DigiCert Public Trust Certificate Policy for Third Party TLS-Issuing CAs

Version: 1.1
Effective Date: 9 June 2026
Document Owner: DigiCert, Inc

Table of Contents

1 Introduction

1.1 Overview

This Certificate Policy (CP) defines the policies followed by third party CAs chaining to one of DigiCert's publicly trusted TLS root certificates. This CP governs certificates issued under the following policies, guidelines and standards:

• The CA/B Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("TLS BRs") - https://cabforum.org/baseline-requirements-documents

• The CA/B Forum Guidelines for Extended Validation Certificates ("EVGs") - https://cabforum.org/extended-validation

• The CA/B Forum Network and Certificate System Security Requirements - https://cabforum.org/network-security-requirements

• Microsoft Trusted Root Store (Program Requirements) - https://docs.microsoft.com/en-us/security/trusted-root/program-requirements

• Mozilla Root Store Policy - https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy

• Apple Root Store Program - https://www.apple.com/certificateauthority/ca_program.html

• 360 Browser CA Policy - https://caprogram.360.cn/#strategy

• Chromium Project Root Store Certificate Policy - https://www.chromium.org/Home/chromiumsecurity/root-ca-policy

• CCADB Policy - https://www.ccadb.org/policy

If any inconsistency exists between this document and the normative provisions of an applicable industry guideline or standard ("Applicable Requirements"), then the Applicable Requirements take precedence over this CP.

1.2 Document Name and Identification

The name of this document is the DigiCert Public Trust Certificate Policy for Third Party TLS-Issuing CAs. The document follows the framework outlined in RFC3647.

1.2.1 Revision

Date	Description	Version
June 10, 2025	Initial Draft	V 1.0

Date	Description	Version
June 9, 2026	Added requirement to adhere to CCADB, updated section headings to better align with TLS Baseline Requirements for readability, added DigiCert Ombudsman contact information, added Mass Revocation Policy Requirements.	V 1.1

1.3 PKI Participants

1.3.1 Certification Authorities

DigiCert cross-signs third party CAs and issues subordinate CAs to third parties provided that third party is also an Application Software Vendor. These entities issue TLS certificates in accordance with this policy, their own CPS, and the CA/Browser Forum's TLS Baseline Requirements.

1.3.2 Registration Authorities

A Registration Authority is an entity that performs identification and authentication of certificate Applicants, initiates or passes along revocation requests for certificates for end-user certificates, and approves applications for renewal or re-keying certificates on behalf of an Issuer CA. Under this policy, the third-party CA is the RA for certificates they issue.

Third-party CAs may only delegate validation responsibilities back to DigiCert and not to an unaffiliated entity. RA personnel involved in the issuance of publicly-trusted certificates must possess the skills and undergo the training required under Section 5.3.

1.3.3 Subscribers

Subscribers may be natural persons or legal entities. A Subscriber is not required to be the Subject of certificates under its control.

1.3.4 Relying Parties

Relying Parties are natural persons, legal entities or organizations that rely on certificates and related services. Relying parties must check the appropriate CRL or OCSP response prior to relying on information featured in a Certificate.

1.3.5 Other Participants

No stipulation

1.4 Certificate Usage

As specified in the applicable CPS.

1.4.1 Appropriate Certificate Uses

As specified in the third-party CA's CPS.

1.4.2 Prohibited Certificate Uses

Certificates do not guarantee that the subject is trustworthy, honest, reputable in its business dealings, safe to do business with, or compliant with any laws. A Certificate only establishes that the information in the certificate was verified in accordance with the Applicable Requirements when the certificate issued.

Subscribers and relying parties must use certificates in accordance with any applicable laws, including any relevant export or import laws.

CA certificates subject to the Mozilla Root Store Policy shall not be used for any functions except CA functions. In addition, end-user subscriber certificates shall not be used as CA certificates.

Participants in the DigiCert Public PKI periodically change CA hierarchies to use different 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 changed. 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.

Pinning is strictly prohibited and is not a reason to delay revocation. Third-party CAs must also avoid mixing certificates trusted for the web with non- web PKI. Subscribers are expected to comply with all requirements of all applicable browser root policies, including revocation periods of 24 hours and 5 days as specified herein.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The DigiCert Policy Authority (DCPA) maintains and enforces this CP.

1.5.2 Contact Person

DigiCert Policy Authority
2801 N. Thanksgiving Way, Suite 500
Lehi, UT 84048 USA
policy@digicert.com

1.5.2.1 Revocation Reporting Contact Person

DigiCert Technical Support
2801 N. Thanksgiving Way, Suite 500
Lehi, UT 84048 USA
revoke@digicert.com

Revocations can also be submitted through our Compromised Key Reporting and Revocation Service: https://problemreport.digicert.com/

1.5.2.2 DigiCert Ombudsman

The Ombudsman addresses DigiCert's conduct within the Bugzilla community relating to fairness and transparency matters. The Ombudsman can be contacted via email: transparency@digicert.com

1.5.3 Person Determining CPS Suitability for the Policy

The DCPA determines the suitability and applicability of this document.

1.5.4 CP Approval Procedures

This CP is reviewed at least annually. Amendments are made by posting an updated version to the online repository. Updates supersede any designated or conflicting provisions of the referenced version. Controls are in place to reasonably ensure that it is not amended and published without the prior authorization of the DCPA.

1.6 Definitions and Acronyms

1.6.1 Definitions

Definition	Description
Applicant	An entity applying for a Certificate.
Application Software Vendor	A software developer whose software displays or uses DigiCert Certificates and distributes DigiCert's root Certificates.
CAB Forum	Defined in Section 1.1
Certificate	An electronic document, digitally signed by a Certificate Authority, that binds a Public Key to an identity.
Certificate Management Process	The policies, practices, and procedures governing the use of the Certificate Management System
Certificate Management System	The keys, software and hardware used to verify Certificate Data, maintain a Repository, and issue and revoke Certificates.
Domain Name	An ordered list of one or more Domain Labels assigned to a node in the Domain Name System.
Hardware Crypto Module	A tamper-resistant device, with a cryptography processor, used for the specific purpose of protecting the lifecycle of cryptographic keys, including generating, managing, processing, and storing cryptographic keys.
Issuer CA	Any CA issuing Certificates under this CP
Key Compromise	A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, or an unauthorized person has had access to it.
Key Pair	A Private Key and associated Public Key.
Linting	A process in which the content of digitally signed data such as a Precertificate [RFC 6962], Certificate, Certificate Revocation List, or OCSP response, or data-to-be-signed object such as a tbsCertificate, as described in RFC 5280, Section 4.1.1.1, is checked for conformance with the profiles and requirements defined in these Requirements.
OCSP Responder	An online software application for processing certificate status requests.

Definition	Description
Private Key	The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create digital signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.
Public Key	The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify digital signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.
Relying Party	An entity that relies upon either the information contained within a Certificate or a time-stamp token.
Relying Party Agreement	An agreement which must be read and accepted by the Relying Party prior to validating, relying on or using a Certificate.
Subscriber	The entity who is issued a certificate.
Subscriber Agreement	An agreement that governs the issuance and use of a Certificate that the Applicant must read and accept before receiving a Certificate.
WebTrust	The current version of CPA Canada's WebTrust Program for Certification Authorities.

