digicert®

DigiCert Public Trust Certificate Policy/Certificate Practices Statement

Version 7.03

September 25, 2024

DigiCert, Inc.

digicert®

Contents

1. Introduction

1.1. Overview

This Certificate Policy/Certification Practices Statement (CP/CPS) defines the policies, principles and practices related to DigiCert's certification and time-stamping services. This document applies to all entities participating in or using DigiCert's Publicly Trusted PKI and specifically excludes participants in DigiCert's Private PKI services, which are not cross-certified or publicly trusted.

This CP/CPS governs certificates issued under the following policies, guidelines and standards:

- The Adobe Approved Trust List Technical Requirements (AATL) - https://helpx.adobe.com/content/dam/help/en/acrobat/kb/approved-trust-list2/_jcr_content/main-pars/download-section/download-1/aatl_technical_requirements_v2.0.pdf
- The Certification Authority / Browser Forum ("CA/B Forum") Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("TLS BRs") - https://cabforum.org/baseline-requirements-documents
- The CAB Forum Guidelines for Extended Validation Certificates ("EVGs") - https://cabforum.org/extended-validation
- The CAB Forum Guidelines for the Issuance and Management of Code Signing Certificates ("CS BRs") - https://cabforum.org/baseline-requirements-code-signing
- The CAB Forum Network and Certificate System Security Requirements - https://cabforum.org/network-security-requirements
- The CAB Forum S/MIME Baseline Requirements ("S/MIME BRs") - https://cabforum.org/smime-br
- 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/enUS/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/chromium-security/root-ca-policy

DigiCert's Public Trust CP/CPs is one of several documents that govern the certification services provided by DigiCert. Other documents include but are not limited to specific agreements with customers, relying party agreements and DigiCert's Privacy 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/CPS.

1.2. Document Name and Identification

The name of this document is the DigiCert Public Trust Certificate Policy/Certification Practices Statement (CP/CPS). The document follows the framework outlined in RFC3647.

The OID arc for DigiCert is joint-iso-ccitt (2) country (16) USA (840) US-company (1) DigiCert (114412).

This CP/CPS was approved for publication on July 29th, 2024 and the table below specifies all revisions.

Date	Changes	Version
2024-07-29	This document replaces the Digicert Certificate Policy v6.06 and DigiCert Certification Practices Statement v6.06	7.0
2024-08-27	Amend CAA identifiers in Section 4	7.01
2024-09-15	Update CAA for S/MIME, clarify logging requirements, include linting process	7.02
2024-09-25	Fix typo in section 4.2.2.	7.03

1.3. PKI PARTICIPANTS

1.3.1. Certification Authorities

DigiCert operates Certification Authorities (CAs) and Time Stamping Authorities (TSA). These services are managed by the DigiCert Policy Authority (DCPA) which is composed of DigiCert management members appointed by DigiCert's executive management. The DCPA is responsible for approving this document and overseeing the conformance of CA practices with this document. Policies and practices described within this document are designed to ensure DigiCert complies with the Applicable 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.

DigiCert and subordinate Issuer CAs may act as RAs for certificates they issue. Validation of domains and IP addresses in TLS and S/MIME Certificates cannot be delegated to a third party. Other obligations under this CP/CPS may be delegated to third party Registration Authorities (RA). DigiCert may also delegate the verification of certificate requests to Enterprise RAs. Enterprise RAs may only verify information for their own organization and may not verify domain or email information included in publicly trusted TLS or S/MIME certificates.

Delegated Third Parties are contractually obligated to abide by all relevant Applicable Requirements.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 to DigiCert's services may be natural persons or legal entities. Prior to issuance of a certificate, a Subscriber is an Applicant. Subscribers utilize DigiCert products and services to support communications, transactions and other relevant functions. 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 provided by DigiCert. 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

Subscribers and Relying Parties must use certificates in accordance with the relevant agreements. The sensitivity of the information which DigiCert's portfolio of publicly trusted certificates is used to protect varies between subscribers and as such each relying party must assess the risk prior to relying on a certificate.

1.4.1. Appropriate Certificate Uses

The appropriate use for a certificate issued pursuant to this CP/CPS depends on the product type which is typically specified by Key Usage and Extended Key Usage extensions in a certificate. However, the sensitivity of the information processed or protected by a certificate varies greatly, and each Relying Party must evaluate the application environment and associated risks before deciding on whether to use the certificate.

DV TLS - Used to secure online communication where the risks and consequences of data compromise are low such as non-monetary transactions or transactions with little risk of fraud or malicious access.

OV TLS - Used to secure online communication where the risks and consequences of data compromise are moderate, including transactions having substantial monetary value or risk of fraud or involving access to private information where the likelihood of malicious access is substantial.

EV TLS - Used to secure online communication where risks and consequences of data compromise are high, including transactions having high monetary value, risk of fraud, or where involving access to private information where the likelihood of malicious access is high.

Code Signing and EV Code Signing - Establishes the identity of the Subscriber named in the Certificate and that the signed code has not been modified since signing.

S/MIME - Used to provide reasonable assurance to recipients of email messages that the Subject identified in an S/MIME Certificate has control of the domain or Mailbox Address being asserted.

Document Signing - Used to sign electronic documents in place of a wet signature.

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. Code Signing Certificates do not indicate that the signed code is safe to install or free from malware, bugs, or vulnerabilities.

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.

DigiCert strongly discourages key pinning and does not consider key pinning a reason to delay revocation. DigiCert counsels customers on the way pinning impacts the agility of the WebPKI (e.g., rotation of intermediate certificates) and always advises against it. Customers should 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/CPS.

1.5.2. Contact Person

DigiCert Policy Authority
2801 N. Thanksgiving Way, Suite 500
Lehi, UT 84043 USA
policy@digicert.com

1.5.2.1. Revocation Reporting Contact Person

DigiCert Technical Support
2801 N. Thanksgiving Way, Suite 500
Lehi, UT 84043 USA
revoke@digicert.com

Revocations can also be submitted through our Compromised Key Reporting and Revocation Service: https://problemreport.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/CPS Approval Procedures

The DigiCert Public Trust CP/CPS 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.

Definition	Description
Application Software Vendor	A software developer whose software displays or uses DigiCert Certificates and distributes DigiCert's 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.
Certification Authority Authorization or CAA	From RFC 9495: "The Certification Authority Authorization (CAA) DNS resource record (RR) provides a mechanism for domains to express the allowed set of Certification Authorities that are authorized to issue certificates for the domain." CAA Resource Records allow a public CA to implement additional controls to reduce the risk of unintended certificate mis-issue.
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 Approver	Defined in the EV Guidelines.
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.
Certificate Requester	Defined in the EV Guidelines.
Contract Signer	Defined in the EV Guidelines.
Domain Name	An ordered list of one or more Domain Labels assigned to a node in the Domain Name System.
EV Guidelines	Defined in Section 1.1.
Hardware Crypto Module	A tamper-resistant device, with a cryptography processor, used for the specific purpose of protecting the lifecycle of cryptographic keys (generating, managing, processing, and storing).
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.
IP Address	A 32-bit or 128-bit number assigned to a device that uses the Internet Protocol for communication.
Issuer CA	Any CA issuing Certificates under this CP/CPS
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.

Definition	Description
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.
Mailbox address	An Email Address as specified in Section 4.1.2 of RFC 5321 and amended by Section 3.2 of RFC 6532, with no additional padding or structure.
OCSP Responder	An online software application operated under the authority of DigiCert and connected to its repository for processing certificate status requests.
Onion Domain Name	A Fully Qualified Domain Name ending with the RFC 7686 ".onion Special-Use Domain Name. For example, 2gzyxa5ihm7nsggfxnu52rck2vv4rvmdlkiu3zzui5du4xyclen53wid.onion is an Onion Domain Name, whereas torproject.org is not an Onion Domain Name.
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 or accessing or using DigiCert's Repository. The Relying Party Agreement is available for reference through a DigiCert online repository.
Reserved IP Address	An IPv4 or IPv6 address that is contained in the address block of any entry in either of the following IANA registries: https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml https://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.xhtml
Signing Service	An organization that generates the Key Pair and securely manages the Private Key associate with a Code Signing Certificate on behalf of a Subscriber.
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.

Definition	Description
Subscriber	Either the entity identified as the subject in the Certificate or the entity that is receiving DigiCert's time-stamping services.
Subscriber Agreement	An agreement that governs the issuance and use of a Certificate that the Applicant must read and accept before receiving a Certificate.
Suspect Code	Code that contains malicious functionality or serious vulnerabilities, including spyware, malware and other code that installs without the user's consent and/or resists its own removal, code that compromises user security and/or code that can be exploited in ways not intended by its designers to compromise the trustworthiness of the Platforms on which it executes
WebTrust	The current version of CPA Canada's WebTrust Program for Certification Authorities.
WHOIS	Information retrieved directly from the Domain Name Registrar or registry operator via the protocol, the Registry Data Access Protocol, or an HTTPS website.

1.6.2. Acronyms

Acronym	Description
AATL	Adobe Approved Trust List
CA	Certificate Authority or Certification Authority
CAA	Certification Authority Authorization
CAB or CA/B	"CA/Browser" as in "CAB Forum"
CMS	Certificate Management System
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CT	Certificate Transparency
DBA	Doing Business As (also known as "Trading As")
DCPA	DigiCert Policy Authority
DNS	Domain Name Service
DV	Domain Validated
ETSI	European Telecommunications Standards Institute EU
EV	Extended Validation

Acronym	Description
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IdM	Identity Management System
IDN	Internationalized Domain Name
IETF	Internet Engineering Task Force
IGTF	International Grid Trust Federation
ITU	International Telecommunication Union
IV	Individual Validated
MICS	Member-Integrated Credential Service (IGTF)
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OV	Organization Validated
PKI	Public Key Infrastructure
PKIX	IETF Working Group on Public Key Infrastructure
RA	Registration Authority
RFC	Request for Comments (at IETF.org)
SAN	Subject Alternative Name
SHA	Secure Hashing Algorithm
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)
SSL	Secure Sockets Layer
TLD	Top-Level Domain
TLS	Transport Layer Security
TSA	Time Stamping Authority

Acronym	Description
TST	Time-Stamp Token
TTL	Time To Live
UTC	Coordinated Universal Time
X.509	The ITU-T standard for Certificates and their corresponding authentication framework

1.6.3. References

- WebTrust Principles and Criteria for Certification Authorities
- WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security
- WebTrust for Certification Authorities – Extended Validation SSL
- WebTrust for Certification Authorities – Publicly Trusted Code Signing Certificates
- WebTrust for Certification Authorities – S/MIME Certificates

2. Publication and Repository Responsibilities

2.1. Repositories

Issuer CAs must publish in an online and 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 CPS documents. DigiCert also publishes its standard Relying Party Agreements and Subscriber Agreements.

DigiCert's legal repository for most services is located at https://www.digicert.com/legal-repository/

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 84043
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 this CP/CPS.

Issuer CAs shall host test web pages that allow Application Software Suppliers to test their software with subscriber certificates that chain up to each publicly trusted Root Certificate.

2.3. Time or Frequency of Publication

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

CRLs for Subscriber Certificates that are subject to the TLS and S/MIME Baseline Requirements and that have CRL requirements are issued at least once every seven days. CRLs for CAs that only issue CA Certificates subject to the applicable Baseline Requirements are generally issued at least annually or within 24 hours of revoking the CA certificate. CRLs for Authenticated Content Signing (ACS) Root CAs are published annually and also whenever a CA Certificate is revoked.

