement of the practices that DigiCert or an Affiliate employs in approving or rejecting Certificate Applications and issuing, managing, and revoking Certificates, and requires its Managed PKI Customers and Gateway Customers to employ.
Challenge Phrase	A secret phrase chosen by a Certificate Applicant during enrollment for a Certificate. When issued a Certificate, the Certificate Applicant becomes a Subscriber and a CA or RA can use the Challenge Phrase to authenticate the Subscriber when the Subscriber seeks to revoke or renew the Subscriber's Certificate.
Class	A specified level of assurances as defined within the CP. See CP § 1.1.1.
Client Service Center	A Service Center that is an Affiliate providing client Certificates either in the Consumer or Enterprise line of business.
Compliance Audit	A periodic audit that a Processing Center, Service Center, Managed PKI Customer, or Gateway Customer undergoes to determine its conformance with STN Standards that apply to it.
Compromise	A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred. With respect to private keys, a Compromise is a loss, theft, disclosure, modification, unauthorized use, or other compromise of the security of such private key.
Confidential/Private Information	Information required to be kept confidential and private pursuant to CP § 2.8.1.
CRL Usage Agreement	An agreement setting forth the terms and conditions under which a CRL or the information in it can be used.
Cross Certificate	A certificate that is used to establish a trust relationship between two Root CAs.
Cryptographically Secure Pseudo-Random Number Generator	A random number generator intended for use in a cryptographic system.
Customer	An organization that is either a Managed PKI Customer or Gateway Customer.
Delegated Third Party	A natural person or Legal Entity that is not the CA but is authorized by the CA to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.
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 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, as in Enterprise Service Center	A line of business that an Affiliate enters to provide Managed PKI services to Managed PKI Customers.
Enterprise RA	An employee or agent of an organization unaffiliated with the CA who authorizes issuance of Certificates to that organization.
Entry 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
Exigent Audit/Investigation	An audit or investigation by DigiCert where DigiCert has reason to believe that an entity's failure to meet STN Standards, an incident or Compromise relating to the entity, or an actual or potential threat to the security of the STN posed by the entity has occurred.
Extended Validation	Validation Procedures defined by the Guidelines for Extended Validation Certificates published by a forum consisting of major certification authorities and browser vendors.
Fully-Qualified Domain Name	A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.
Government Entity	A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).
Intellectual Property Rights	Rights under one or more of the following: any copyright, patent, trade secret, trademark, and any other intellectual property rights.

Term	Definition
Intermediate Certification Authority (Intermediate CA)	A Certification Authority whose Certificate is located within a Certificate Chain between the Certificate of the root CA and the Certificate of the Certification Authority that issued the end-user Subscriber's Certificate.
Internal Name	A string of characters (not an IP address) in a Common Name or Subject Alternative Name field of a Certificate that cannot be verified as globally unique within the public DNS at the time of certificate issuance because it does not end with a Top Level Domain registered in IANA's Root Zone Database.
Issuing CA	In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.
Key Compromise	A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, an unauthorized person has had access to it, or there exists a practical technique by which an unauthorized person may discover its value.
Key Generation Ceremony	A procedure whereby a CA's or RA's key pair is generated, its private key is transferred into a cryptographic module, its private key is backed up, and/or its public key is certified.
Key Generation Script	A documented plan of procedures for the generation of a CA Key Pair.
Key Manager Administrator	An Administrator that performs key generation and recovery functions for a Managed PKI Customer using Managed PKI Key Manager.
Key Pair	The Private Key and its associated Public Key.
Key Recovery Block (KRB)	A data structure containing a Subscriber's private key that is encrypted using an encryption key. KRBs are generated using Managed PKI Key Manager software.
Key Recovery Service	A DigiCert service that provides encryption keys needed to recover a Key Recovery Block as part of a Managed PKI Customer's use of Managed PKI Key Manager to recover a Subscriber's private key.
Legal Entity	An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.
Managed PKI	DigiCert's fully integrated managed PKI service that allows enterprise Customers of DigiCert and its Affiliates to distribute Certificates to individuals, such as employees, partners, suppliers, and customers, as well as devices, such as servers, routers, and firewalls. Managed PKI permits enterprises to secure messaging, intranet[24], extranet, virtual private network, and e-commerce applications.