1.6.2 Acronyms

Acronym	Description
CA	Certificate Authority or Certification Authority
CAB or CA/B	"CA/Browser" as in "CAB Forum"
CP	Certificate Policy
CRL	Certificate Revocation List
DCPA	DigiCert Policy Authority
DNS	Domain Name Service
ETSI	European Telecommunications Standards Institute EU
EV	Extended Validation
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers

Acronym	Description
IETF	Internet Engineering Task Force
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request for Comments (at IETF.org)
SAN	Subject Alternative Name
SHA	Secure Hashing Algorithm
SSL	Secure Sockets Layer
TLD	Top-Level Domain
TLS	Transport Layer Security
UTC	Coordinated Universal Time
X.509	The ITU-T standard for Certificates and their corresponding authentication framework

1.6.3 References

1. WebTrust Program for Certification Authorities;
2. WebTrust Principles and Criteria for Certification Authorities – SSL Baseline
3. WebTrust Principles and Criteria for Certification Authorities – Network Security
4. WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security
5. WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL;

1.6.4. Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this CP shall be interpreted in accordance with RFC 2119.

2 Publication and Repository Responsibilities

2.1 Repositories

Issuer CAs must publish in an online, publicly-accessible, and regularly-available repository:

1. All publicly trusted CA Certificates and Cross-Certificates, issued to and from the Issuer CA,
2. Revocation data for issued digital certificates,
3. CP and/or CPS documents.

2.2 Publication of Certification Information

The DigiCert certificate services, business practices, and the repository are accessible through several means of communication:

1. On the web: https://www.digicert.com (and via URIs included in the certificates themselves)
2. By email to admin@digicert.com
3. By mail addressed to:
   DigiCert, Inc.
   2801 N. Thanksgiving Way, Suite 500
   Lehi, UT 84048
4. By telephone: +1-801-877-2100

CRLs and OCSP responses are published in accordance with Section 4.9.7 and Section 4.9.10 of the CPS.

2.3 Time or Frequency of Publication

CA Certificates are published in a repository as soon as possible after issuance. Under special circumstances, Issuing CAs may publish new CRLs prior to the scheduled issuance of the next CRL. (See Section 4.9 for additional details.)

The CA must issue CRLs for Subscriber Certificates that are subject to the TLS Baseline Requirements and that have CRL requirements at least once every seven days. CP documents are updated at least every 365 days to describe in detail how Issuer CAs comply with the Applicable Requirements.

2.4 Access Controls on Repositories

Read-only access to the repository is unrestricted and continuous. Logical and physical controls prevent unauthorized write access to repositories.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

As specified in the applicable CPS.

3.1.2 Need for Names to be Meaningful

As specified in the applicable CPS.

3.1.3 Anonymity or Pseudonymity of Subscribers

As specified in the applicable CPS.

3.1.4 Rules for Interpreting Various Name Forms

As specified in the applicable CPS.

3.1.5 Uniqueness of Names

As specified in the applicable CPS.

3.1.6 Recognition, Authentication, and Role of Trademarks

As specified in the applicable CPS.

3.2 Initial Identity Validation

As specified in the applicable CPS.

3.2.1 Method to Prove Possession of Private Key

No stipulation

3.2.2 Authentication of Organization Identity

As specified in the applicable CPS.

3.2.3 Authentication of Individual Identity

As specified in the applicable CPS.

3.2.4 Non-Verified Subscriber Information

The CA verifies the contents of the certificate in accordance with the Applicable Requirements.

3.2.5 Validation of Authority

As specified in the applicable CPS.

3.2.6 Criteria for Interoperation

Interoperation with DigiCert PKI is permitted pursuant to this CP. All cross-certified Subordinate CA certificates should be disclosed in the applicable repository.

3.2.7 Third-Party Validators

As specified in the applicable CPS.

3.2.8 Validation of Domain Control

The CA must verify all domains listed in the certificate using a method specified in the CA/Browser Forum's TLS Baseline Requirements.

3.2.9 Validation of Wildcard Domains

The CA must verify all domains listed in the certificate using a method specified in the CA/Browser Forum's TLS Baseline Requirements.

3.2.10 Data Source Accuracy

Data sources used in validation must be evaluated based on:

- The age of the information provided,
- The frequency of updates to the information source,
- The data provider and purpose of the data collection,
- The public accessibility of the data availability, and
- The relative difficulty in falsifying or altering the data.

3.2.11 Multi-Perspective Issuance Corroboration

As specified in the applicable CPS.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-key

As specified in the applicable CPS.

3.3.2 Identification and Authentication for Re-key After Revocation

As specified in the applicable CPS.

3.4 Identification and Authentication For Revocation Request

No stipulation.

4 Certificate Lifecycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

As specified in the applicable CPS.

4.1.2 Enrollment Process and Responsibilities

As specified in the applicable CPS.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

As specified in the applicable CPS.

4.2.2 Approval or Rejection of Certificate Applications

As specified in the applicable CPS.

4.2.3 Time to Process Certificate Applications

As specified in the applicable CPS.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

RAs verify certificate requests prior to issuance. Issuer CAs and RAs must protect databases under their control from unauthorized modification or use. All parties must perform their obligations under this CP in a secure manner.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

As specified in the applicable CPS.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

As specified in the applicable CPS.

4.4.2 Publication of the Certificate by the CA

As specified in the applicable CPS.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

As specified in the applicable CPS.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

As specified in the applicable CPS.

4.5.2 Relying Party Public Key and Certificate Usage

As specified in the applicable CPS.

4.6 Certificate Renewal

4.6.1 Circumstance for Certificate Renewal

As specified in the applicable CPS.

4.6.2 Who May Request Renewal

As specified in the applicable CPS.

4.6.3 Processing Certificate Renewal Requests

As specified in the applicable CPS.

4.6.4 Notification of New Certificate Issuance to Subscriber

As specified in the applicable CPS.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

As specified in the applicable CPS.

4.6.6 Publication of the Renewal Certificate by the CA

As specified in the applicable CPS.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

As specified in the applicable CPS.

4.7 Certificate Re-Key

Re-keying a certificate reissues the certificate with a new key pair. Typically, the re-keyed certificate has a new serial number but the same subject and validity period.

4.7.1 Circumstance for Certificate Re-Key

As specified in the applicable CPS.

4.7.2 Who May Request Certification of a New Public Key

As specified in the applicable CPS.

4.7.3 Processing Certificate Re-Keying Requests

As specified in the applicable CPS.

4.7.4 Notification of New Certificate Issuance to Subscriber

As specified in the applicable CPS.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

As specified in the applicable CPS.

4.7.6 Publication of the Re-Keyed Certificate by the CA

As specified in the applicable CPS.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

As specified in the applicable CPS.

4.8 Certificate Modification

4.8.1 Circumstances for Certificate Modification

Certificate modification requests are treated as a request for a new certificate. Modified information requires validation.

4.8.2 Who May Request Certificate Modification

As specified in the applicable CPS.

