DigiCert TLS PQC Pilot Certificate Policy and Practices Statement

Version: 1.0
Effective Date: 18 September 2026
Document Owner: DigiCert, Inc

1. Introduction

1.1. Overview

This document is the DigiCert TLS PQC Pilot Certificate Policy and Certification Practices Statement and is one of several documents that govern the certification services provided by DigiCert. For clarity, “TLS” refers to Transport Layer Security and applies to certificates used to secure web-based communications.

[!IMPORTANT]
Certificates issued under this TLS PQC Pilot are intended for closed testing environments, custom applications, and enterprise testbeds. The purpose of the PQC Pilot is to evaluate the impact of PQC in those environments, not to establish a standard for publicly-accessible web connections. Certificates issued under this PQC Pilot:

- Are **NOT** publicly trusted.
- Are **NOT** intended for production trust scenarios.
- Are **NOT** intended to secure public-facing web connections.
- Will **NOT** be added to the Common CA Database (CCADB).
- Will **NOT** be considered for public trust inclusion by Microsoft.
- Will **NOT** be added to Certificate Transparency Logs.
- Exist solely for interoperability testing and ecosystem-readiness purposes.

Each in-scope Subordinate CA Certificate asserts an extendedKeyUsage (EKU) extension containing id-kp-serverAuth and id-kp-clientAuth.

1.1.1. Applicable Requirements

Described below is a list of requirements to which DigiCert adheres. In the event of any inconsistency between this document and these requirements, these requirements take precedence over this document. Collectively, these requirements are referred to as the “Applicable Requirements” and are referred to as such throughout this document. Unless otherwise specified, DigiCert adheres to the latest version.

- Microsoft Post-Quantum Cryptography (PQC) TLS Pilot Program Requirements - https://github.com/TrustedRootProgram/Program-Requirements/blob/main/PQC%20Pilot%20Program.md

1.1.2. Applicable Roots

This CP/CPS applies to Certificates issued under the following hierarchies:

Root: DigiCert PQC TLS PILOT MLDSA87 Root CA
Serial Number: 097bdab35689305cc1bf34ef35158789
Thumprint: 057f507d6c93d3a348628572d517f4f10eb2b967

The PQC TLS Pilot will operate for a limited duration and there are no plans for this hierarchy to continue in normal production after the Pilot concludes. At the conclusion of the Pilot, Microsoft will remove the certificate from the Microsoft Trusted Root Program CTL.

1.2 Document Name and Identification

This document is the DigiCert TLS PQC Pilot Certificate Policy and Certification Practices Statement (TLS PQC Pilot CP/CPS). It came into effect on September 18, 2026.

The CP/CPS is structured according to the RFC3647 framework. To preserve the RFC 3647 structure alignment, some sections will state “Not Applicable” or “No Stipulation”.

Separate policy documents addressing other PKI products are contained in the Legal Repository on the DigiCert website: https://www.digicert.com/legal-repository

1.3 PKI Participants

1.3.1 Certification Authorities

DigiCert operates certification authorities that issue or support the issuance of in-scope TLS certificates. As operator of those CAs, DigiCert performs or oversees functions associated with public key operations, including receiving certificate requests, validating certificate requests, issuing certificates, revoking certificates, renewing or re-keying certificates where permitted, and maintaining, issuing, and publishing CRLs responses.

Issuing CAs may be operated directly by DigiCert or by organizations authorized by DigiCert to participate within the DigiCert PKI. Such parties are required to ensure that the services they perform within the DigiCert PKI always comply with their respective agreements, applicable standards, and this CP/CPS.

1.3.2 Registration Authorities

DigiCert performs registration authority functions directly or through authorized RAs or delegated third parties. An RA or delegated third party performing validation, support, or other certificate-related functions shall operate under written agreement, documented controls, and oversight by DigiCert.

An Enterprise RA may perform certain parts of the RA function for their own organization. In these instances, the Enterprise RA will be required to meet the relevant requirements as set out by this CP/CPS and their contract.

Validation of domains and IP addresses cannot be delegated to a third party.

1.3.3 Subscribers

A Subscriber is the legal or natural person bound by agreement with DigiCert to the obligations outlined in that agreement. A Subscriber is not required to be the Subject of certificates under its control.

1.3.4 Relying Parties

A Relying Party is any natural person or legal entity that relies on a certificate or CRL issued under this CP/CPS.

1.3.5 Other Participants

Other participants not otherwise covered in this CP/CPS may be identified by DigiCert where relevant to the provision, oversight, supervision, accreditation, or reliance framework applicable to the certificate service. Such participants may include auditors, supervisory bodies, trusted list operators, accreditation authorities and application software suppliers.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

Certificate usage is restricted by the key usage and extended key usage values stipulated within the relevant certificate profile and governed by the Applicable Requirements, the Master Services Agreement, and this CP/CPS.

1.4.2 Prohibited Certificate Uses

Certificates governed by this CP/CPS shall not be used for any purpose inconsistent with the relevant Key Usage or Extended Key Usage values, for any purpose prohibited by the Subscriber Agreement, Relying Party Agreement, or applicable law, or in any manner that misrepresents the identity, authority, authorizations, or entitlements of the Subscriber.