Certificates are typically removed from CRLs after the expiration date, except for Code Signing and Timestamp Certificates which may remain on the CRL for at least 10 years after its expiration.

CP/CPS documents are updated at least every 365 days to describe in detail how Issuer CAs comply with the Applicable Requirements. Those updates indicate conformance using version number control. Significant changes are added to a changelog entry.

New or modified versions of this document, Subscriber Agreements, or Relying Party Warranties are typically published within seven days after their approval.

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. Certificate Lifecycle Operational Requirements

3.1.1. Types of Names

The issuer and distinguished name fields of a certificate are populated in accordance DigiCert's certificate profiles. Issuer CAs may require different profiles which align with the Applicable Requirements.

3.1.2. Need for Names to be Meaningful

Personal names included in certificates issued to individuals are a meaningful representation of the authenticated common name of the subscriber.

Issuer CAs may provide information as the User Principal Name (UPN) in the SubjectAltName extension of certificates at the request of an Applicant. UPN details are not independently validated.

3.1.3. Anonymity or Pseudonymity of Subscribers

Issuer CAs may issue pseudonymous subscriber certificates if they are not prohibited by policy and any applicable name space uniqueness requirements are met.

For S/MIME Certificates with the pseudonym attribute, the associated subject must be verified according to Section 3.2.4 of the S/MIME Baseline Requirements. The pseudonym shall be either a unique identifier selected by the Issuer CA for the subject of the certificate, or an identifier selected by the Enterprise RA which identifies the subject of the certificate within the organization.

3.1.4. Rules for Interpreting Various Name Forms

Distinguished Names in certificates are interpreted using X.500 standards and ASN.1 syntax. DigiCert may allow the conversion of identity information usually rendered in non-ASCII characters (for example é and à may be represented by e or a, and umlauts such as ö or ü may be represented by oe or ue, o or u respectively). DigiCert may use language variants (such as Munich or München) for geographic names. For personal names, DigiCert may include an ASCII character name that is not a direct conversion of the Applicant's registered name after verifying the name using a Reliable Data Source or suitable Attestation.

3.1.5. Uniqueness of Names

Unique subject names are generally not enforced. Uniqueness between certificates is maintained by assigning unique certificate serial numbers.

3.1.6. Recognition, Authentication, and Role of Trademarks

Applicants are prohibited from using names in their certificate applications that infringe on the Intellectual Property Rights of others. Issuer CAs are entitled, without liability to any applicant, to reject or revoke any certificate application because of such dispute.

3.2. Initial Identity Validation

DigiCert may use any means of communication or investigation to ascertain the identity of an organizational or individual Applicant. The application for a certificate may be refused by an Issuer CA in its sole discretion.

Sources used for S/MIME and EV validation are publicly disclosed in our repository:
https://github.com/digicert/reports/tree/master/validation-sources

DigiCert may request documents to assist with validating your certificate request in accordance with the Applicable Requirements. These documents will be used in accordance with Section 9.4 of this CP/CPS.

3.2.1. Method to Prove Possession of Private Key

No stipulation

3.2.2. Authentication of Organization Identity

Issuer CAs shall maintain and regularly review internal policies and procedures that ensure compliance with the Applicable Requirements when vetting the identity of organizations.

3.2.2.1. Organization Validated

DigiCert relies on a QGIS, QTIS, Incorporating Agency, QIIS, Legal Entity Identifier (LEI) (SMIME only), Reliable Data Source or attestation letter to verify the identity of a business or trade name of the applicant. DigiCert may also visit the site to verify identity. Organization verification is required for TLS, Code Signing, and S/MIME certificates that contain a value in the organizationName (O) field.

Address information is also verified whenever an Organization Name is present in the certificate subject.

The same documentation may be used to verify the address, telephone number or email address of the applicant. In addition to the above, DigiCert may accept a utility bill, bank statement, credit card statement or other form of identification determined reliable to verify the address, telephone number or email address.

3.2.2.2. Extended Validation (EV) and Extended Validation Code Signing (EVCS)

3.2.2.2.1. Private Organizations

Organizations are considered Private Organizations when they meet the following criteria:

- The Private Organization must be a legally recognized entity whose existence was created by a filing with (or an act of) the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration (e.g., by issuance of a certificate of incorporation) or is an entity that is chartered by a state or federal regulatory agency;
- The Private Organization should have a Registration (or similar) Number assigned to it by the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration, as appropriate. If the Jurisdiction of Incorporation or Registration does not provide a Registration Number, then the date of Incorporation or Registration is used.
- The Private Organization must designate with the Incorporating or Registration Agency either a Registered Agent, or a Registered Office (as required under the laws of the Jurisdiction of Incorporation or Registration) or an equivalent facility;
- The Private Organization must not be designated on the records of the Incorporating or Registration Agency by labels such as “inactive,” “invalid,” “not current,” or the equivalent;
- The Private Organization, or their Affiliate’s, Parent Company’s, or Subsidiary Company’s date of formation is indicated by a QGIS as at least 3 years prior to the date of the certificate request or is listed in QTIS or QIIS;
- The Private organization must have a verifiable physical existence and business presence;
- The Private Organization’s Jurisdiction of Incorporation, Registration, Charter, or License, and/or its Place of Business must not be in any country where DigiCert is prohibited from doing business or issuing a certificate;

3.2.2.2.2. Government Entities

Government Entities are Organizations that meet the following criteria:

- The legal existence of the Government Entity must be established by the political subdivision in which such Government Entity operates;
- For Government Entities that do not have a Registration Number or readily verifiable date of creation, the phrase "Government Entity" is used in its place.
- The Government Entity must not be in any country where DigiCert is prohibited from doing business or issuing a certificate by the laws of DigiCert's jurisdiction;

3.2.2.2.3. Business Entity Subjects

Business Entities are organizations that do not qualify under the criteria listed for Private Organizations but that do satisfy the following requirements:

- The Business Entity must be a legally recognized entity whose formation included the filing of certain forms with the Registration Agency in its Jurisdiction, the issuance or approval by such Registration Agency of a charter, certificate, or license, and whose existence can be verified with that Registration Agency;
- For Business Entities, the Registration Number that was received by the Business Entity upon government registration is entered in this field. For those Business Entities that register with an Incorporating Agency or Registration Agency in a jurisdiction that does not issue numbers pursuant to government registration, the date of the registration is entered into this field;
- The Business Entity must have a verifiable physical existence and business presence;
- At least one Principal Individual associated with the Business Entity must be identified and validated;
- The identified Principal Individual must attest to the representations made in the Subscriber Agreement;
- Where the Business Entity represents itself under an assumed name, DigiCert verifies the Business Entity's use of the assumed name;
- The Business Entity and the identified Principal Individual associated with the Business Entity must not be located or residing in any country where the DigiCert is prohibited from doing business or issuing a certificate by the laws of the DigiCert's jurisdiction;

3.2.2.2.4. Non-Commercial Entities

Non-Commercial Entities are Organization that meet the following criteria:

- The Applicant is an International Organization Entity, created under a charter, treaty, convention, or equivalent instrument that was signed by, or on behalf of, more than one country's government. The CA/Browser Forum may publish a listing of applicants who qualify as an International Organization for EV eligibility;
- For Non-Commercial Entities that do not have a Registration Number or readily verifiable date of creation, the phrase "International Organization Entity" is used in its place;
- The applicant is not headquartered in any country where DigiCert is prohibited from doing business or issuing a certificate.

3.2.2.3. S/MIME Organization Validation

The following requirements are fulfilled to authenticate Organization identity included in the Organization-validated and Sponsor-validated S/MIME profiles.

3.2.2.3.1. Attribute collection of organization identity

DigiCert collects and retains evidence supporting the following identity attributes for the Organization:

1. Formal name of the Legal Entity;
2. A registered Assumed Name for the Legal Entity (if included in the Subject);
3. An Affiliate of the Legal Entity as described in Section 7.1.4.2.2 (if included in the Subject as an subject:organizationalUnitName);
4. An address of the Legal Entity (if included in the Subject);
5. Jurisdiction of Incorporation or Registration of the Legal Entity; and
6. Unique identifier and type of identifier for the Legal Entity.

The unique identifier is included in the Certificate subject:organizationIdentifier as specified in Section 7.1.4.2.2 and Appendix A of the CA/B Forum *Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates*.

If an Attestation is used as evidence for the validation of the attributes described in this section, then the Attestation SHALL be verified for authenticity as described in Section 3.2.12.2

3.2.2.3.2. Verification of name, address, and unique identifier

The full legal name and an address (if included in the Certificate Subject) of the Legal Entity Applicant are verified using documentation provided by, or through communication with, at least one of the following:

1. A government agency in the jurisdiction of the Legal Entity's creation, existence, or recognition;
2. A Legal Entity Identifier (LEI) data reference;
3. A site visit by the CA or a third party who is acting as an agent for the CA; or
4. An Attestation which includes a copy of supporting documentation used to establish the Applicant's legal existence (such as a certificate of registration, articles of incorporation, operating agreement, statute, or regulatory act) and its current status.

The Issuer CA MAY use the same documentation or communication described in 1 through 4 above to verify both the Applicant's identity and address.

In cases 1 and 4 above, the Issuer CA verifies that the status of the Applicant is not designated by labels such as "ceased," "inactive," "invalid," "not current," or the equivalent.

In case 2 above when LEI data reference is used, the Issuer CA verifies that the RegistrationStatus is ISSUED and the EntityStatus is ACTIVE. The CA only allows use of an LEI if the ValidationSources entry is FULLY_CORROBORATED. An LEI is not used if ValidationSources entry is PARTIALLY_CORROBORATED, PENDING, or ENTITY_SUPPLIED_ONLY.

3.2.2.4 Document Signing

DigiCert or an RA relies on a QGIS, QTIS, QIIS or Incorporating Agency to verify the identity of the applicant. In addition to the above, DigiCert or the RA may rely on a utility bill, bank statement, credit card statement or other form of identification determined reliable to verify the address, telephone number and email address of the applicant.

The authorized representative of an organization applicant is verified by appearing before a Third Party Validator (See section 3.2.7 Third-Party Validators), a DigiCert representative or an RA. Other processes providing equivalent assurance of positive identification may be used.

3.2.2.3.3. Verification of Assumed Name

Applicants MAY request an Assumed Name to be included in the Certificate. The Issuer CA verifies that:

1. The Applicant has registered its use of the Assumed Name with the appropriate government agency for such filings in the jurisdiction of its incorporation or registration; and
2. The Assumed Name filing continues to be valid.

The CA MAY rely on an Attestation that indicates the Assumed Name under which the Applicant conducts business, the government agency with which the Assumed Name is registered, and that such filing continues to be valid.

3.2.3. Authentication of Individual Identity

Individuals specified in a S/MIME or TLS certificate are verified using a legible copy, which discernibly shows the applicant's face, of at least one currently valid government issued photo ID (passport, driver's license, military ID, national ID or equivalent document type).

The named individual's address is verified using a government issued photo ID described above, a QIIS or a QGIS. DigiCert may also physically mail an access code to an address provided by the certificate requester.

For Code Signing, the request is verified as authentic by having the requestor submit a photo of themselves holding their government issued photo ID, performing secure face to face video communication where the requestor presents their ID or obtain an executed Declaration of Identity of the requester that includes at least one unique biometric identifier.

For EV, face to face verification of a principal individual of a Business Entity is carried out via attestation before a Third Party Validator such as a Notary, Latin Notary, Attorney or Accountant, or via video with a DigiCert representative.