4.8.3 Processing Certificate Modification Requests

As specified in the applicable CPS.

4.8.4 Notification of New Certificate Issuance to Subscriber

As specified in the applicable CPS.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

As specified in the applicable CPS.

4.8.6 Publication of the Modified Certificate by the CA

As specified in the applicable CPS.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

As specified in the applicable CPS.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

Certificate revocation ends the operational period of the certificate prior to the certificate's expiration date. DigiCert may revoke for any reason.

4.9.1 Circumstances for Revocation

4.9.1.1 Circumstances for revocation within 24 hours

Issuer CAs must revoke a certificate within 24 hours and use the corresponding CRL Reason confirming one or more of the following occurred:

1. The subscriber requests in writing that the Issuer CA revoke the certificate but does not specify a reason (CRLReason, "unspecified (0)"). Selecting this option omits the reasonCode extension from the CRL);
2. The subscriber notifies the Issuer CA that the original certificate request was not authorized and does not retroactively grant authorization (CRLReason #9, privilegeWithdrawn);
3. The Issuer CA obtains evidence that the subscriber's Private Key corresponding to the Public Key in the certificate suffered a key compromise (CRLReason #1, keyCompromise);
4. The Issuer CA is made aware of a demonstrated or proven method that can easily compute the subscriber's Private Key based on the Public Key in the certificate including but not limited to those identified in Section 6.1.1.2. (CRLReason #1, keyCompromise); or
5. The Issuer CA obtains evidence that the validation of domain authorization or control for any FQDN or IP address or mailbox control for any email address in the certificate should not be relied upon (CRLReason #4, superseded).

4.9.1.2 Circumstances for revocation within 5 days

The Issuer CA may revoke a certificate within 24 hours and must revoke a certificate within 5 days after receipt and confirming any of the following reasons:

1. The certificate no longer complies with the requirements of Section 6.1.5 and Section 6.1.6 of the applicable Baseline Requirements or any section of the Mozilla Root Store Policy (CRLReason #4, superseded);
2. The Issuer CA obtains evidence that the certificate was misused and/or used outside the intended purpose as indicated by the relevant agreement (CRLReason #9, privilegeWithdrawn);
3. The subscriber or the Cross-Certified CA breached a material obligation under this CP, the applicable CPS, or another relevant agreement that requires revocation (CRLReason #9, privilegeWithdrawn);
4. The Issuer CA confirms any circumstance indicating that use of a FQDN, IP address, or email address in the certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a domain name registrant's right to use the Domain Name, a relevant licensing or services agreement between the domain name registrant and the applicant has terminated, or the domain name registrant has failed to renew the Domain Name) (CRLReason #5 cessationOfOperation);
5. The Issuer CA confirms that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate FQDN (CRLReason #9, privilegeWithdrawn);
6. The Issuer CA confirms a material change in the information contained in the certificate (CRLReason #9, privilegeWithdrawn);
7. The Issuer CA confirms that the certificate was not issued in accordance with the CAB/Forum requirements or relevant browser policy (CRLReason #9, privilegeWithdrawn);
8. The Issuer CA determines or confirms that any of the information appearing in the certificate is inaccurate (CRLReason #9, privilegeWithdrawn);
9. The Issuer CA's right to issue certificates under the CAB/Forum requirements expires or is revoked or terminated, unless the Issuer CA has made arrangements to continue maintaining the CRL/OCSP Repository (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);
10. Revocation is required by this CP or the applicable CPS for a reason that is not otherwise required to be specified by this section (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL); or
11. The Issuer CA confirms a demonstrated or proven method that exposes the subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed (CRLReason #1, keyCompromise).

4.9.1.3 Other Revocation Considerations

As specified in the applicable CPS.

4.9.1.4 Revocation of subordinate CA certificates

DigiCert revokes subordinate CA Certificates within seven (7) days after receiving and confirming one or more of the following occurred:

1. The Subordinate CA requests revocation in writing;
2. The Subordinate CA notifies DigiCert that the original certificate request was not authorized and does not retroactively grant authorization;
3. The Issuer CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the certificate suffered a key compromise or no longer complies with the requirements of Sections

6.1.5 and 6.1.6 of the TLS Baseline Requirements or any section of the Mozilla Root Store Policy;
4. The Issuer CA obtains evidence that the CA Certificate was misused and/or used outside the intended purpose as indicated by the relevant agreement;
5. The Issuer CA confirms that the CA Certificate was not issued in accordance with or that Subordinate CA has not complied with this CP or the applicable CPS;
6. The Issuer CA determines that any of the information appearing in the CA Certificate is inaccurate or misleading;
7. The Issuer CA or the Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the CA Certificate;
8. The Issuer CA's or the Subordinate CA's right to issue certificates under the TLS Baseline Requirements expires or is revoked or terminated, unless DigiCert has made arrangements to continue maintaining the CRL/OCSP Repository;
9. Revocation is required by this CP and/or the applicable CPS; or
10. The technical content or format of the CA Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties.
    DigiCert will revoke a cross-certificate if the cross-certified entity or cross-certificate no longer meets the Applicable Requirements.

4.9.2 Who Can Request Revocation

Any appropriately authorized party, such as a recognized representative of a subscriber or cross- signed partner, may request revocation of a certificate.

Third parties may request certificate revocation for problems related to fraud, non-compliance, misuse, or compromise. Certificate revocation requests must identify the entity requesting revocation and specify the reason for revocation. Generally, an example certificate is required to research any allegations of non-compliance with the Applicable Requirements. DigiCert does not require a revocation request to revoke a certificate and may revoke a certificate for any reason.

4.9.3 Procedure for Revocation Request

As specified in the applicable CPS.

4.9.4 Revocation Request Grace Period

All revocation requests and revocations must be processed in accordance with the CA/Browser Forum's TLS Baseline Requirements.

4.9.5 Time within which CA Must Process the Revocation Request

CAs must investigate all Certificate Problem Reports and provide a preliminary report on its findings within 24 hours. Actual revocation occurs as specified in the applicable CPS but must follow the revocation time frames specified in this CP.

4.9.6 Revocation Checking Requirements for Relying Parties

Prior to relying on a certificate, a Relying Party must confirm the validity of each certificate in the certificate chain using the CRL or OCSP responder listed in the certificate.

4.9.7 CRL Issuance Frequency

As specified in the applicable CPS.

4.9.8 Maximum Latency for CRLs

No stipulation.

4.9.9 On-line Revocation/Status Checking Availability

As specified in the applicable CPS.

4.9.10 On-line Revocation Checking Requirements

As specified in the applicable CPS.

4.9.11 Other Forms of Revocation Advertisements Available

Issuer CAs may use other or additional methods to publicize revoked certificates, provided that:

1. The alternative method is described in its CPS and complies with the Application Software Vendor requirements,
2. The alternative method provides authentication and integrity services commensurate with the assurance validation level of the certificate being verified, and
3. The alternative method meets the issuance and latency requirements for CRLs stated in Sections 4.9.5, 4.9.7, and 4.9.8.

4.9.12 Special Requirements Related to Key Compromise

As specified in the applicable CPS.