Managed PKI Administrator	An Administrator that performs validation or other RA functions for a Managed PKI Customer.
Managed PKI Control Center	A web-based interface that permits Managed PKI Administrators to perform Manual Authentication of Certificate Applications
Managed PKI Key Manager	A key recovery solution for those Managed PKI Customers choosing to implement key recovery under a special Managed PKI Agreement.
Managed PKI Key Management Service Administrator's Guide	A document setting forth the operational requirements and practices for Managed PKI Customers using Managed PKI Key Manager.
Manual Authentication	A procedure whereby Certificate Applications are reviewed and approved manually one-by-one by an Administrator using a web-based interface.
NetSure Protection Plan	An extended warranty program, which is described in CP §9.2.3.
Non-verified Subscriber Information	Information submitted by a Certificate Applicant to a CA or RA, and included within a Certificate, that has not been confirmed by the CA or RA and for which the applicable CA and RA provide no assurances other than that the information was submitted by the Certificate Applicant.
Non-repudiation	An attribute of a communication that provides protection against a party to a communication falsely denying its origin, denying that it was submitted, or denying its delivery. Denial of origin includes the denial that a communication originated from the same source as a sequence of one or more prior messages, even if the identity associated with the sender is unknown. Note: only an adjudication by a court, arbitration panel, or other tribunal can ultimately prevent repudiation. For example, a digital signature verified with reference to a STN Certificate may provide proof in support of a determination of Non-repudiation by a tribunal, but does not by itself constitute Non-repudiation.
Object Identifier	A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.
OCSP (Online Certificate Status Protocol)	An online Certificate-checking protocol for providing Relying Parties with real-time Certificate status information.
OCSP Responder	An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.

[24] The use of SSL/Code Signing Certificates with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Name has been deprecated by the CA / Browser Forum and will be eliminated by October 2016. Any such certificate still being issued after the effective date must have an expiry date of 1 November 2015 or earlier. Previously issued certificates with expiry dates after 1 October 2016 will be revoked effective 1 October 2016.

Term	Definition
Offline CA	STN PCAs, Issuing Root CAs and other designated intermediate CAs that are maintained offline for security reasons in order to protect them from possible attacks by intruders by way of the network. These CAs do not directly sign end user Subscriber Certificates.
Online CA	CAs that sign end user Subscriber Certificates are maintained online so as to provide continuous signing services.
Operational Period	The period starting with the date and time a Certificate is issued (or on a later date and time certain if stated in the Certificate) and ending with the date and time on which the Certificate expires or is earlier revoked.
PKCS #10	Public-Key Cryptography Standard #10, developed by RSA Security Inc., which defines a structure for a Certificate Signing Request.
PKCS #12	Public-Key Cryptography Standard #12, developed by RSA Security Inc., which defines a secure means for the transfer of private keys.
Primary Certification Authority (PCA)	A CA that acts as a root CA for a specific Class of Certificates, and issues Certificates to CAs subordinate to it.
Private Key	The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.
Processing Center	An organization (DigiCert or certain Affiliates) that creates a secure facility housing, among other things, the cryptographic modules used for the issuance of Certificates. In the Consumer and Web Site lines of business, Processing Centers act as CAs within the STN and perform all Certificate lifecycle services of issuing, managing, revoking, and renewing Certificates. In the Enterprise line of business, Processing Centers provide lifecycle services on behalf of their Managed PKI Customers or the Managed PKI Customers of the Service Centers subordinate to them.
Public Key	The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.
Public Key Infrastructure (PKI)	The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based public key cryptographic system. The STN PKI consists of systems that collaborate to provide and implement the STN.
Publicly-Trusted Certificate	A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software.
Qualified Auditor	A natural person or Legal Entity that meets the requirements of Section 17.6 (Auditor Qualifications).
Registered Domain Name	A Domain Name that has been registered with a Domain Name Registrar.
Registration Authority (RA)	A Legal Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the certificate application process or revocation process or both. When “RA” is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.
Reliable Method of Communication	A method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative.