For Document Signing, the applicant is verified by appearing before a Third Party Validator (See section 3.2.7 Third-Party Validators) or a DigiCert representative. Other processes providing equivalent assurance of positive identification may be used.

3.2.4. Non-Verified Subscriber Information

Contents of the certificate are verified in accordance with the Applicable Requirements.

3.2.5. Validation of Authority

When an organization is named in a certificate, the authority of the requester is verified using a Reliable Method of Communication. A Reliable Method of Communication is any source of communication that originates from an entity other than the applicant representative.

For EV, an Acceptable Method of Communication is a telephone number, fax number, email address or postal delivery address verified for the Applicant, their parent, subsidiary, or affiliate. The address MUST be verified using a QGIS, QTIS, QIIS or Legal Opinion Letter.

The Acceptable Method of Communication will be used to reach a representative of the applicant and confirm the name, title, agency and authority of Contract Signer and Certificate Approver as described in the EV Guidelines.

In all EV certificates, DigiCert may rely on other methods described in the EV Guidelines to complete this step such as the Legal Opinion Letter, a corporate resolution, or the Contract Signer and/or the Certificate Approver listed in a QIIS/QGIS as a corporate officer, sole proprietor, or other senior official of the applicant.

3.2.6. Criteria for Interoperation

Interoperation with DigiCert PKI is permitted pursuant to the CP. All cross certified Subordinate CA certificates that identify DigiCert as the subject are disclosed in the applicable repository.

3.2.7. Third-Party Validators

Certain documents or steps requested as part of the validation process, such as Legal Opinion Letters, attestation letters or face to-face validation must be performed before a third-party validator such as a notary (or equivalent in the Applicant's jurisdiction), lawyer or accountant.

Prior to relying on any of these documents, these parties are verified as active with the relevant licensing authority in the applicant's jurisdiction.

Contact information is verified through the licensing authority, a QGIS or QIIS to verify the authenticity of the document in a similar manner to what is described in Section 3.2.5.

3.2.8. Validation of Domain Control

For TLS, all domains listed in the certificate are verified using one of the following methods. For S/MIME, DigiCert either verifies the domain component of each email address listed in the certificate using one of the following methods or verifies control of the email address using a challenge/response process.

3.2.8.1. Email, Fax, SMS, or Postal Mail to the Domain Contact

Confirm the applicant's control over the FQDN by sending a unique Random Value (valid for no more than 30 days from its creation) through email, fax, SMS, or postal mail, to the Domain Contact and receiving confirmation by their use of the Random Value, performed in accordance with TLS BR Section 3.2.2.4.2;

3.2.8.2 Constructed Email to Domain Contact

Confirm the applicant's control over the FQDN by sending an email created by using 'admin', 'administrator', 'webmaster', 'hostmaster' or 'postmaster' as the local part followed by the ("@") sign, followed by an Authorization Domain name, including a Random Value in the email, and receiving a response using the Random Value, performed in accordance with TLS BR Section 3.2.2.4.4;

3.2.8.3. Domain Name Service (DNS) Change

Confirm the applicant's control over the FQDN by confirming the presence of a Random Value or Request Token in a DNS CNAME, TXT, or CAA record for either an Authorization Domain Name or an Authorization Domain Name prefixed with a label that begins with an underscore character, performed in accordance TLS BR Section 3.2.2.4.7;

3.2.8.4. IP Address

Confirm the applicant's control over the FQDN by confirming the Applicant's control over the FQDN through control of an IP address returned from a DNS lookup for A or AAAA records for the FQDN, performed in accordance with TLS BR Sections 3.2.2.5 and 3.2.2.4.8;

3.2.8.5. Email to DNS CAA Contact

Confirm the applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value will be sent to a DNS CAA Email Contact. The relevant CAA Resource Record Set is found using the search algorithm defined in RFC 8659 performed in accordance with TLS BR Section 3.2.2.4.13;

3.2.8.6. Email to DNS TXT Contact

Confirm the applicant's control over the FQDN by sending a Random Value via email to the DNS TXT Record Email Contact for the Authorization Domain Name for the FQDN and then receiving a confirming response utilizing the Random Value, performed in accordance with TLS BR Section 3.2.2.4.14;

3.2.8.7. Phone Contact with Domain Contact

Confirm the applicant's control over the FQDN by calling the Domain Contact's phone number and obtaining a confirming response to validate the authorized Domain Name. Each phone call can confirm control of multiple authorized Domain Names provided that the same Domain Contact phone number is listed for each authorized Domain Name being verified and they provide a confirming response for each authorized Domain Name, performed in accordance with TLS BR Section 3.2.2.4.15;

3.2.8.8. Phone Contact with DNS TXT Record Phone Contact

Confirm the applicant's control over the FQDN by calling the DNS TXT Record Phone Contact's phone number and obtaining a confirming response to validate the authorized Domain Name. Each phone call can confirm control of multiple authorized Domain Names provided that the same DNS TXT Record Phone Contact phone number is listed for each authorized Domain Name being verified and they provide a confirming response for each authorized Domain Name, performed in accordance with TLS BR Section 3.2.2.4.16;

3.2.8.9. Phone Contact with DNS CAA Phone Contact

Confirm the applicant's control over the FQDN by calling the DNS CAA Phone Contact's phone number and obtain a confirming response to validate the ADN. Each phone call can confirm control of multiple ADNs provided that the same DNS CAA Phone Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN, performed in accordance with TLS BR Section 3.2.2.4.17;

3.2.8.10. Agreed-Upon Change to Website v2

Confirm the applicant's control over the FQDN by verifying that the Request Token or Random Value is contained in the contents of a file (such as a Request Token, Random Value that does not appear in the request used to retrieve the file and receipt of a successful HTTP 2xx status code response from the request) located on the Authorized Domain name, located under the "/.well-known/pki-validation" directory, retrieved via either the "http" or "https" scheme and is accessed over an Authorized Port; performed in accordance with TLS BR Section 3.2.2.4.18; and

3.2.8.11. Agreed-Upon Change to Website - ACME

Confirm the Applicant's control over a FQDN by validating domain control of the FQDN using the ACME HTTP Challenge method defined in Section 8.3 of RFC 8555, performed in accordance with TLS BR Section 3.2.2.4.19 and Section 8.3 of RFC 8555 as prescribed.

3.2.9. Validation of IP Addresses

For each IP Address listed in a TLS Certificate, DigiCert confirms that, as of the date the certificate was issued, the applicant controlled the IP Address by:

3.2.9.1 Agreed-Upon Change to Website

Having the applicant demonstrate practical control over the IP Address by confirming the presence of a Request Token or Random Value contained in the content of a file or webpage in the form of a meta tag under the "/.well- known/pki-validation" directory on the IP Address, performed in accordance with TLS BR Section 3.2.2.5.1;

3.2.9.2 Email, Fax, SMS, or Postal Mail to IP Address Contact

Confirming the applicant's control over the IP Address by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value, performed in accordance with TLS BR Section 3.2.2.5.2;

3.2.9.3 Reverse Address Lookup

Performing a reverse-IP address lookup and then verifying control over the resulting Domain Name, as set forth above and in accordance with TLS BR Section 3.2.2.5.3;

3.2.9.4 Phone Contact with IP Address Contact

Confirming the applicant's control over the IP Address by calling the IP Address Contact's phone number, as identified by the IP Address Registration Authority, and obtaining a response confirming the applicant's request for validation of the IP Address, performed in accordance with TLS BR Section 3.2.2.5.5;

3.2.9.5 ACME "http-01" method for IP Addresses

Confirming the applicant's control over the IP Address by performing the procedure documented for an "http-01" challenge in draft 04 of "ACME IP Identifier Validation Extension," available at ACME IP Identifier Validation Extension performed in accordance with TLS BR Section 3.2.2.5.6.

3.2.10. Validation of Wildcard Domains

If the FQDN portion of any Wildcard Domain Name in the Certificate is "registry-controlled" or is a "public suffix" (e.g. "**.com", "**.co.uk", see RFC 6454 Section 8.2 for further explanation), DigiCert applies additional scrutiny and checks to ensure the applicant has rightful control over the entire Domain Namespace.

3.2.11. Email Challenge-Response Procedure

If the domain component of an email address is not verified, DigiCert verifies the requester's control over the email address.

Control of an email address included in a Certificate may be verified by sending a random value via email and then receiving a confirming response utilizing the random value. The random value is valid for no more than 24 hours and is reset whenever the email is resent.

3.2.12. Data Source Accuracy

For EV, data sources are evaluated 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.

3.3. Identification and Authentication for Re-Key Requests

3.3.1. Identification and Authentication for Routine Re-key

The same procedures as described in Section 3.2 are required for a re-key request.

3.3.2. Identification and Authentication for Re-key After Revocation

The same procedures as described in Section 3.2 are required for a re-key request.

3.4. Identification and Authentication For Revocation Request

The procedure for identification and authentication of a revocation request is described throughout Section 4.9.

4. Certificate Lifecycle Operational Requirements

4.1. Certificate Application

4.1.1. Who Can Submit a Certificate Application

Applicants are responsible for any data supplied to the Issuer CA.

EV certificate requests must be submitted by an authorized Certificate Requester and approved by a Certificate Approver. A Certificate Requestor is a natural person who is either the Applicant, employed by the Applicant or an authorized agent of the Applicant.

DigiCert does not issue certificates to entities on a government denied list maintained by the United States, or which are in a country with which the laws of the United States prohibit doing business.

Issuer CAs may describe additional requirements within their CPS.

4.1.2. Enrollment Process and Responsibilities

Prior to the issuance of a certificate, Issuer CAs obtain a certificate request, and executed Subscriber Agreement, Terms of Use and/or Master Services Agreement, in accordance with the relevant CA/B Forum requirements.

In no particular order the enrollment process may include:

- Submitting a certificate application;
- Generating a key pair;
- Delivering the public key of the key pair to DigiCert;
- Agreeing to the applicable Subscriber Agreement, Terms of Use and/or Master Services Agreement; and
- Paying any applicable fees.

Issuer CAs may outline additional requirements in their CPS.

4.2. Certificate Application Processing

4.2.1. Performing Identification and Authentication Functions

After receiving a certificate application, the RA authenticates Subject information using the procedures described in Section 3.2.

4.2.1.1. CAA Checking

Prior to issuing a TLS certificate, Issuer CAs check the DNS for the existence of a CAA record for each DNSName in the subjectAltName extension of the certificate to be issued. DigiCert processes the “issue” and “issuewild” property tags.

Prior to issuing an S/MIME certificate on or after March 15, 2025, Issuer CAs check the DNS for the existence of a CAA record in accordance with RFC 9495 for each Mailbox Address in the subjectAltName extension of the S/MIME certificate to be issued. DigiCert processes the “issuemail” property tag.

Certificates passing the CAA check are issued within the Time to Live (TTL) of the CAA record, or 8 hours, whichever is greater. DigiCert logs actions taken based on CAA records, and documents issuance prevented by CAA for feedback to the CA/B Forum. DigiCert may not dispatch reports of issuance requests to the

contact(s) listed in an "iodef" property tag. CAA checking is optional for certificates issued by a Technically Constrained Subordinate CA Certificate.

DigiCert may treat a record lookup failure as permission to issue if:

- The failure is outside the DigiCert's infrastructure; and
- The lookup has been retried at least once; and
- The domain's zone does not have a DNSSEC validation chain to the ICANN root.