4.9.13 Circumstances for Suspension

Suspension is not available for publicly trusted certificates.

4.9.13.1 Who Can Request Suspension

Suspension is not available for publicly trusted certificates.

4.9.13.2 Procedure for Suspension Request

Suspension is not available for publicly trusted certificates.

4.9.13.3 Limits on Suspension Period

Suspension is not available for publicly trusted certificates.

4.10 CERTIFICATE STATUS SERVICES

4.10.1 Operational Characteristics

As specified in the applicable CPS.

4.10.2 Service Availability

All Issuer CAs must maintain a 24/7 ability to respond internally to a high-priority certificate problem report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a certificate that is the subject of such a complaint.

4.10.3 Optional Features

No stipulation.

4.11 END OF SUBSCRIPTION

As specified in the applicable CPS.

4.12 KEY ESCROW AND RECOVERY

4.12.1 Key Escrow and Recovery Policy and Practices

Issuer CAs are not permitted to escrow CA Private Keys.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation

5 Facility, Management, and Operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

As specified in the applicable CPS.

5.1.2 Physical Access

As specified in the applicable CPS.

5.1.3 Power and Air Conditioning

As specified in the applicable CPS.

5.1.4 Water Exposures

As specified in the applicable CPS.

5.1.5 Fire Prevention and Protection

As specified in the applicable CPS.

5.1.6 Media Storage

As specified in the applicable CPS.

5.1.7 Waste Disposal

As specified in the applicable CPS.

5.1.8 Off-site Backup

As specified in the applicable CPS.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

As specified in the applicable CPS.

5.2.2 Number of Persons Required per Task

Issuing CAs must require at least two people acting in a trusted role to take action for the most sensitive tasks, such as activating CA Private Keys, generating a CA Key Pair, or creating a backup of a CA Private Key.

5.2.3 Identification and Authentication for each Role

As specified in the applicable CPS.

5.2.4 Roles Requiring Separation of Duties

As specified in the applicable CPS.

5.3 PERSONNEL CONTROLS

5.3.1 Qualifications, Experience, and Clearance Requirements

The identity and trustworthiness of each person acting in a trusted role must be verified before engaging in CA-specific operations, regardless of whether the person is an employee, agent, or an independent contractor.

5.3.2 Background Check Procedures

The issuing CA must complete background checks and identity verification before appointing an individual to a trusted role. Background check specifics are set forth in the applicable CPS.

5.3.3 Training Requirements

The Issuing CA must provide skills training for trusted roles.

5.3.4 Retraining Frequency and Requirements

Personnel must maintain their skill levels in order to continue acting in trusted roles.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

Issuing CAs must hold employees and agents failing to comply with this CP accountable for their actions.

5.3.7 Independent Contractor Requirements

Independent contractors assigned to perform trusted roles must meet the requirements of Sections 5.3.1, 5.3.2, 5.3.3 and are held to the sanctions stated in Section 5.3.6.

5.3.8 Documentation Supplied to Personnel

As specified in the applicable CPS.

5.4 AUDIT LOGGING PROCEDURES

5.4.1 Types of Events Recorded

The issuing CA must ensure essential event auditing capabilities of the CA and RA applications are enabled and record all events related to the security of the Certificate Systems, Certificate Management Systems, Root CA Systems, and Registration Authority Systems. Specific information about audit logs are specified in the applicable CPS.

5.4.2 Frequency of Processing Log

As specified in the applicable CPS.

5.4.3 Retention Period for Audit Log

As specified in the applicable CPS.

5.4.4 Protection of Audit Log

As specified in the applicable CPS.

5.4.5 Audit Log Backup Procedures

As specified in the applicable CPS.

5.4.6 Audit Collection System (internal vs. external)

As specified in the applicable CPS.

5.4.7 Notification to Event-causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

Each CA's security program must include an annual risk assessment that includes the following:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;
2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and

3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that are in place to counter such threats.

5.5 RECORDS ARCHIVAL

Archived records must include sufficient detail to show that a certificate was issued in accordance with the relevant CP.

5.5.1 Types of Records Archived

In addition to the logs described in Section 5.4.1, the following records must be archived:

1. Documentation related to the security of their Certificate Systems, Certificate Management Systems, Root CA Systems, and Delegated Third Party Systems; and
2. Documentation related to their verification, issuance, and revocation of certificate requests and certificates.

5.5.2 Retention Period for Archive

As specified in the applicable CPS.

5.5.3 Protection of Archive

As specified in the applicable CPS.

5.5.4 Archive Backup Procedures

As specified in the applicable CPS.

5.5.5 Requirements for Time-stamping of Records

As specified in the applicable CPS.

5.5.6 Archive Collection System (internal or external)

No stipulation.

5.5.7 Procedures to Obtain and Verify Archive Information

No stipulation.

5.6 KEY CHANGEOVER

When rolling over a CA, DigiCert generates a new Key Pair and begins using the new certificate. The old CA Private Keys are still protected, and the old CA certificate is still made available to verify signatures until all of the certificates signed with the Private Key expire. Towards the end of a CA Private Key's lifetime, whether due to expiration or due to unilateral change by DigiCert, DigiCert ceases using the expiring CA Private Key to sign certificates and uses the old Private Key only to sign CRLs and OCSP responder certificates. At that time, a new CA signing Key Pair is commissioned. All subsequently issued Certificates and CRLs are signed with the new private signing key.

Both the old and new Key Pairs may be concurrently active. This key changeover process helps minimize any adverse effects from CA Certificate expiration. The new CA Public Key Certificate is provided to subscribers and relying parties through the delivery methods detailed in Section 6.1.4.

Where a cross-certified CA performs a key rollover, DigiCert obtains a new CA Public Key (PKCS#10) or new CA Certificate from the other CA and distributes a new CA Cross Certificate as specified herein.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

Issuing CAs must have a documented incident response plan that includes procedures for addressing serious security incidents or system compromise. Required CA emergency documentation includes an Incident Response Plan, a Disaster Recovery, or Business Continuity Plan (DR/BCP), and related resources. DR/BCP documentation must be tested annually on a calendar basis. The documentation must include how DigiCert will notify and reasonably protect Application Software Suppliers, subscribers, and Relying Parties if a disaster, security compromise, or business failure occurs.

5.7.1.1. Mass Revocation Plans

Issuer CAs must maintain a Mass Revocation Plan to ensure a rapid, consistent, and reliable response to large-scale certificate revocation events. The Mass Revocation Plan must be tested, reviewed, and updated at least annually. The Mass Revocation Plan must be made available to DigiCert and/or the Issuer CAs auditors upon request.

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

All CAs are required to make regular system back-ups on at least a weekly basis.

5.7.3 Entity Private Key Compromise Procedures

If the Issuer CA suspects that a CA Private Key is compromised or lost then the Issuer CA shall follow its Incident Response Plan and take appropriate action.

Following revocation of a CA Certificate and implementation of the Issuer CA's Incident Response Plan, the Issuer CA shall generate a new CA Key Pair and sign a new CA Certificate in accordance with its CPS. The Issuer CA shall distribute the new self-signed certificate in accordance with Section 6.1.4.