Relying Party	An individual or organization that acts in reliance on a certificate and/or a digital signature.
Relying Party Agreement	An agreement used by a CA setting forth the terms and conditions under which an individual or organization acts as a Relying Party.
Repository	An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.
Reseller	An entity marketing services on behalf of DigiCert or an Affiliate to specific markets.
Reserved IP Address	An IPv4 or IPv6 address that the IANA has marked as reserved: http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml
Retail Certificate	A Certificate issued by DigiCert or an Affiliate, acting as CA, to individuals or organizations applying one by one to DigiCert or an Affiliate on its web site.
Root CA	The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.
Root Certificate	The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.
RSA	A public key cryptographic system invented by Rivest, Shamir, and Adelman.
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.

Term	Definition
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.
Security and Audit Requirements Guide	A DigiCert document that sets forth the security and audit requirements and practices for Processing Centers and Service Centers.
Security and Practices Review	A review of an Affiliate performed by DigiCert before an Affiliate is permitted to become operational.
Service Center	An Affiliate that does not house Certificate signing units for the issuance of Certificates for the purpose of issuing Certificates of a specific Class or type, but rather relies on a Processing Center to perform issuance, management, revocation, and renewal of such Certificates.
Sub-domain	The portion of the STN under control of an entity and all entities subordinate to it within the STN hierarchy.
Subject	The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject and holder of a private key corresponding to a public key. The Subject is either the Subscriber or a device under the control and operation of the Subscriber. The term "Subject" can, in the case of an organizational Certificate, refer to the equipment or device that holds a private key. A Subject is assigned an unambiguous name, which is bound to the public key contained in the Subject's Certificate.
Subject Identity Information	Information that identifies the Certificate Subject. Subject Identity Information does not include a domain name listed in the *subjectAltName* extension or the Subject *commonName* field.
Subordinate CA	A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.
Subscriber	In the case of an individual Certificate, a person who is the Subject of, and has been issued, a Certificate. In the case of an organizational Certificate, an organization that owns the equipment or device that is the Subject of, and that has been issued, a Certificate. A Subscriber is capable of using, and is authorized to use, the private key that corresponds to the public key listed in the Certificate.
Subscriber Agreement	An agreement used by a CA or RA setting forth the terms and conditions under which an individual or organization acts as a Subscriber.
Superior Entity	An entity above a certain entity within a STN hierarchy (the Class 1, 2, or 3 hierarchy).
Supplemental Risk Management Review	A review of an entity by DigiCert following incomplete or exceptional findings in a Compliance Audit of the entity or as part of the overall risk management process in the ordinary course of business.
Terms of Use	Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with these Requirements when the Applicant/Subscriber is an Affiliate of the CA.
Trusted Person	An employee, contractor, or consultant of an entity within the STN responsible for managing infrastructural trustworthiness of the entity, its products, its services, its facilities, and/or its practices as further defined in CP § 5.2.1.
Trusted Position	The positions within a STN entity that must be held by a Trusted Person.
Trustworthy System	Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy. A trustworthy system is not necessarily a "trusted system" as recognized in classified government nomenclature.
Symantec Trust Network (STN)	The Certificate-based Public Key Infrastructure governed by the DigiCert Certificate Policies for Symantec Trust Network, which enables the worldwide deployment and use of Certificates by DigiCert and its Affiliates, and their respective Customers, Subscribers, and Relying Parties.
STN Participant	An individual or organization that is one or more of the following within the STN: DigiCert, an Affiliate, a Customer, a Universal Service Center, a Reseller, a Subscriber, or a Relying Party.
STN Standards	The business, legal, and technical requirements for issuing, managing, revoking, renewing, and using Certificates within the STN.
Unregistered Domain Name	A Domain Name that is not a Registered Domain Name.
Valid Certificate	A Certificate that passes the validation procedure specified in RFC 5280.
Validation Specialists	Someone who performs the information verification duties specified by these Requirements.
Validity Period	The period of time measured from the date when the Certificate is issued until the Expiry Date.
Wildcard Certificate	A Certificate containing an asterisk (*) in the left-most position of any of the Subject Fully-Qualified Domain Names contained in the Certificate.