The CA identifiers that DigiCert recognizes are:

- www.digicert.com
- digicert.com
- digicert.ne.jp
- cybertrust.ne.jp
- thawte.com
- geotrust.com
- rapidssl.com
- symantec.com
- volusion.digitalcertvalidation.com
- stratossl.digitalcertvalidation.com
- intermediatecertificate.digitalcertvalidation.com
- 1and1.digitalcertvalidation.com
- amazon.com
- amazontrust.com
- awstrust.com
- amazonaws.com
- digitalcertvalidation.com
- quovadisglobal.com
- pkioverheid.nl

4.2.1.2. EV TLS and Code Signing

Once verification is complete, the Issuer CA evaluates the corpus of information and decides whether or not to issue the certificate.

4.2.1.3. S/MIME

Validation of mailbox control according to Section 3.2.8 must be completed within 30 days of certificate issuance. Validation of mailbox authorization or control in accordance with Section 3.2.2.3 must be

completed within 398 days of certificate issuance. Authentication of organizational entity or Individual Identity must be completed within 825 days prior to certificate issuance.

4.2.2. Approval or Rejection of Certificate Applications

Issuer CAs can reject certificate applications for any reason. Issuer CAs must reject any certificate application that does not comply with the Applicable Requirements, including certificate applications that include internal names, reserved IP addresses or gTLD's under consideration. DigiCert may reject a certificate application if it believes issuance could damage DigiCert's business or reputation.

4.2.2.1. EV TLS and Code Signing

Unless issued by an Enterprise RA, EV certificates are validated and approved by two separate validation specialists. The second validation specialist cannot be the same individual who collected the documentation and validated the information contained in EV certificate. The second validation specialist reviews the collected information and determines if it is in order and ready for issuance. If any discrepancies are found, the application is sent back for additional information and documentation. If satisfactory explanations and/or additional documents are not received within a reasonable time, DigiCert, rejects the certificate application.

Enterprise RAs may perform the final cross-correlation and due diligence described herein using a single person representing the Enterprise RA.

4.2.3. Time to Process Certificate Applications

DigiCert uses reasonable efforts to process certificate applications. Other than as specified in the relevant Subscriber Agreement/Master Services Agreement, DigiCert does not stipulate when the validation process will complete.

DigiCert may reject an application if the applicant is unable to provide all required documentation within a reasonable timeframe.

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/CPS in a secure manner.

TLS certificates are logged in two or more Certificate Transparency databases.

DigiCert requires that two individuals in trusted roles (i.e. the CA system operator, system officer, or PKI administrator) act to issue certificates signed by a Root CA. One of these individuals must deliberately command the Root CA to perform a certificate signing operation.

TLS certificates issued on or after March 15, 2025 must follow a Linting process. Other certificate types may also follow a Linting process, at DigiCert's discretion.

4.3.2. Notifications to Subscriber by the CA of Issuance of Certificate

Certificates are delivered in a secure manner after issuance. Generally, DigiCert delivers certificates using the email address designated by the subscriber during enrolment.

4.4. Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

Certificates are considered accepted if not revoked by the subscriber within 30 days of issuance.

4.4.2. Publication of the Certificate by the CA

CA Certificates are published in the Issuer CA's repository. End-entity certificates are published by delivering them to the subscriber.

4.4.3. Notification of Certificate Issuance by the CA to Other Entities

RAs, partners, and other entities involved in the enrollment process may be informed of issuance. The public receives notice of certificates intended for the WebPKI via publication to a CT log.

4.5. Key Pair and Certificate Usage

4.5.1. Subscriber Private Key and Certificate Usage

Subscribers must use issued certificates in accordance with applicable laws, the relevant Subscriber Agreement, and requirements in this CP/CPS. Subscribers are required to protect their Private Keys from unauthorized use or disclosure, discontinue using a Private Key after expiration or revocation of the associated certificate, and use certificates in accordance with their intended purpose.

4.5.2. Relying Party Public Key and Certificate Usage

Relying Parties must adhere to the Relying Party agreement available in DigiCert's legal repository.

4.6. Certificate Renewal

4.6.1. Circumstance for Certificate Renewal

DigiCert allows subscribers to renew Certificates through its automation tools, GUIs, and API. DigiCert uses reasonable efforts to notify Subscribers of Certificate expiration dates using the contact details provided by the subscriber.

4.6.2. Who May Request Renewal

See Section 4.1.1.

4.6.3. Processing Certificate Renewal Requests

Renewals are processed the same way as new certificates as described in Sections 4.1.2 and 4.2.

4.6.4. Notification of New Certificate Issuance to Subscriber

See Section 4.3.2.

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

See Section 4.4.1.

4.6.6. Publication of the Renewal Certificate by the CA

See Section 4.4.2.

4.6.7. Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

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

DigiCert's subscribers may request a rekey through its online portals, automation solutions, and APIs. Subscribers may request a re-key for any reason, including when a key is compromised.

4.7.2. Who May Request Certification of a New Public Key

See Section 4.1.1.

4.7.3. Processing Certificate Re-Keying Requests

See Section 4.1.2.

4.7.4. Notification of New Certificate Issuance to Subscriber

See Section 4.3.2.

4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate

See Section 4.4.1.

4.7.6. Publication of the Re-Keyed Certificate by the CA

See Section 4.4.2.

4.7.7. Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3

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 is validated as described in Section 4.2.1.

4.8.2. Who May Request Certificate Modification

See Section 4.1.1.

4.8.3. Processing Certificate Modification Requests

See Section 4.2.

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

Certificate revocation ends the operational period of the certificate prior to the certificate's expiration date. DigiCert may revoke for any reason, including if DigiCert believes that any one of the reasons in this section occurred.

4.9.1. Circumstances for Revocation

4.9.1.1. Circumstances for revocation within 24 hours

Issuer CAs will 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 FDQN or IP address or mailbox control for any email address in the certificate should not be relied upon (CRLReason #4, superseded).
6. The Issuer CA has reasonable assurance that a code signing certificate was used to sign suspect code.

4.9.1.2. Circumstances for revocation within 5 days

The Issuer CA may revoke a certificate within 24 hours and will revoke a certificate within 5 days after receipt and confirming that one or more of the following occurred:

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 the DigiCert Public Trust CP/CPS, 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. For code signing, the Application Software Supplier requests revocation and the Issuer CA does not intend to pursue an alternative course of action;
6. The Issuer CA confirms that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate FQDN (CRLReason #9, privilegeWithdrawn);
7. The Issuer CA confirms a material change in the information contained in the certificate (CRLReason #9, privilegeWithdrawn);
8. The Issuer CA confirms that the certificate was not issued in accordance with the CAB/Forum requirements or relevant browser policy (CRLReason #9, privilegeWithdrawn);
9. The Issuer CA determines or confirms that any of the information appearing in the certificate is inaccurate (CRLReason #9, privilegeWithdrawn);
10. 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);
11. Revocation is required by the DigiCert Public Trust CP/CPS and/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
12. 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).
13. The certificate no longer complies with the requirements of Section 6.1.5 and Section 6.1.6 of the Code Signing Baseline Requirements.

For Code Signing Certificates, Application Software Suppliers may request the Issuer CA delays revocation where immediate revocation has a potentially large negative impact to the ecosystem.

4.9.1.3. Other Revocation Considerations

The Issuer CA may revoke any certificate in its sole discretion, including if the Issuer CA believes that:

1. Either the subscriber's or the Issuer CA's obligations under the DigiCert Public Trust CP/CPS or the applicable CPS are delayed or prevented by circumstances beyond the party's reasonable control, including computer or communication failure, and, as a result, another entity's information is materially threatened or compromised;
2. The Issuer CA received a lawful and binding order from a government or regulatory body to revoke the certificate;
3. The Issuer CA ceased operations and did not arrange for another Certificate Authority to provide revocation support for the certificates;
4. The technical content or format of the certificate presents an unacceptable risk to Application Software Suppliers, Relying Parties, or others;
5. The subscriber was added as a denied party or prohibited person to a blocklist or is operating from a destination prohibited under the laws of the United States;
6. For Document Signing Certificates, Adobe has requested revocation; or

7. For Code Signing Certificates, the certificate was used to sign, publish, or distribute malware, code that is downloaded without user consent, or other harmful content.

4.9.1.4. Revocation of subordinate CA certificates

The Issuer CA will revoke a Subordinate CA Certificate 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 applicable 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 the DigiCert Public Trust CP/CPS 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 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 the DigiCert Public Trust CP/CPS 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. All Issuer CAs 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. Issuer CAs must publicly disclose the instructions on its website.

DigiCert allows for certificates to reported for the aforementioned reasons via the certificate reporting tool: https://problemreport.digicert.com/ Other contact methods are specified in Section 1.5.2.1.

4.9.3. Procedure for Revocation Request

Issuer CAs provide a process for subscribers to request revocation of their own certificates and describe this in their CPS.

DigiCert processes a revocation request as follows:

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

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

DigiCert maintains a continuous 24/7 ability to internally respond to any high priority revocation requests and certificate problem reports on the following website: https://problemreport.digicert.com/ and other resources as indicated in Section 1.5.2.1 of this CP/CPS.

4.9.4. Revocation Request Grace Period

Certificates revoked through a subscriber's account are processed immediately. DigiCert processes all other revocation requests within 24 hours of receipt of the request. Actual revocation timelines depends on the reasons for revocation as described in this section.

4.9.5. Time within which CA Must Process the Revocation Request

DigiCert investigates all Certificate Problem Reports and provides a preliminary report on its findings within 24 hours. The period from receipt of when DigiCert determines revocation is required and when a certificate is revoked will match the time frame set forth in Section 4.9.1.1. while also considering:

1. The nature of the alleged problem (scope, context, severity, magnitude, risk of harm);

2. The consequences of revocation (direct and collateral impacts to subscribers and Relying Parties);
3. The number of Certificate Problem Reports received about a particular certificate or subscriber;
4. The entity making the complaint (for example, a complaint from a law enforcement official that a web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that they didn't receive the goods they ordered); and
5. Relevant legislation.

Under normal operating circumstances, DigiCert will revoke certificates as quickly as practical after validating the revocation request following the guidelines of this section and Section 4.9.1.

DigiCert follows the revocation timeframes specified for malware in the Baseline Requirements for Issuance and Management of Publicly Trusted Code Signing Certificates in Section 4.9.5.

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

Subscriber certificates

Updated CRLs are issued at least once every seven days, and the value of the nextUpdate field is not more than ten days beyond the value of the thisUpdate field. A new CRL is published within 24 hours of revoking a certificate.

Subordinate CA and Timestamp

DigiCert updates and reissues CRLs at least once every twelve months and within 24 hours after revoking a Subordinate CA Certificate, and the value of the nextUpdate field is not more than twelve months beyond the value of the thisUpdate field.

Other certificates issued pursuant to this CP/CPS

DigiCert uses its offline root CAs to publish CRLs for its intermediate CAs at least every 6 months. All other CRLs are published at least every seven days.

4.9.8 Maximum Latency for CRLs

No stipulation.

4.9.9. On-line Revocation/Status Checking Availability

OCSP responses must conform to RFC 6960 and/or RFC 5019. OCSP responses must either:

1. Be signed by the CA that issued the certificates whose revocation status is being checked, or
2. Be signed by an OCSP Responder whose certificate is signed by the CA that issued the certificate whose revocation status is being checked.

In the latter case, the OCSP signing certificate must contain an extension of type id-pkix-ocsp- nocheck, as defined by RFC 6960.

4.9.10. On-line Revocation Checking Requirements

OCSP is supported using the GET method.