5.7.4 Business Continuity Capabilities after a Disaster

As specified in the applicable CPS.

5.8 CA OR RA TERMINATION

As specified in the applicable CPS.

6 TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

CA Key Pairs are generated in and protected by hardware security modules certified to at least FIPS 140-2 Level 3, FIPS 140-3 Level 3 or higher.

Key Pair generation requires the following process:

1. Prepare and follow a Key Pair generation script;
2. Have a qualified auditor witness the CA Key Pair generation process;
3. Have a qualified auditor issue a report opining that the CA followed its CA Key Pair generation ceremony during its key generation process and the controls to ensure the integrity and confidentiality of the CA Key Pair;
4. Generate the CA Key Pair in a physically secured environment;
5. Generate the CA Key Pair using personnel in trusted roles under the principles of multiple person control and split knowledge;
6. Generate the CA Key Pair within cryptographic modules meeting the applicable requirements of Section 6.2.11;
7. Log its CA Key Pair generation activities; and
8. Maintain effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in the applicable CPS and the CA Key Pair generation script

6.1.1.2 Subscriber Key Pair Generation

The Issuer CA shall reject a certificate request if one or more of the following conditions are met:

1. The Key Pair does not meet the requirements set forth in Section 6.1.5 and/or Section 6.1.6;
2. There is clear evidence that the specific method used to generate the Private Key was flawed;
3. The Issuer CA is aware of a demonstrated or proven method that exposes the Applicant's Private Key to compromise;
4. The Issuer CA has previously been notified that the applicant's Private Key has suffered a Key Compromise using the Issuer CA's procedure for revocation request as described in Section 4.9.3 and Section 4.9.12;
5. The Public Key corresponds to an industry-demonstrated weak Private Key. The following precautions SHALL be implemented:
   a. In the case of Debian weak keys vulnerability (https://wiki.debian.org/SSLkeys), the Issuer CA shall reject all keys found at https://github.com/cabforum/Debian-weak-keys/ for each key type (e.g. RSA, ECDSA) and size listed in the repository. For all other keys meeting the requirements of Section 6.1.5, with the exception of RSA key sizes greater than 8192 bits, the Issuer CA shall reject Debian weak keys.
   b. In the case of ROCA vulnerability, the Issuer CA shall reject keys identified by the tools available at https://github.com/crocs-muni/roca or equivalent.
   c. In the case of Close Primes vulnerability (https://fermatattack.secvuln.info/), the Issuer CA shall reject weak keys which can be factored within 100 rounds using Fermat's factorization method.
   Issuer CAs must not generate the key pair on behalf of a subscriber if the certificate request has an extendedKeyUsage extension containing either the values id-kp-serverAuth [RFC5280] or anyExtendedKeyUsage [RFC5280].

6.1.2 Private Key Delivery to Subscriber

The CA must never have access to the private key of TLS certificate subscribers.

6.1.3 Public Key Delivery to Certificate Issuer

As specified in the applicable CPS.

6.1.4 CA Public Key Delivery to Relying Parties

As specified in the applicable CPS.

6.1.5 Key Sizes

As specified in the applicable CPS and the CA/Browser Forum's TLS Baseline Requirements.

6.1.6 Public Key Parameters Generation and Quality Checking

As specified in the applicable CPS.

6.1.7 Key Usage Purposes (as per X.509 v3 key usage field)

As specified in the applicable CPS.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards and Controls

CAs must use cryptographic hardware modules validated to at least FIPS 140-2 Level 3.

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

Multiple trusted personnel are required to act before accessing and using a CA's Private Keys, including any Private Key backups.

6.2.3 Private Key Escrow

CAs may not escrow subscriber keys for TLS certificates.

6.2.4 Private Key Backup

CA and certificate status Private Keys are backed up under multi-person control.

6.2.5 Private Key Archival

Issuing CAs may not archive their CA Private Keys.

6.2.6 Private Key Transfer into or from a Cryptographic Module

All keys must be generated by and in a cryptographic module. CA and RA Private Keys are not permitted to exist in plain text outside of the cryptographic module. Private Keys are only exported from a cryptographic

module to perform CA key backup procedures. When transported between cryptographic modules, the Private Key is encrypted. The encryption key is protected from disclosure.

6.2.7 Private Key Storage on Cryptographic Module

All CA Private Keys are stored on a cryptographic module which has been evaluated to at least FIPS 140-2 Level 3.

6.2.8 Method of Activating Private Key

CAs must activate Private Keys in accordance with the specifications of the cryptographic module manufacturer.

6.2.9 Method of Deactivating Private Key

CAs must deactivate their Private Keys and store cryptographic modules in secure containers when not in use. CAs must prevent unauthorized access to any activated cryptographic modules.

6.2.10 Method of Destroying Private Key

CA and status server Private Keys are destroyed by individuals in trusted roles when the keys are no longer needed.

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

As specified in the applicable CPS.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

As specified in the applicable CPS but not to exceed the timeframe specified in the CA/Browser Forum's TLS Baseline Requirements.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

CAs use activation data that has sufficient strength to protect Private Keys from loss, theft, modification, unauthorized disclosure, or unauthorized use. DigiCert activates the cryptographic module containing its CA Private Keys according to the specifications of the hardware manufacturer. For roots and public issuing CAs, this method was evaluated as meeting the requirements of FIPS 140-2 Level 3.

Activation data may only be transmitted via an appropriately protected channel and at a time and place that is distinct from the delivery of the associated cryptographic module.
When passwords are required, Issuer CAs must enforce passwords that meet the requirements specified by the CAB/Forum's Network Security Requirements.

6.4.2 Activation Data Protection

Data used to unlock private keys from disclosure is protected using a combination of cryptographic and physical access control mechanisms. These procedures are described in internal policies.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

All CA systems must be configured to:

1. Authenticate the identity of users before permitting access to the system or applications;
2. Manage the privileges of users and limit users to their assigned roles;
3. Generate and archive audit records for all transactions;
4. Enforce domain integrity boundaries for security critical processes; and
5. Support recovery from key or system failure.
   CA operators protect the network from internal and external intrusion and limit the nature and source of activities that may access such systems and information.
   Multi-factor authentication must be enforced for all accounts capable of directly causing certificate issuance.

6.5.2 Computer Security Rating

No stipulation.

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

Issuer CAs may only use:

1. Commercial off-the-shelf software that was designed and developed under a formal and documented development methodology,
2. Hardware and software developed specifically for the CA by verified personnel, using a structured development approach and a controlled development environment,
3. Open source software that meets security requirements through software verification and validation, and a documented software development life cycle process,
4. Hardware and software purchased and shipped in a fashion that reduces the likelihood of tampering, and
5. For CA operations, hardware and software is dedicated only to performing the CA functions.
   CAs must have procedures that prevent malicious software from being loaded onto the CA equipment and must scan all hardware and software for malicious code on first use and periodically thereafter.

CAs use a formal configuration management methodology for installation and ongoing maintenance of any CMS. CAs must document and control modifications and upgrades to a CMS.

CAs must use linting software for all issued Certificates. CAs are required to monitor for updated versions of that software and plan for updates no later than 3 months from the release of the update.