Key pinning is strongly discouraged and is not considered a sufficient reason to delay revocation. Customers should not mix Certificates trusted for the web with non-web PKI.

1.5 Policy Administration

1.5.1 Organization Administering the Document

This CP/CPS is administered by the DigiCert Policy Authority (DCPA).

1.5.2. Contact Person

Enquiries or other communications about this CP/CPS should be addressed to:
DigiCert, Inc
2801 N Thanksgiving Way #500
Lehi
UT 84043
United States
E-mail: policy@digicert.com

1.5.2.1 Revocation Reporting Contact Person

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

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

Entities submitting Certificate revocation requests must explain the reason for requesting revocation. DigiCert will authenticate and log each revocation request according to Section 4.9 of this CP/CPS. DigiCert will always revoke a Certificate if the request is authenticated as originating from the Subscriber or an authorized representative of the Organization listed in the Certificate.

If revocation is requested by someone other than an authorized representative of the Subscriber or Affiliated Organization, DigiCert will investigate the alleged basis for the revocation request prior to acting.

1.5.3 Person Determining CPS Suitability for the Policy

The DCPA determines the suitability and applicability of this CPS.

1.5.4 CPS Approval Procedures

Approval of this CP/CPS and any amendments hereto is by the DCPA. Amendments may be made by updating this entire document or by addendum.

1.6 Definitions and Acronyms

Key terms used frequently in this CP/CPS are summarized below.

1.6.1 Definitions

Term	Definition
Applicant	The Applicant is an entity applying for a Certificate.
Applicant Representative	A Natural Person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant; who signs and submits, or approves a Certificate Request on behalf of the Applicant; who signs and submits the Master Services Agreement on behalf of the Applicant; and/or who acknowledges the Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA or is the CA.
Application Software Supplier	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

Term	Definition
	such information.
Authorization Domain Name	The FQDN used to perform validation of domain authorization or control for a given FQDN or Wildcard Domain Name.
Certificate Application	Any of several forms completed by the Applicant or DigiCert and used to process the Certificate request, including but not limited to agreements signed by Contract Signers and online forms submitted by Certificate Requesters.
Certificate Problem Report	A complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.
Certificate Profile	A set of documents that defines Certificate content and Certificate extensions.
Certificate Requester	A natural person who is employed by the Applicant, or an authorized agent who has express authority to represent the Applicant or a third party (such as an ISP or hosting company), and who completes and submits a Certificate request on behalf of the Applicant.
Certification Authority Authorization (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-issuance.
Contract Signer	A natural person who is employed by the Applicant and who has express authority to sign Subscriber Agreements on behalf of the Applicant.
Cryptographic Module	Secure software, device or utility that (1) generates Key Pairs; (2) stores cryptographic information; and/or (3) performs cryptographic functions.
DigiCert Policy Authority	The group within DigiCert responsible for overseeing and approving CP/CPS amendments and general management of the PKI.
Digital Certificate	An electronic document that identifies the Issuing CA, identifies the Subject, contains the Subject's Public Key, specifies the Certificate validity period and permitted uses, and is digitally signed by the Issuing CA.
Domain Name	An ordered list of one or more Domain Labels assigned to a node in the Domain Name System.
Fully Qualified Domain Name	A Domain Name that includes the Domain Labels of all superior nodes in the Internet Domain Name System.
Key Pair	A Private Key and associated Public Key.
Linting	A process in which the content of digitally signed data such as a Precertificate (RFC 6962), Certificate, Certificate Revocation List (CRL), or a data-to-be-signed object such as a `tbsCertificate` (RFC 5280, Section 4.1.1.1), is checked for conformance with the applicable profiles and requirements.

Term	Definition
Multi-Perspective Issuance Corroboration	A process by which the determinations made during domain validation and CAA checking by the Primary Network Perspective are corroborated by other Network Perspectives before Certificate issuance.
Network Perspective	Related to Multi-Perspective Issuance Corroboration. A system (for example, a cloud-hosted server instance) or collection of network components (for example, a VPN and corresponding infrastructure) used for sending outbound Internet traffic associated with domain control validation and/or CAA checking. The location of a Network Perspective is determined by the point where unencapsulated outbound Internet traffic is first handed off to the Internet connectivity provider.
PQC Pilot Certificate Profile	A documents that defines Certificate content and Certificate extensions.
Private Key	The key of a Key Pair that is kept secret by the holder of the Key Pair and is used to create digital signatures and/or decrypt information 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 is used to verify digital signatures or encrypt messages for the holder of the corresponding Private Key.
Reliable Data Source	An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate.
Reliable Method of Communication	A method of communication, such as a postal address, courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative.
Relying Party	A natural person or legal entity that relies on a Certificate, CRL, or OCSP response, whether directly or through application software, subject to applicable relying-party terms and law.
Relying Party Agreement	An agreement that must be read and accepted by a Relying Party prior to validating, relying on, or using a Certificate or accessing or using the DigiCert Repository.
Short-lived Subscriber Certificate	For Certificates issued on or after 15 March 2026, a Subscriber Certificate with a Validity Period less than or equal to 7 days (604,800 seconds).
Subordinate CA	A Certification Authority whose Certificate is signed by the Root CA or another Subordinate CA. Also known as an Issuing CA.
Subscriber Agreement	An agreement governing the issuance and use of a Certificate that the Applicant must read and accept before receiving a Certificate.