Subscriber Certificates

1. OCSP responses have a validity interval greater than or equal to eight hours;
2. OCSP responses have a validity interval less than or equal to ten days;
3. For OCSP responses with validity intervals less than sixteen hours, then DigiCert updates the information provided via an Online Certificate Status Protocol prior to one-half of the validity period before the nextUpdate; and
4. For OCSP responses with validity intervals greater than or equal to sixteen hours, then DigiCert updates the information provided via an Online Certificate Status Protocol at least eight hours prior to the nextUpdate, and no later than four days after the thisUpdate.

Code Signing Certificates

1. OCSP responses are updated at least every four days with a maximum validity of ten days.
2. OSCP responses for code signing and timestamp certificates may be available for up to 10 years after the expiration of the certificate.

Subordinate CA, Intermediate CA and Timestamp Certificates

OCSP information for Intermediates CAs are updated:

1. At least every twelve months;
2. Within 24 hours after revoking the Certificate.

A certificate serial number within an OCSP request is one of the following three options:

1. "assigned" if a certificate with that serial number has been issued by the Issuing CA, using any current or previous key associated with that CA subject; or
2. "reserved" if a Precertificate [RFC6962] with that serial number has been issued by (a) the Issuing CA; or (b) a Precertificate Signing Certificate [RFC6962] associated with the Issuing CA; or
3. "unused" if neither of the previous conditions are met. For "unused" serial numbers, the OCSP responder will not provide a "good" response.

4.9.11. Other Forms of Revocation Advertisements Available

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

1. The alternative method is described in its CPS,
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

DigiCert uses commercially reasonable efforts to notify impacted parties when a Private Key is compromised. Previously revoked certificates are updated with the reasonCode of "key compromise" if a key is discovered as compromised after certificate revocation. Issuer CAs are required to revoke all certificates with a compromised key within 24 hours after receiving proof of the key compromise.

key compromise reports must include:

1. Proof of key compromise in either of the following formats:
    - A CSR signed by the compromised private key with the Common Name "Proof of Key Compromise for DigiCert"; or
    - The private key itself.
2. If a CSR is provided, the Issuer CA will only accept proof of key compromise, if one of the following algorithms are used to sign the CSR:
    - SHA256WithRSA
    - SHA384WithRSA
    - SHA512WithRSA
    - ECDSAWithSHA256
    - ECDSAWithSHA384
    - ECDSAWithSHA512
    - SHA256WithRSAPSS
    - SHA384WithRSAPSS
    - SHA512WithRSAPSS
    - PureEd25519
3. A valid email address that is monitored for follow-up questions and investigations related to the key compromise report.

4.9.13. Circumstances for Suspension

Suspension is not available for publicly trusted certificates.

4.9.14. Who Can Request Suspension

Suspension is not available for publicly trusted certificates.

4.9.15. Procedure for Suspension Request

Suspension is not available for publicly trusted certificates.

4.9.16 Limits on Suspension Period

Suspension is not available for publicly trusted certificates.

4.10. CERTIFICATE STATUS SERVICES

4.10.1. Operational Characteristics

Certificate validity information is available via either CRL and/or an OCSP responder for TLS, SMIME, and Code Signing certificates. Revocation entries are removed from a CRL or OCSP after the certificate expires or in the case of Code Signing, 10 years after it has expired.

4.10.2. Service Availability

DigiCert operates its CRL and OCSP services in a manner that provides response times of ten seconds or less under normal operating conditions.

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

Subscribers may end their subscription to certificate services by revoking all issued certificates or by allowing their certificates or applicable Subscriber Agreement to expire without renewal. Some terms of the Subscriber Agreement and this CP/CPS may survive termination of the subscription service.

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.

Issuer CAs may escrow subscriber key management keys to provide key recovery services provided:

1. The Issuer CA encrypts all Private Keys,
2. The Issuer CA stores escrowed Private Keys with at least the level of security used to generate and deliver the Private Key, and
3. The Issuer CA protects Private Keys from unauthorized disclosure.

Enterprise customers utilizing key escrow services provided by DigiCert may escrow keys within their infrastructure. Enterprise customers must notify subscribers when keys are escrowed.

Subscribers and other authorized entities may request recovery of an escrowed (decryption) Private Key. Keys are recovered at the request of the subscriber, contracting entity, or as required by law. Entities escrowing Private Keys must have controls in place that prevent unauthorized access to Private Keys.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

Issuer CAs that support session key encapsulation and recovery shall describe their practices in their CPS.

5. Facility, Management, and Operational Controls

5.1. Physical Controls

5.1.1. Site Location and Construction

DigiCert performs its CA and TSA operations from secure data centers.

Certificate management systems are housed in secure facilities that are protected by multiple tiers of physical security, video monitoring, and dual access.

5.1.2. Physical Access

Data centers are equipped with logical and physical controls that make DigiCert's CA and TSA operations inaccessible to non-trusted personnel. DigiCert operates under a security policy designed to detect, deter, and prevent unauthorized access to DigiCert's operations.

Access to the date centers are continuously monitored.

5.1.3. Power and Air Conditioning

Data centers have primary and secondary power supplies that ensure continuous and uninterrupted access to electric power. Uninterrupted power supplies (UPS) and generators provide redundant backup power.

5.1.4. Water Exposures

Reasonable precautions are taken to minimize the impact of water exposure to CA systems.

5.1.5. Fire Prevention and Protection

Data centers are equipped with fire suppression mechanisms.

5.1.6. Media Storage

Media is protected from accidental damage, environmental hazards, and unauthorized physical access.

5.1.7. Waste Disposal

All unnecessary copies of printed sensitive information are shredded on-site before disposal. Sensitive data on magnetic or other digital media are permanently erased before disposal.

5.1.8. Off-site Backup

DigiCert performs weekly system backups that are used to recover from system failure. Backups, including one full backup, are stored in offsite locations that have procedural and physical controls that are commensurate with its operational location.

5.2. PROCEDURAL CONTROLS

5.2.1. Trusted Roles

Functions and duties performed by persons in trusted roles are distributed so that one person alone cannot circumvent security measures or subvert the security and trustworthiness of the PKI or TSA operations.

The following six trusted roles are defined by this CP/CPS, although Issuer CAs may define additional roles:

5.2.1.1. CA Administrators

CA Administrators install and configure the CA software, including key generation, key backup, and key management. CA Administrators perform and securely store regular CA system backups. Administrators do not issue certificates to subscribers.

5.2.1.2. Registration Officers – Validation and Vetting Personnel

Registration Officers collect and validate data included in certificates. Registration Officers approve and revoke certificates.

5.2.1.3. System Administrators / System Engineers (Operator)

Operators install and configure system hardware, including servers, routers, firewalls, and network configurations. Operators also keep critical systems updated with software patches and perform other maintenance as needed.

5.2.1.4. Internal Auditors

Internal Auditors review, maintain, and archive audit logs and oversee compliance audits to determine if the CA is operating in accordance with this CP/CPS and other applicable documents.

5.2.1.5. RA Administrators

RA Administrators manage and use RA software.

5.2.1.6. Security Officers

Security Officers administer and implement security practices.

5.2.2. Number of Persons Required per Task

Policy and control procedures are used to segment job responsibilities. DigiCert requires that at least two people acting in a trusted role 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.

An Internal Auditor may participate as a trusted role in granting physical access to the CA system but cannot fulfill the requirement of multiparty control for logical access.

5.2.3. Identification and Authentication for each Role

DigiCert personnel authenticate themselves to the certificate management system before they are allowed access to the systems necessary to perform their trusted roles.

5.2.4. Roles Requiring Separation of Duties

Individuals are specifically designated to the roles defined in Section 5.2.1. Individuals designated as Registration Officer or Administrator may also assume the Operator role. An Internal Auditor may not assume any other role.

DigiCert enforces separation of duties using physical, logical, or procedural controls. The CA and RA software and hardware identifies and authenticates users and ensures that an identity cannot assume multiple identities at the same time.

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 the Certificate Management Process, regardless of whether the person is as an employee, agent, or an independent contractor.

Managerial personnel involved in time-stamping operations must possess experience with information security and risk assessment, security procedures, knowledge of time-stamping technology, digital signature technology, and mechanisms for calibration of time stamping clocks with UTC.

5.3.2. Background Check Procedures

Background checks and identity verification are completed before appointing an individual to trusted role. Identity verification requires a government-issued photo (e.g., passports and/or driver's licenses reviewed pursuant to U.S. Citizenship and Immigration Services Form I-9, Employment Eligibility Verification, or comparable procedure for the jurisdiction in which the individual's identity is being verified).

Background checks may include the following:

- Checks for criminal activity over the last five years,
- Checks of previous residences are over the past three years, and
- Verification of the highest education degree obtained.

All background checks are restricted to the applicable legal limits allowed. If a check cannot be completed, the CA may substitute another investigative technique permitted by law that provides substantially similar information.

5.3.3. Training Requirements

DigiCert provides skills training for trusted roles. This training may include:

1. Basic Public Key Infrastructure (PKI) knowledge;
2. Software versions used by the CA;
3. Authentication and verification policies and procedures, including this document;
4. Security principles and mechanisms;
5. Disaster recovery and business continuity procedures;
6. Common threats to the validation process, including phishing and other social engineering tactics; and
7. The Applicable Requirements.

The CA must maintain a record of trainings. Registration Officers must have the minimum skills required to perform the validation process and must demonstrate those skills by passing an exam on the EV Guidelines, TLS Baseline Requirements and the S/MIME Baseline Requirements before validating and approving the issuance of the corresponding certificates.

5.3.4. Retraining Frequency and Requirements

Personnel must maintain their skill levels in order to continue acting in trusted roles. When operations change, DigiCert provides documented training to impacted trusted roles.

5.3.5. Job Rotation Frequency and Sequence

No stipulation.

5.3.6. Sanctions for Unauthorized Actions

Employees and agents failing to comply with this CP/CPS are subject to administrative or disciplinary actions. This may include termination of contract, termination of employment and civil and/or criminal sanctions.

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

Documentation is provided to trusted roles as needed to perform their their duties.

5.4. AUDIT LOGGING PROCEDURES

5.4.1. Types of Events Recorded

CA systems require identification and authentication at system logon. Important system actions are logged to ensure the accountability of the operators who initiate such actions.

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. A message from any source requesting action related to the operational state of the CA is an auditable event. If the system owner's applications cannot automatically record an event, the system owner implements manual procedures to satisfy these requirements. For each event, the system owner records the:

1. Date and time;
2. Type of event;
3. Success or failure; and
4. User or system that caused the event or initiated the action.

The system owner must make all event records available to its auditors as proof of the its practices. Logs are maintained as per the requirements of the relevant policies and programs.

System owners must record at least the following events:

1. CA Certificate and key lifecycle events, including:
    - Key generation, backup, storage, recovery, archival, and destruction;
    - Certificate requests, renewal, and re-key requests, and revocation;
    - Approval and rejection of certificate requests and
    - Cryptographic device lifecycle management events.
    - Generation of Certificate Revocation Lists
    - Signing of OCSP responses (as described in Sections 4.9 and 4.10); and
    - Introduction of new Certificate Profiles and retirement of existing Certificate Profiles
2. CA and Subscriber Certificate lifecycle management events, including:
    - Certificate requests, renewal, and re-key requests, and revocation;
    - All verification activities stipulated in the CA/Browser Forum Requirements, the DigiCert Public Trust CP/CPS and the Issuer CA's CPS;

- Approval and rejection of certificate requests;
- Issuance of certificates;
- Generation of Certificate Revocation Lists
- Signing of OCSP Responses (as described in Sections 4.9 and 4.10)

3. Security events, including:
   - Successful and unsuccessful PKI system access attempts;
   - PKI and security system actions performed;
   - Security profile changes;
   - Installation, update and removal of software on a certificate System;
   - System crashes, hardware failures, and other anomalies;
   - Relevant firewall and router activities; and
   - Entries to and exits from the CA facility.
4. Log entries must include at least the following elements:
   - Date and time of event;
   - Identity of the person making the journal record (when applicable); and
   - Description of the event.