6.6.2 Security Management Controls

CAs must document, control, monitor, and maintain the installation and configuration of its CA systems, including any modifications or upgrades. The CA verifies that all software is the correct version and is supplied by the vendor free of any modifications.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 NETWORK SECURITY CONTROLS

All CA and RA systems must be protected in accordance with the CA/Browser Forum's Network and Certificate System Security Requirements.

Vulnerability scans of networks must be performed at least once a quarter, and penetration tests at least annually. Remediation timelines are governed by severity, with critical vulnerabilities addressed within 48 hours and high/medium issues resolved within 45 to 60 days. Exceptions are documented, assessed for risk, and recorded.

6.8 TIME-STAMPING

Audit logs and archives should be time-stamped using a reliable time source.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

7.1.1 Version Number(s)

Publicly trusted certificates must be X.509 version 3 certificates.

7.1.2 Certificate Extensions

All certificate extensions must follow RFC5280 and comply with the Applicable Requirements.

7.1.3 Algorithm Object Identifiers

Certificates must be signed using an algorithm permitted by the Applicable Requirements. These algorithms are specified in the applicable CPS. All algorithms must meet the requirement specified in the TLS Baseline Requirements in Section 7 and the Applicable Requirements.

7.1.4 Name Forms

As specified in the applicable CPS.

7.1.5 Name Constraints

Technically Constrained Subordinate CA certificates are issued with an extended key usage extension. The extension does not include the anyExtendedKeyUsage key usage purpose. The extended key usage may contain values permitted by the Applicable Requirements.

7.1.6 Certificate Policy Object Identifier

An object identifier (OID) is a unique number that identifies an object or policy. OIDs are included as appropriate in certificates, including the relevant OIDs required by the CA/Browser Forum. Issuer CAs must disclose the OIDs included in publicly trusted certificates used in their CPS or a publicly available document.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

As specified in the applicable CPS.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 CRL PROFILE

7.2.1 Version number(s)

CRLs must be version 2 CRLs that conform to RFC5280.

7.2.2 CRL and CRL Entry Extensions

CRLs must use CRL extensions that conform to RFC 5280 and other requirements as applicable. CRLs containing revocation information about TLS Certificates conform to the TLS BR.

If a CRL entry reasonCode extension is present, the reason must indicate the appropriate reason for revocation of the certificate.

If a CRL entry is for a Root CA or Subordinate CA Certificate, including Cross Certificates, the reasonCode extension SHALL be present and MUST NOT be unspecified (0) or certificateHold(6).

Certificates may be revoked with one of the following reason codes. The codes are arranged in order of preference and in cases where multiple reason codes are applicable the code of highest preference should be used. cACompromise or aACompromise shall be used to indicate key compromise of Certificate Authority (CA) or Attribute Authority (AA) certificates respectively.

Code	Description	TLS Permitted
0	Unspecified; If permitted, the reasonCode extension should just be omitted	Yes, but not for CA certificates
1	keyCompromise	Yes
2	cACompromise	Yes

Code	Description	TLS Permitted
10	aACompromise	No
9	privilegeWithdrawn	Yes
5	cessationOfOperation	Yes
3	affiliationChanged	Yes
4	superseded	Yes
6	certificateHold	No
7	Value 7 is not used	No
8	removeFromCRL	No

7.2.3 CRL reasonCode Extension Entries

As specified in the applicable CPS.

7.3 OCSP PROFILE

OCSP services are operated in accordance with RFC 6960 and/or RFC 5019.

7.3.1 Version Number(s)

Issuing CAs shall configure OCSP responses in accordance with industry standards.

7.3.2 OCSP Extensions

The singleExtensions of an OCSP response shall not contain the reasonCode (OID 2.5.29.21) CRL entry extension.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The policies in this CP are designed to meet or exceed the requirements of generally accepted industry standards, including the latest versions of the WebTrust Programs for Certification Authorities as required by the Applicable Requirements in Section 1.1.

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

On at least an annual basis, Issuer CAs and any other participants contractually requiring an audit must retain an independent auditor for a period in time audit. This audit assesses the Issuer CA's and other parties' compliance with the applicable CPS. This audit must cover any CMSs, Sub CAs, RAs, and status servers that are used in the WebPKI. Any independent entity interoperating within the DigiCert PKI must submit its practices statement and the results of its compliance audit on an annual basis for review and approval.

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

Only a qualified auditor may perform the assessment described in Section 8.1. A qualified auditor means a natural person, legal entity, or group of natural persons or legal entities that collectively possess the following qualifications and skills:

1. Independence from the subject of the audit;
2. The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme;
3. Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
4. Licensed by WebTrust;
5. Bound by law, government regulation, or professional code of ethics; and
6. Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

Qualified auditors must not have a financial interest, business relationship, or course of dealing that could foreseeably create a significant bias for or against the audited party.

8.4 TOPICS COVERED BY ASSESSMENT

The audit covers the audited parties' business practices disclosure, the integrity of its PKI operations, and compliance with the relevant CP. At least one or a combination - as required by CA/B Forum or applicable Root Programs - of the audit schemes below must be used:
7. WebTrust Program for Certification Authorities;
8. WebTrust Principles and Criteria for Certification Authorities – SSL Baseline
9. WebTrust Principles and Criteria for Certification Authorities – Network Security
10. WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security
11. WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL;

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

If an audit reports a material noncompliance with applicable law, the relevant CPS, or any other contractual obligations related to the audited party's services, then:
12. The auditor will document the discrepancy,
13. The auditor will promptly notify DigiCert and the Issuer CA, and
14. The Issuer CA will develop a plan to cure the noncompliance.

DigiCert submits all curative plans to the DCPA for approval. Curative plans are submitted to other parties as necessary to fulfill DigiCert's legal obligations.

8.6 COMMUNICATION OF RESULTS

The results of each audit are reported to the DCPA for review and approval. Other parties may also receive a copy of the audit results.

Annual Audit Reports are made publicly available no later than three (3) months after the end of the audit period. If there is a delay greater than three (3) months, DigiCert will provide an explanatory letter signed by the Qualified Auditor.

8.7 SELF-AUDITS

Internal Auditors perform regular internal audits of a CAs operations, personnel, and compliance with this CP. Internal audits of certificate issuance are performed using a randomly selected sample of certificates issued since the last internal audit. Internal Auditors must self-audit at least three percent of TLS certificates on a quarterly basis. Audits of other certificate types will be at the discretion of the CA to gain reasonable assurance of compliance to applicable root program requirements.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

As specified in the applicable CPS.

9.1.2 Certificate Access Fees

As specified in the applicable CPS.

9.1.3 Revocation or Status Information Access Fees

As specified in the applicable CPS.

9.1.4 Fees for Other Services

As specified in the applicable CPS.