5.4.1.1 Router and Firewall Activities Logs

Logging of router and firewall activities necessary to meet the requirements of Section 5.4.1, must at a minimum include:

1. Successful and unsuccessful login attempts to routers and firewalls; and
2. Logging of all administrative actions performed on routers and firewalls, including configuration changes, firmware updates, and access control modifications; and
3. Logging of all changes made to firewall rules, including additions, modifications, and deletions; and
4. Logging of all system events and errors, including hardware failures, software crashes, and system restarts.

5.4.2. Frequency of Processing Log

DigiCert periodically performs system and file integrity checks and runs vulnerability assessments. Integrity checks verify that logs were not tampered with. DigiCert examines any statistically significant set of security audit data generated since the last review and searches for evidence of malicious activity. Any anomalies or irregularities found are investigated. Any actions taken are documented. DigiCert makes a summary of the review available to its auditors upon request.

5.4.3. Retention Period for Audit Log

The CA retains audit logs on-site until after the log is reviewed. Logs are retained for at least two (2) years, in accordance with Sections 5.5.2 and 4.10.1, or as otherwise specified herein or in the log documentation. DigiCert makes all audit logs available to auditors upon request. Retained records include:

1. CA certificate and key lifecycle management event records as set forth in Section 5.4.1 (1) of the TLS Baseline Requirements, which includes:
    - Destruction of the CA Private Key; or
    - Revocation or expiration of the final CA Certificate;
2. Subscriber certificate lifecycle management as set forth in Section 5.4.1 (2) of the TLS Baseline Requirements;
3. Security event records as set forth in Section 5.4.1 (3) of the TLS Baseline Requirements.

5.4.4. Protection of Audit Log

Audit logs are protected from destruction prior to the end of the audit log retention period and are retained securely on-site until transferred to a backup site.

Both current and archived logs are maintained in a form that prevents unauthorized modification, substitution or destruction.

5.4.5. Audit Log Backup Procedures

Audit logs are backed up periodically.

5.4.6. Audit Collection System (internal vs. external)

Audit processes are often automated. Automated logs areinvoked at system startup and end only at system shutdown.

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 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/CPS.

5.5.1. Types of Records Archived

In addition to the logs described in Section 5.4.1, the following records are 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

All records described in Section 5.5.1 are retained for at least two (2) years.

5.5.3. Protection of Archive

All archived records are stored at a secure location in a way that prevents unauthorized modification, substitution, or destruction.

5.5.4. Archive Backup Procedures

Archives are regularly backed up and copies are maintained at separate locations.

5.5.5. Requirements for Time-stamping of Records

Archive records are time-stamped as they are created.

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

DigiCert and any cross-signed partners must each 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 should include how the CA will notify and reasonably protect Application Software Suppliers, subscribers, and Relying Parties if a disaster, security compromise, or business failure occurs.

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

DigiCert makes regular back-up copies of its Private Keys and stores them in a secure separate location. All CAs are required to make regular system back-ups on at least a weekly basis.

If a disaster causes DigiCert's operations to become inoperative, then DigiCert will ensure the integrity of its systems and re-initiate its operations on replacement hardware using backup copies of its software, data, and Private Keys at a secure facility. DigiCert prioritizes reestablishing the generation of certificate status information. If the Private Keys are destroyed, DigiCert will reestablish operations as quickly as possible, giving priority to generating new Key Pairs.

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

DigiCert maintains a secure facility in at least one secondary, geographically diverse location to ensure that its directory and on-line status servers remain operational if a physical disaster impairs DigiCert's main site.

DigiCert will provide reasonable notice to interested parties if a disaster physically damages the CA equipment or destroys all copies of the a CA's signature keys.

5.8. CA OR RA TERMINATION

When a CA terminates operations, the CA may provide notice to interested parties and may transfer its responsibilities and records to successor entities. A successor may re-issue certificates if the successor has all relevant permissions to do so and has operations that are at least as secure as the transferring CA. Any requirements of this section that vary by contract apply only to the contracting parties and supersede this section.

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 FIPS 140-2 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. For requests submitted on or after November 15, 2024, at least 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].

For Document Signing Certificates, subscribers must generate their Key Pairs in a medium that prevents exportation or duplication and that meets or exceeds FIPS 140-2 Level 3 certification standards.

6.1.2. Private Key Delivery to Subscriber

If a key is generated by a CA system for a subscriber, then the CA must deliver the Private Key securely to the subscriber. The CA may deliver keys electronically (such as through secure email or stored in a cloud-based system) or on a hardware cryptographic module.

In all cases:

- Except where escrow/backup services are authorized and permitted, the key generator must not retain access to the subscriber's Private Key after delivery,
- The key generator must protect the Private Key from activation, compromise, or modification during the delivery process,
- The subscriber must acknowledge receipt of the Private Key(s), typically by having the Subscriber use the related certificate, and
- The key generator delivers the Private Key in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers securely.

If the Issuer CA or an Enterprise RA becomes aware that a subscriber's Private Key has been communicated to a person or organization not authorized by the subscriber, then the Issuer CA must revoke all certificates associated with that Private Key.

6.1.3. Public Key Delivery to Certificate Issuer

Subscribers should provide their Public Keys for signing in a secure fashion and in a manner that binds the subscriber's verified identity to the Public Key.

6.1.4. CA Public Key Delivery to Relying Parties

CA Public Keys are provided to Relying Parties as specified in a certificate validation or path discovery policy file, as trust anchors in commercial browsers and operating system root store, and/or as roots signed by other CAs.

DigiCert permits redistribution of their root anchors by application software providers and accreditation authorities. DigiCert may also distribute Public Keys that are part of an updated signature Key Pair as a self-signed certificate, as a new CA Certificate, or in a key roll-over certificate. Relying Parties may obtain DigiCert's self- signed CA Certificates from its web site or by email.

6.1.5. Key Sizes

As of January 1, 2021, the minimum key size for new CA Certificates which issue Code Signing and Time-stamping Certificates is 3072-bit RSA and ECC NIST P-384.

For RSA key pairs:

- The modulus size, when encoded, is at least 2048 bits, and
- The modulus size, in bits, is evenly divisible by 8.

For ECDSA key pairs:

- For roots and Sub CAs, the key represents a valid point on the NIST P-256, NIST P-384, NIST P-521 elliptic curve,
- For end-entity, the key represents a valid point on the NIST P-256 or NIST P-384 elliptic curve or
- For S/MIME end-entity only, the key represents a valid point on the curve25519 or curve 448 elliptic curve.

If the Key is DSA, then:

- Key length (L) of 2048 bits and modulus length (N) of 224 bits or
- Key length (L) of 2048 bits and modulus length (N) of 256 bits

6.1.6. Public Key Parameters Generation and Quality Checking

The value of the public exponent in an RSA key is an odd number equal to 3 or more and is between 2^16 + 1 and 2^256 - 1. The modulus is also be an odd number, not the power of a prime, and has no factors smaller than 752.

ECDSA public key validity is confirmed using either the ECC Full Public Key Validation Routine or the ECC Partial Public Key Validation Routine.

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

Private Keys corresponding to Root Certificates must not be used to sign certificates except in the following cases:

1. Self-signed Certificates to represent the Root CA itself;
2. Certificates for Subordinate CAs and Cross-Certified Subordinate CA Certificates;
3. Certificates for infrastructure purposes (administrative role certificates, internal CA operational device certificates); and
4. Certificates for OCSP Response verification.

The use of a specific key is determined by the key usage extension in the X.509 certificate.

6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1. Cryptographic Module Standards and Controls

CAs and systems that sign OCSP responses or CRLs use cryptographic hardware modules validated to FIPS 140-2 Level 3.

Cryptographic module requirements for subscribers and registration authorities are as follows:

Assurance Level	Subscriber	Registration Authority
EV Code Signing	FIPS 140-2 Level 2 or Common Criteria EAL 4+ (Hardware)	FIPS 140-2 Level 2 or Common Criteria EAL 4 (Hardware)
OV Code Signing	FIPS 140-2 Level 2 or Common Criteria EAL 4+ (Hardware)	FIPS 140-2 Level 2 or Common Criteria EAL 4+ (Hardware)
Adobe Signing	FIPS 140-2 Level 2 (Hardware)	FIPS 140-2 Level 3 (Hardware)

For OV or EV Code Signing Certificates, subscribers must protect all Private Keys in a Hardware Crypto Module conforming to at least FIPS 140-2 level 2 or Common Criteria EAL 4+. DigiCert verifies this key protection via:

1. Use of an HSM, verified by means of a manufacturer's certificate;
2. A cloud-based key generation and protection solution with the following requirements:
    - Key creation, storage, and usage of Private Key must remain within the security boundaries of the cloud solution's Hardware Crypto Module that conforms to the specified requirements;
    - Subscription at the level that manages the Private Key must be configured to log all access, operations, and configuration changes on the resources securing the Private Key.
    - A Hardware Crypto Module provided by the Issuing CA;
    - Contractual terms in the Subscriber Agreement requiring the subscriber to protect the Private Key to a standard of at least FIPS 140-2 level 2 or Common Criteria EAL 4+ and with compliance being confirmed by means of an audit.

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. CAs may escrow other key types as described in Section 4.12.1.

6.2.4. Private Key Backup

CA and certificate status Private Keys are backed up under multi-person control. DigiCert stores the backup in a secure location. DigiCert protects all copies of its CA, CRL, and certificate status Private Keys in the same manner as the originals.

6.2.5. Private Key Archival

DigiCert does not archive its 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.

If DigiCert becomes aware that a Subordinate CA's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subordinated CA, then DigiCert will mandate revocation of all certificates that include the Public Key corresponding to the communicated Private Key.

Issuer CAs pre-generating private keys and transferring them into a hardware token, for example transferring generated end-user subscriber private keys into a smart card, must 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

All CA Private Keys are stored on a cryptographic module which has been evaluated to at least FIPS 140-2 Level 3. Can and RA private keys held on hardware cryptographic modules are stored in encrypted form.

6.2.8. Method of Activating Private Key

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

Subscribers are solely responsible for protecting their Private Keys in a manner commensurate with the certificate type. At a minimum, Subscribers must authenticate themselves to the cryptographic module before activating their Private Keys. Entry of activation data shall be protected from disclosure.

Subscribers should also take commercially reasonable measures for the physical protection of their 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 and secured.

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.

Subscribers should deactivate their Private Keys via logout and removal procedures when not in use.

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. Subscribers shall destroy their Private Keys when the corresponding certificate is revoked or expired or if the Private Key is no longer needed.

For software cryptographic modules, DigiCert may destroy the Private Keys by overwriting the data. For hardware cryptographic modules, DigiCert may destroy the Private Keys by executing a "zeroize" command. Physical destruction of hardware is not required.