9.1.5 Refund Policy

As specified in the applicable CPS.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

As specified in the applicable CPS.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

As specified in the applicable CPS.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The following information is considered confidential and must be protected against disclosure using a reasonable degree of care:

1. Private Keys;
2. Activation data used to access Private Keys or to gain access to the CA system;
3. Business continuity, incident response, contingency, and disaster recovery plans;
4. Other security practices used to protect the confidentiality, integrity, or availability of information;
5. Information held by an Issuer CA as private information in accordance with Section 9.4;
6. Audit logs and archive records; and
7. Transaction records, financial audit records, and external or internal audit trail records and any audit reports (with the exception of an auditor's letter confirming the effectiveness of the controls set forth in this CP).

9.3.2 Information Not Within the Scope of Confidential Information

Any information not listed as confidential is considered public information. Published certificate and revocation data is considered public information.

9.3.3 Responsibility to Protect Confidential Information

Issuer CA employees, agents, and contractors are responsible for protecting confidential information and are contractually obligated to do so. Employees receive training on how to handle confidential information.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

As specified in the applicable CPS.

9.4.2 Information Treated as Private

As specified in the applicable CPS.

9.4.3 Information Not Deemed Private

Subject to local laws, private information does not include certificates, CRLs, or their contents.

9.4.4 Responsibility to Protect Private Information

As specified in the applicable CPS.

9.4.5 Notice and Consent to Use Private Information

For public certificates issued to corporate subscribers, personal information collected during the application or identity verification process is considered private information. For individual subscriber certificates, personal information is considered private unless such information is required to be included in the certificate.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

As specified in the applicable CPS.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

No stipulation.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

Except as expressly stated in this CP or in a separate agreement with a subscriber, DigiCert does not make any representations regarding its products or services. DigiCert represents, to the extent specified in this CP, that DigiCert complies, in all material aspects, with this CP and all applicable laws and regulations.

9.6.2 RA Representations and Warranties

No stipulation.

9.6.3 Subscriber Representations and Warranties

DigiCert does not make representations to subscribers for certificates issued by third party CAs.

9.6.4 Relying Party Representations and Warranties

Each Relying Party represents that, prior to relying on a Certificate, it:

1. Obtained sufficient knowledge on the use of digital certificates and PKI,
2. Studied the applicable limitations on the usage of certificates and agrees to applicable limitations on liability related to the use of certificates,
3. Has read, understands, and agrees to the applicable CPS and this CP,
4. Will not use a certificate if the certificate has expired or been revoked, and
5. Any unauthorized reliance on a certificate is at a party's own risk.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

EXCEPT AS EXPRESSLY STATED IN SECTION 9.6.1, ALL CERTIFICATES AND ANY RELATED SOFTWARE AND SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE". TO THE MAXIMUM EXTENT PERMITTED BY LAW, DIGICERT DISCLAIMS ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING ALL WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. DIGICERT DOES NOT WARRANT THAT ANY SERVICE OR PRODUCT WILL MEET ANY EXPECTATIONS OR THAT ACCESS TO CERTIFICATES WILL BE TIMELY OR ERROR-FREE. DigiCert does not guarantee the availability of any products or services and may modify or discontinue any product or service offering at any time.

9.8 Limitations of Liability

NOTHING HEREIN LIMITS LIABILITY RELATED TO (I) DEATH OR PERSONAL INJURY RESULTING FROM DIGICERT'S NEGLIGENCE OR (II) FRAUD COMMITTED BY DIGICERT. EXCEPT AS STATED ABOVE, ANY ENTITY USING A DIGICERT CERTIFICATE OR SERVICE WAIVES ALL LIABILITY OF DIGICERT RELATED TO SUCH USE, PROVIDED THAT DIGICERT HAS MATERIALLY COMPLIED WITH THIS CP IN PROVIDING THE CERTIFICATE OR SERVICE. DIGICERT'S LIABILITY FOR CERTIFICATES AND SERVICES THAT DO NOT MATERIALLY COMPLY WITH THIS CP IS LIMITED AS SET FORTH IN THE NETSURE EXTENDED WARRANTY PROTECTION PLAN AND THE DIGICERT RELYING PARTY AGREEMENT.

All liability is limited to actual and legally provable damages. DigiCert is not liable for:

1. Any indirect, consequential, special, or punitive damages or any loss of profit, revenue, data, or opportunity, even if DigiCert is aware of the possibility of such damages;
2. Liability related to fraud or willful misconduct of the Applicant;
3. Liability related to use of a Certificate that exceeds the limitations on use, value, or transactions as stated either in the Certificate or this CP;
4. Liability related to the security, usability, or integrity of products not supplied by DigiCert, including the subscriber's and Relying Party's hardware; or
5. Liability related to the compromise of a subscriber's Private Key.

The limitations in this section apply to the maximum extent permitted by law and apply regardless of (i) the reason for or nature of the liability, including tort claims, (ii) the number of claims of liability, (iii) the extent or nature of the damages, (iv) whether DigiCert failed to follow any provision of this CP, or (v) whether any provision of this CP was proven ineffective. The disclaimers and limitations on liabilities in this CP are fundamental terms to the use of DigiCert's Certificates and services.

To the extent DigiCert has issued and managed the certificate(s) at issue in compliance with this CP, 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 any extended warranty protection program. Limitations of liability shall include an exclusion of indirect, special, incidental, and consequential damages.

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 DigiCert

To the extent permitted by applicable law, DigiCert shall indemnify each Application Software Vendor against any claim, damage, or loss suffered by an Application Software Vendor related to an EV Certificate issued by DigiCert, regardless of the cause of action or legal theory involved, except where the claim, damage, or loss suffered by the Application Software Vendor was directly caused by the Application Software Vendor's software displaying either (1) a valid and trustworthy EV Certificate as not valid or trustworthy or (2) displaying

as trustworthy (i) an EV Certificate that has expired or (ii) a revoked EV Certificate where the revocation status is available online but the Application Software Vendor's software failed to check or ignored the status.

9.9.2 Indemnification by Subscribers

To the extent permitted by law, each Subscriber shall indemnify DigiCert, its partners, and any cross-signed entities, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to (i) any misrepresentation or omission of material fact by Subscriber, regardless of whether the misrepresentation or omission was intentional or unintentional; (ii) Subscriber's breach of the Subscriber Agreement, this CP, or applicable law; (iii) the compromise or unauthorized use of a Certificate or Private Key caused by the Subscriber's negligence or intentional acts; or (iv) Subscriber's misuse of the Certificate or Private Key.

The applicable Subscriber Agreement may include additional indemnity obligations.

9.9.3 Indemnification by Relying Parties

To the extent permitted by law, each Relying Party shall indemnify DigiCert, its partners, and any cross- signed entities, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to the Relying Party's (i) breach of the Relying Party Agreement, an End-User License Agreement, this CP, or applicable law; (ii) unreasonable reliance on a Certificate; or (iii) failure to check the Certificate's status prior to use.

9.10 Term and Termination

9.10.1 Term

This CP and any amendments to the CP are effective when published to DigiCert's online repository and remain in effect until replaced with a newer version.

9.10.2 Termination

This CP as amended from time to time, shall remain in effect until replaced by a newer version.

9.10.3 Effect of Termination and Survival

DigiCert will communicate the conditions and effect of this CP's termination via the DigiCert Repository. The communication will specify which provisions survive termination. At a minimum, all responsibilities related to protecting confidential information will survive termination. All Subscriber Agreements remain effective until the certificate is revoked or expired, even if this CP terminates.

9.11 Individual Notices and Communications With Participants

DigiCert accepts notices related to this CP at the locations specified in Section 2.2. Notices are deemed effective after the sender receives a valid and digitally signed acknowledgment of receipt from DigiCert. If an acknowledgement of receipt is not received within five days, the sender must resend the notice in paper form to the street address specified in Section 2.2 using either a courier service that confirms delivery or via certified or registered mail with postage prepaid and return receipt requested. DigiCert may allow other forms of notice in its Subscriber Agreements.

Notices to Application Software Vendors are sent out in accordance with the respective requirements.

9.12 Amendments

9.12.1 Procedure for Amendment

This CP is reviewed annually. Amendments are made by posting an updated version of the CP to the online repository. Updates supersede any designated or conflicting provisions of the referenced version of the CP. Controls are in place to reasonably ensure that this CP is not amended and published without the prior authorization of the DCPA.

9.12.2 Notification Mechanism and Period

DigiCert posts revisions of this CP to its website. DigiCert does not guarantee or set a notice-and- comment period and may make changes to this CP without notice and without changing the version number. Major changes affecting accredited Certificates are announced and approved by the accrediting agency prior to becoming effective. The DCPA is responsible for determining what constitutes a material change of the CP.

9.12.3 Circumstances under which OID Must Be Changed

The DCPA is solely responsible for determining whether an amendment to the CP requires an OID change.

9.13 Dispute Resolution Provisions

For dispute resolution, to the extent permitted by law, before a Participant files suit or initiates an arbitration claim with respect to a dispute involving any aspect of this Agreement, Participant shall notify DigiCert, and any other party to the dispute for the purpose of seeking business resolution. Both Participant and DigiCert shall make good faith efforts to resolve such dispute via business discussions. If the dispute is not resolved within sixty (60) days after the initial notice, then a party may proceed as permitted under applicable law and as specified under this CP and other relevant agreements.

1. Arbitration: In the event a dispute is allowed or required to be resolved through arbitration, the parties will maintain the confidential nature of the existence, content, or results of any arbitration hereunder, except as may be necessary to prepare for or conduct the arbitration hearing on the merits, or except as may be necessary in connection with a court application for a preliminary remedy, a judicial confirmation or challenge to an arbitration award or its enforcement, or unless otherwise required by law or judicial decision.

2. Class Action and Jury Trial Waiver: THE PARTIES EXPRESSLY WAIVE THEIR RESPECTIVE RIGHTS TO A JURY TRIAL FOR THE PURPOSES OF LITIGATING DISPUTES HEREUNDER. Each party agrees that any dispute must be brought in the respective party's individual capacity, and not as a plaintiff or class member in any purported class, collective, representative, multiple plaintiffs, or similar proceeding ("Class Action"). The parties expressly waive any ability to maintain any Class Action in any forum in connection with any dispute. If the dispute is subject to arbitration, the arbitrator will not have authority to combine or aggregate similar claims or conduct any Class Action nor make an award to any person or entity not a party to the arbitration. Any claim that all or part of this Class Action waiver is unenforceable, unconscionable, void, or voidable may be determined only by a court of competent jurisdiction and not by an arbitrator.

9.14 Governing Law

The (i) laws that govern the interpretation, construction, and enforcement of this Agreement and all matters, claims or disputes related to it, including tort claims, and (ii) the courts or arbitration bodies that have exclusive jurisdiction over any of the matters, claims or disputes contemplated in sub-Section (i) above, will each depend on where Customer is domiciled as set forth in the table below; provided, for clarity, that rights and obligations arising from other applicable local laws continue to be governed by such laws.

In instances where the International Chamber of Commerce is designated below as the court or arbitration body with exclusive jurisdiction of such matters, claims or disputes, then the parties hereby agree that (x) all matters, claims or disputes arising out of or in connection with this Agreement shall be finally settled under the Rules of Arbitration of the International Chamber of Commerce (Rules) by one or more arbitrators appointed in accordance with the Rules, (y) judgment on the award rendered by such arbitration may be entered in any court having jurisdiction, and (z) this arbitration clause shall not preclude parties from seeking provisional remedies in aid of arbitration from a court of appropriate jurisdiction.

Customer is Domiciled in or the Services are	**Governing Law is laws of**	**Court or arbitration body with exclusive jurisdiction**
The United States of America, Canada, Mexico, Central America, South America, the Caribbean, or any other country not otherwise included in the rest of the table below	Utah state law and United States federal law	State and Federal courts located in Salt Lake County, Utah
Europe, Switzerland, the United Kingdom, Russia, the Middle East or Africa	England	International Chamber of Commerce, International Court of Arbitration, with seat of arbitration in the below city corresponding to the DigiCert Europe contracting entity listed in the Order Form. For CH: Zurich For NL: Amsterdam For DE: Munich For BE/DigiCert Europe: Brussels For UK: London
Japan	Japan	International Chamber of Commerce, International Court of Arbitration, with seat of arbitration in Tokyo
Australia or New Zealand	Australia	International Chamber of Commerce, International Court of Arbitration, with seat of arbitration in Melbourne
A Country in Asia or the Pacific region, other than Japan, Australia or New Zealand	Singapore	International Chamber of Commerce, International Court of Arbitration, with seat of arbitration in Singapore

9.15 Compliance With Applicable Law

This CP is subject to all applicable laws and regulations, including United States restrictions on the export of software and cryptography products. Subject to Section 9.4.5's Notice and Consent to Use Private Information contained in Certificates, DigiCert meets the requirements of the European data protection laws and has established appropriate technical and organizational measures against unauthorized or unlawful processing of personal data and against the loss, damage, or destruction of personal data.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

DigiCert contractually obligates each sub CA to comply with this CP and applicable industry guidelines. DigiCert also requires each party using its products and services to enter into an agreement that delineates the terms associated with the product or service. If an agreement has provisions that differ from this CP, then the agreement with that party controls, but solely with respect to that party. Third parties may not rely on or bring action to enforce such agreement.

9.16.2 Assignment

Any entities operating under this CP may not assign their rights or obligations without the prior written consent of DigiCert. Unless specified otherwise in a contract with a party, DigiCert does not provide notice of assignment.

9.16.3 Severability

If any provision of this CP is held invalid or unenforceable by a competent court or tribunal, the remainder of the CP will remain valid and enforceable. Each provision of this CP that provides for a limitation of liability, disclaimer of a warranty, or an exclusion of damages is severable and independent of any other provision.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

DigiCert may seek indemnification and attorneys' fees from a party for damages, losses, and expenses related to that party's conduct. DigiCert's failure to enforce a provision of this CP does not waive DigiCert's right to enforce the same provision later or right to enforce any other provision of this CP. To be effective, waivers must be in writing and signed by DigiCert.

9.16.5 Force Majeure

DigiCert is not liable for any delay or failure to perform an obligation under this CP to the extent that the delay or failure is caused by an occurrence beyond DigiCert's reasonable control. The operation of the Internet is beyond DigiCert's reasonable control.

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

9.17 Other Provisions

No stipulation.