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

DigiCert archives a copy of each Public Key.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

DigiCert certificates have maximum validity periods of:

Type	Private Key Use	Certificate Term
Publicly Trusted Root CAs	No stipulation	25 years
Root CAs Not Otherwise Restricted	No stipulation	100 years
Publicly Trusted Sub CAs / Issuer CAs	No stipulation	15 years
IGTF Cross-certified Sub CA	6 years	15 years
CRL and OCSP responder signing	3 years	No stipulation
DV TLS	No stipulation	398 days
OV TLS	No stipulation	398 days
EV TLS	No stipulation	398 days
S/MIME	No stipulation	1185 days
Time Stamping Authority	15 months	135 months
Document Signing	No stipulation	39 months
Code Signing Certificate or EV Code Signing Certificate issued to subscriber under the Minimum Requirements for Code Signing Certificates	No stipulation	39 months
EV Code Signing Certificate issued to Signing Authority	123 months	123 months
IGTF End Entity Client used for signatures	36 months	36 months
IGTF Client used for key management	36 months	36 months
IGTF on hardware	60 months	13 months

Participants shall cease all use of their key pairs after their usage periods have expired.

Relying parties may still validate signatures generated with these keys after expiration of the Certificate.

For the purpose of calculations, a day is measured as 86,400 seconds. Any amount of time greater than this, including fractional seconds and/or leap seconds, represents an additional day. For purposes of calculating time periods in this document, increments are rounded down subject to the imposed maximum requirements listed in Section 1.1 as applicable.

CA Private Keys may retire before the periods listed above. CAs must not issue subscriber certificate with an expiration date that exceeds the CA's public key term stated in the table above or that exceeds the routine re-key identification requirements specified in Section 3.1.1.

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, DigiCert enforces 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.

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.

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 are 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.

Passwords require a minimum character length and a combination of alphanumeric and special characters. Password procedures are described in internal documentation.

Multi-factor authentication is enforced for all accounts capable of directly causing certificate issuance.

6.5.1. 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. Opensource 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.

If the CA uses Linting software developed by third parties, it should 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.

These protections include:

- Operating hardware firewalls for network perimeter control
- Continuously monitoring for system health and security events
- Performing periodic vulnerability scans and applying system security patches in a timely manner
- Managing logical access permissions in accordance with a formal procedure
- Enforcing multi-factor authentication
- Monitoring the configuration of access permissions

- Regular training of personnel in trusted roles

Additional procedures may be documented internally.

6.8. TIME-STAMPING

DigiCert operates a Timestamp Authority that complies with RFC 3161. DigiCert recommends that subscribers use the DigiCert Timestamp Authority to timestamp signed code.

DigiCert maintains clock synchronization when a leap second occurs. DigiCeret synchronizes its timestamp server at least every 24 hours with a UTC(k) time source. The timestamp server automatically detects and reports on clock drifts or jumps out of synchronization with UTC. Clock adjustments of one second or greater are auditable events. Any changes to the timestamp server's process are auditable events. The digest algorithm used to sign Timestamp tokens must match the digest algorithm used to sign the Timestamp certificate.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1. CERTIFICATE PROFILE

7.1.1 Version Number(s)

Publicly trusted certificates are X.509 version 3 certificates.

7.1.2. Certificate Extensions

IGTF Certificates comply with the Grid Certificate Profile as defined by the Open Grid Forum GFD.125.

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

7.1.3 Algorithm Object Identifiers

Certificates are signed using an algorithm permitted by the Applicable Requirements.

These algorithms include:

id-dsa-with-sha1	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 3}
sha-1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 5}
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 11}
sha384WithRSAEncryption	[iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12]
id-RSASSA-PSS	{ iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 10 }
ecdsa-with-SHA256	[iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2]
ecdsa-with-SHA1	{ iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) 1 }
ecdsa-with-SHA224	{ iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 1 }
ecdsa-with-SH256	{ iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2 (3) 2 }
ecdsa-with-SHA384	{ iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 3 }
ecdsa-with-SHA512	{ iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 4 }

TLS, S/MIME and OCSP Certificates are not signed with sha-1WithRSAEncryptiion.

Certificates using RSA with PSS padding have an RSA signature with PSSpadding using the following algorithms and OIDs:

id-sha256	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1 }
id-sha512	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 3 }

Key Pairs may be generated using the following:

id-dsa	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1}
RsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
Dhpublicnumber	{iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1}
id-ecPublicKey	{iso(1) member-body(2) us(840) ansi-X9-62(10045) id- publicKeyType(2) 1}
id-keyExchangeAlgorithm	{joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) algorithms(1) 22}

Keys and hash algorithms for TLS certificates meet the requirement specified in the TLS Baseline Requirements in Section 7 and the Applicable Requirements.

7.1.4. Name Forms

Each Certificate includes a unique serial number. Optional subject fields in a certificate either contain verified information or are left empty. Certificates cannot contain metadata such as '.', '-' and ' ' characters or and/or any other indication that the value/field is absent, incomplete, or not applicable.

S/MIME

Enterprise RAs may include optional attributes in the certificate as specified in Section 7.1.4.2.5 of the S/MIME Requirements. The Enterprise RA must validate this information using the process described in Section 3.

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 but, in addition to other values, may only include one of the following: serverAuth, code signing, emailProtection or timestamping.

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.

DigiCert maintains its OIDs in the following GitHub repository:
https://github.com/digicert/digicert_official_oids

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8. Policy Qualifiers Syntax and Semantics

Certificates may contain information in the Certificate Policy extension.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2. CRL PROFILE

DigiCert CRL profile conforms to RFC 5280. For TLS revocations the CRL profile conforms to the TLS BR.

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. 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 most appropriate reason for revocation of the certificate. The CRLReason for a revoked CA cannot be unspecified (0) or certificateHold(6).

Certificates may be revoked with one of the following reason codes, in order of preference when multiple reason codes are applicable:

- keyCompromise (1),
- cACompromise (2), which is only used for Sub CAs,
- privilegeWithdrawn (9);
- cessationOfOperation (5)
- affiliationChanged (3),
- superseded (4)
- unspecified (0), in which case the reasonCode entry extension is omitted.

7.2.2.1. CRL reasonCode Extension Entries

The following is a description of each of these reason codes and circumstances where DigiCert or a subscriber will be obligated to use it for their revocation circumstances:

7.2.2.1.1. keyCompromise

The CRLReason keyCompromise is used if:

- DigiCert obtains verifiable evidence that the certificate subscriber's private key corresponding to the public key in the certificate suffered a key compromise; or
- DigiCert is made aware of a demonstrated or proven method that exposes the certificate subscriber's private key to compromise; or
- There is clear evidence that the specific method used to generate the private key was flawed; or
- DigiCert is made aware of a demonstrated or proven method that can easily compute the certificate subscriber's private key based on the public key in the certificate (such as a Debian weak key, see https://wiki.debian.org/TLSkeys); or
- The certificate subscriber requests that DigiCert revoke the certificate for this reason, with the scope of revocation being described below.

If the entity requesting revocation for keyCompromise can demonstrate possession of the certificate's private key, then DigiCert will revoke all instances of that key across all subscribers.

If the entity requesting revocation cannot demonstrate possession of the certificate's private key, then DigiCert may revoke all certificates associated with that subscriber that contain that public key.

If DigiCert obtains verifiable evidence of private key compromise for a certificate whose CRL entry does not contain a reasonCode extension or has a reasonCode extension with a non- keyCompromise reason, DigiCert may update the CRL entry to enter keyCompromise as the CRLReason in the reasonCode extension. Additionally, DigiCert may update the revocation date in a CRL entry when it is determined that the private key of the certificate was compromised prior to the revocation date that is indicated in the CRL entry for that certificate.

7.2.2.1.2. privilegeWithdrawn

The CRLReason privilegeWithdrawn is used for subscriber-side infractions that do not compromise the certificate's private key, such as when the certificate subscriber provided misleading information in their certificate request or has breached a non-waived breach of the subscriber agreement or terms of use.

CRLReason privilegeWithdrawn is used when:

- DigiCert obtains evidence that the certificate was misused; or
- DigiCert is made aware that the certificate subscriber has violated one or more of its material obligations under the subscriber agreement or terms of use; or
- DigiCert is made aware that a wildcard certificate has been used to authenticate a fraudulently misleading subordinate fully-qualified domain name; or
- DigiCert is made aware of a material change in the information contained in the certificate; or
- DigiCert determines or is made aware that any of the information appearing in the certificate is inaccurate; or
- DigiCert is made aware that the original certificate request was not authorized and that the Subscriber does not retroactively grant authorization.

7.2.2.1.3. cessationOfOperation

The CRLReason cessationOfOperation is used when a website with the certificate is shut down prior to the expiration of the certificate or the subscriber no longer owns or controls the domain name in the certificate.

CRL cessationOfOperations is used when:

- The certificate subscriber will no longer be using the certificate because they are discontinuing their website; or
- DigiCert is made aware of any circumstance indicating that use of a fully-qualified domain name or IP address in the certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a domain name registrant's right to use the domain name, a relevant licensing or services agreement between the domain name registrant and the applicant has terminated, or the domain name registrant has failed to renew the domain name).
- The certificate subscriber has requested that their certificate be revoked for this reason; or
- DigiCert received verifiable evidence that the certificate subscriber no longer controls, or is no longer authorized to use, all of the domain names in the certificate.

Otherwise, the cessationOfOperation CRLReason is not used.

7.2.2.1.4. affiliationChanged

CRLReason affiliationChanged indicates that the subject's name or other subject identity information in the certificate has changed but there is no evidence that the certificate's private key was compromised.

CRLReason affiliationChanged is used when:

- The certificate subscriber has requested that their certificate be revoked for this reason; or
- DigiCert replaced the certificate due to changes in the certificate's subject information and the CA has not replaced the certificate for the other reasons: keyCompromise, superseded, cessationOfOperation, or privilegeWithdrawn.

Otherwise, the affiliationChanged CRLReason must not be used.

7.2.2.1.5. superseded

The CRLReason superseded is used when:

- The certificate subscriber has requested a new certificate to replace an existing certificate; or
- DigiCert obtains reasonable evidence that the validation of domain authorization or control for any fully-qualified domain name or IP address in the certificate should not be relied upon; or
- DigiCert revoked the certificate for compliance reasons such as the certificate does not comply with the DigiCert Public Trust CP/CPS, the CA/B Forum's Baseline Requirements, or the Mozilla Root Store Policy. Unless the keyCompromise CRLReason is being used, the CRLReason superseded must be used when:
- The certificate subscriber has requested that their certificate be revoked for this reason; or
- DigiCert revoked the certificate due to domain authorization or compliance issues other than those related to keyCompromise or privilegeWithdrawn.

Otherwise, the superseded CRLReason is notyou used.

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 the DigiCert Public Trust CP/CPS 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 assess the Issuer CA's and other parties' compliance with the applicable CPS. This audit must cover any CMSs, Sub CAs, RAs, and status server that is 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/CPS using one of the following audit schemes:

1. WebTrust Program for Certification Authorities;
2. WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security
3. WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL;
4. WebTrust Principles and Criteria for Certification Authorities – Code Signing Baseline Requirements
5. WebTrust Principles and Criteria for Certification Authorities – S/MIME
6. WebTrust Principles and Criteria for Certification Authorities – Network Security

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:

1. The auditor will document the discrepancy,
2. The auditor will promptly notify DigiCert and the Issuer CA, and
3. The Issuer CA will develop a plan to cure the noncompliance.

DigiCert submit 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 the DigiCert Public Trust CP/CPS. 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, Code Signing certificates and S/MIME 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. DigiCert may complete additional self-assessments as required by the root programs.

9. Other Business and Legal Matters

9.1. Fees

9.1.1. Certificate Issuance or Renewal Fees

DigiCert charges fees for certificate issuance and renewal. DigiCert may change its fees at any time in accordance with the applicable customer agreement.

9.1.2. Certificate Access Fees

DigiCert may charge a reasonable fee for access to its certificate databases.

9.1.3. Revocation or Status Information Access Fees

DigiCert does not charge a certificate revocation fee or a fee for checking the validity status of an issued Certificate using a CRL.

DigiCert may charge a fee for providing customized CRLs, OCSP services, or other value-added revocation and status information services. DigiCert does not permit access to revocation information, Certificate status information, or time stamping in their repositories by third parties that provide products or services that utilize such certificate status information without DigiCert's prior express written consent.

9.1.4. Fees for Other Services

DigiCert does not charge a fee for access to this CP/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

Subscribers must request refunds, in writing, within 30 days after a Certificate issues. After receiving the refund request, DigiCert may revoke the certificate. Refunds are discretionary and may be subject to applicable application processing fees.

9.2. Financial Responsibility

9.2.1. Insurance Coverage

DigiCert maintains Commercial General Liability insurance with a policy limit of at least $2 million in coverage and Professional Liability/Errors & Omissions insurance with a policy limit of at least $5 million in coverage.

Insurance is carried through companies rated no less than A- as to Policy Holder's Rating in the current edition of Best's Insurance Guide (or with an association of companies, each of the members of which are so rated).

9.2.2. Other Assets

No stipulation.

9.2.3. Insurance or Warranty Coverage for End-Entities

DigiCert provides a warranty to Subscribers according to the terms of the Netsure Extended Warranty Protection Plan. DigiCert provides a limited warranty to Relying Parties in DigiCert's Relying Party Agreement.

9.3. Confidentiality of Business Information

9.3.1. Scope of Confidential Information

The following information is considered confidential and 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 DigiCert 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/CPS).

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

DigiCert's 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

DigiCert follows the privacy policy posted on its website when handling personal information. Personal information is only disclosed when the disclosure is required by law or when requested by the subject of the personal information. Such privacy policies shall conform to applicable local privacy laws. DigiCert follows the Privacy Notices posted on its website when handling personal information. See https://www.digicert.com/digicert-privacy-policy

9.4.2. Information Treated as Private

DigiCert treats all personal information about an individual that is not publicly available in the contents of a certificate or CRL as private information. DigiCert protects private information using appropriate safeguards and a reasonable degree of care.

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

DigiCert employees and contractors are expected to handle personal information in strict confidence and meet the requirements outlined in DigiCert's Data Privacy Framework Policy. All sensitive information is securely stored and protected against accidental disclosure.

9.4.5. Notice and Consent to Use Private Information

Personal information obtained from an applicant during the application or identity verification process is considered private information if the information is not included in a certificate. DigiCert will only use private information after obtaining the subject's consent or as required by applicable law or regulation. All Subscribers must consent to the global transfer and publication of any personal data contained in a certificate.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

DigiCert may disclose private information, without notice, if DigiCert believes the disclosure is required by law or regulation.

9.4.7. Other Information Disclosure Circumstances

No stipulation.

9.5. Intellectual Property Rights

DigiCert and/or its business partners own the intellectual property rights in DigiCert's services, including the certificates, trademarks used in providing the services, and this CP/CPS. "DigiCert" is a registered trademark of DigiCert, Inc.

DigiCert retains all intellectual property rights in and to the certificates and revocation information that they issue. DigiCert 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.

Subscribers and Applicants retain all rights it has (if any) in any trademark, service mark, or trade name contained in any certificate and distinguished name within any certificate issued to such Subscriber or Applicant. DigiCert does not verify an applicant's right to use a trademark and does not resolve trademark disputes. DigiCert may reject any application or require revocation of any certificate that is part of a trademark dispute.

DigiCert shall not knowingly violate the intellectual property rights of any third party.

9.6. Representations and Warranties

9.6.1. CA Representations and Warranties

Except as expressly stated in this CP/CPS 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/CPS, that:

1. DigiCert complies, in all material aspects, with the DigiCert Public Trust CP/CPS, and all applicable laws and regulations,
2. DigiCert publishes and updates CRLs and OCSP responses on a regular basis,
3. All Certificates issued under this CP/CPS will be verified in accordance with this CP/CPS and meet the minimum requirements found herein and in the Applicable Requirements, and
4. DigiCert will maintain a repository of public information on its website.

To the extent allowed under EU law, DigiCert:

1. Does not warrant the accuracy, authenticity, completeness, or fitness of any unverified information, including name verification for (1) Certificates intended for email and intranet use, (2) Multi-SAN Certificates, and (3) other certificates issued to individuals and intranets.
2. Is not responsible for information contained in a certificate except as stated in this CP/CPS,
3. Does not warrant the quality, function, or performance of any software or hardware device, and
4. Is not responsible for failing to comply with this CP/CPS because of circumstances outside of DigiCert's control.

For EV Certificates, DigiCert represents to Subscribers, Subjects, Application Software Vendors that distribute DigiCert's Root Certificates, and Relying Parties that use a DigiCert Certificate while the Certificate is valid that DigiCert followed the EV Guidelines when verifying information and issuing EV Certificates.

This representation is limited solely to DigiCert's compliance with the EV Guidelines (e.g., DigiCert may rely on erroneous information provided in an attorney's opinion or accountant's letter that is checked in accordance with the Guidelines).

Subscriber Agreements may include additional representations and warranties that do not contradict or supersede this CP/CPS.

9.6.2. RA Representations and Warranties

RAs represent that: 1. The RA's certificate issuance and management services conform to the DigiCert Public Trust CP/CPS, 2. Information provided by the RA does not contain any false or misleading information, 3. Translations performed by the RA are an accurate translation of the original information, and 4. All Certificates requested by the RA meet the requirements of the DigiCert Public Trust CP/CPS.

DigiCert's agreement with the RA may contain additional representations.

9.6.3. Subscriber Representations and Warranties

Prior to being issued and receiving a certificate, subscribers are solely responsible for any misrepresentations they make to third parties and for all transactions that use subscriber's Private Key, regardless of whether such use was authorized. Subscribers are required to notify DigiCert and any applicable RA if a change occurs that could affect the status of the certificate. DigiCert requires, as part of the Subscriber Agreement or Terms of Use for TLS, that the Applicant make the commitments and warranties in this section for the benefit of DigiCert and the Certificate Beneficiaries.

Prior to the issuance of a Certificate, DigiCert will obtain, for the express benefit of DigiCert and the Certificate Beneficiaries, either:

1. The Applicant's agreement to the Subscriber Agreement with DigiCert, or
2. The Applicant's acknowledgement of the Terms of Use.

Subscribers represent to DigiCert, Application Software Vendors, and Relying Parties that, for each certificate, the subscriber will:

1. Securely generate its Private Keys and protect its Private Keys from compromise,
2. Provide accurate and complete information when communicating with DigiCert,
3. Confirm the accuracy of the certificate data prior to using the Certificate,

4. Promptly (i) request revocation of a Certificate, cease using it and its associated Private Key, and notify DigiCert if there is any actual or suspected misuse or compromise of the Private Key associated with the Public Key included in the Certificate, and (ii) request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate,
5. Ensure that individuals using certificates on behalf of an organization have received security training appropriate to the Certificate,
6. Use the certificate only for authorized and legal purposes, consistent with the certificate purpose, this CP/CPS, any other applicable CP, and the relevant Subscriber Agreement, including only installing TLS certificates on servers accessible at the domain listed in the certificate and not using code signing certificates to sign malicious code or any code that is downloaded without a user's consent, and
7. Promptly cease using the certificate and related Private Key after the certificate's expiration.

Subscriber Agreements may include additional representations and warranties.

9.6.4. Relying Party Representations and Warranties

Each Relying Party represents that, prior to relying on a DigiCert 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 DigiCert's limitations on liability related to the use of certificates,
3. Has read, understands, and agrees to the DigiCert Relying Party Agreement and the DigiCert Public Trust CP/CPS,
4. Verified both the DigiCert Certificate and the certificates in the certificate chain using the relevant CRL or OCSP,
5. Will not use a DigiCert Certificate if the certificate has expired or been revoked and
6. Will take all reasonable steps to minimize the risk associated with relying on a digital signature, including only relying on a DigiCert Certificate after considering:
    - Applicable law and the legal requirements for identification of a party, protection of the confidentiality or privacy of information, and enforceability of the transaction;
    - The intended use of the certificate as listed in the certificate or this CP/CPS,
    - The data listed in the certificate,
    - The economic value of the transaction or communication,
    - The potential loss or damage that would be caused by an erroneous identification or a loss of confidentiality or privacy of information in the application, transaction, or communication,
    - The Relying Party's previous course of dealing with the Subscriber,
    - The Relying Party's understanding of trade, including experience with computer-based methods of trade, and

- Any other indicia of reliability or unreliability pertaining to the subscriber and/or the application, communication, or transaction.

Any unauthorized reliance on a certificate is at a party's own risk.

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

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/CPS IN PROVIDING THE CERTIFICATE OR SERVICE. DIGICERT'S LIABILITY FOR CERTIFICATES AND SERVICES THAT DO NOT MATERIALLY COMPLY WITH THIS CP/CPS 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/CPS;
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/CPS, or (v) whether any provision of this CP/CPS was proven ineffective. The disclaimers and limitations on liabilities in this CP/CPS 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/CPS , 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/CPS, 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/CPS, 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/CPS and any amendments to the CP/CPS 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/CPS 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/CPS'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/CPS terminates.

9.11. Individual Notices and Communications With Participants

DigiCert accepts notices related to this CP/CPS 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

The DigiCert Public Trust CP/CPS is reviewed annually. Amendments are made by posting an updated version of the CP/CPS to the online repository. Updates supersede any designated or conflicting provisions of the referenced version of the CP/CPS. Controls are in place to reasonably ensure that this CP/CPS 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/CPS to its website. DigiCert does not guarantee or set a notice-and-comment period and may make changes to this CP/CPS 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/CPS.

9.12.3. Circumstances under which OID Must Be Changed

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

9.13. Dispute Resolution Provisions

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall contain a dispute resolution clause. Unless otherwise approved by DigiCert, the procedure to resolve disputes involving DigiCert require an initial negotiation period of sixty (60) days followed by litigation in the federal or state court encompassing Salt Lake 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

Parties are required to notify DigiCert and attempt to resolve disputes directly with DigiCert before resorting to any dispute resolution mechanism, including adjudication or any type of alternative dispute resolution.

9.14. Governing Law

The laws of the state of Utah govern the interpretation, construction, and enforcement of this CP/CPS and all proceedings related to DigiCert's products and services, including tort claims, without regard to any conflicts

of law principles. The state of Utah, and Salt Lake County, has non-exclusive venue and jurisdiction over any proceedings related to the CP/CPS or any DigiCert product or service.

9.15. Compliance With Applicable Law

The DigiCert Public Trust CP/CPS 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 organization 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 RA to comply with this CP/CPS 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/CPS, 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/CPS may not assign their rights or obligations without the prior written consent of DigiCert. Unless specified otherwise in a contact with a party, DigiCert does not provide notice of assignment.

9.16.3. Severability

If any provision of this CP/CPS is held invalid or unenforceable by a competent court or tribunal, the remainder of the CP/CPS will remain valid and enforceable. Each provision of this CP/CPS 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/CPS does not waive DigiCert's right to enforce the same provision later or right to enforce any other provision of this CP/CPS. 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/CPS 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.