Term	Definition
Subscriber	A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use.
Terms and Conditions	The Master Services Agreement, Certificate Terms of Use, Privacy Policy, and relevant CP/CPS. The Master Services Agreement incorporates the Certificate Terms of Use, Privacy Policy, and relevant CP/CPS into the Terms and Conditions.

1.6.2 Acronyms

Acronym	Definition
ADN	Authorization Domain Name
ALPN	TLS Application-Layer Protocol Negotiation (ALPN) Extension ([RFC 7301]) as defined in RFC 8737
CA	Certificate Authority or Certification Authority
CAA	Certificate Authority Authorization
CP/CPS	Certificate Policy and Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CT	Certificate Transparency
DCPA	DigiCert Policy Authority
FIPS	Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
MPIC	Multi-Perspective Issuance Corroboration
OID	Object Identifier
OV	Organization Validated
PKI	Public Key Infrastructure
SSL	Secure Sockets Layer
TLD	Top-Level Domain
TLS	Transport Layer Security
TTL	Time to Live

Acronym	Definition
UTC	Coordinated Universal Time
X.509	The ITU-T standard for Certificates and their corresponding authentication framework

1.6.3 References

- Microsoft Post-Quantum Cryptography (PQC) TLS Pilot Program Requirements - https://github.com/TrustedRootProgram/Program-Requirements/blob/main/PQC%20Pilot%20Program.md
- CA/Browser Forum Issuance and Management of Publicly-Trusted TLS Server Certificates - https://cabforum.org/working-groups/server/baseline-requirements/requirements/

1.6.4 Conventions

Within this CP/CPS, DigiCert uses prescriptive language such as shall, must, and may in accordance with the interpretation described in RFC2119.

2. Publication and Repository Responsibilities

2.1 Repositories

DigiCert maintains online repositories containing current and, where required by the Applicable Requirements, historical information concerning the certificates and services governed by this CP/CPS.

The repositories shall include this CP/CPS, related legal notices, root and subordinate CA certificates, CRLs, certificate status service information, audit or assessment information where publication is required or appropriate, hierarchy information, policy OID information, and other certification information that DigiCert elects or is required to publish.

Certificates issued in the PQC TLS Pilot are not registered in Certificate Transparency (CT) Logs.

DigiCert shall publish certification information in a manner reasonably designed to permit Subscribers, Relying Parties, application software suppliers, auditors, supervisory bodies, and other authorized stakeholders to access current information relevant to in-scope certificates.

This document and its related agreements are made available 24/7 via the DigiCert Repository located at https://www.digicert.com/legal-repository.

2.3 Time or Frequency of Publication

DigiCert publishes CRL resources to allow Relying Parties to determine the validity of a DigiCert Certificate. Certificate information is published promptly following generation, issue and following the completion of the revocation process. For frequency of CRL issuance, see Section 4.9.

DigiCert updates this CP/CPS as required to describe how DigiCert meets the relevant requirements. Those updates indicate conformance by incrementing the version number and adding a dated changelog. New or modified versions of the CP/CPS and other related policies are published within 7 days after their approval.

2.4 Access Controls on Repositories

Repository information intended for public disclosure shall be publicly readable. DigiCert shall implement logical, administrative, and physical controls to restrict unauthorized creation, modification, deletion, or publication of repository content.

If the Repository is unavailable, DigiCert aims to restore availability within 24 hours.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

Distinguished Names (DN) included in Certificates comply with the ITU X.500 standard for Distinguished Names (DN).

Certificates governed by this CP/CPS shall contain Subject and Subject Alternative Name information consistent with applicable PQC Pilot certificate profiles and product requirements.

3.1.2 Need for Names to be Meaningful

Subject and Subject Alternative Name information accurately reflect the identity, domain information, authorizations, or other certificate content validated by DigiCert, as applicable to the certificate type.

3.1.3 Anonymity or Pseudonymity of Subscribers

DigiCert shall not issue in-scope TLS certificates to anonymous or pseudonymous subscribers.

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.

3.1.5 Uniqueness of Names

Unique subject names are not enforced. Uniqueness between certificates is maintained by assigning unique certificate serial numbers. Name uniqueness is not violated when multiple Certificates are issued to the same entity.

3.1.6 Recognition, Authentication, and Role of Trademarks

DigiCert may include verified trade names, assumed names, or d/b/a names, where permitted by applicable requirements and where DigiCert has verified the applicant's right to use them.

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

3.2 Initial Identity Validation

DigiCert may use any legal means of communication or investigation to ascertain the identity of Applicants in compliance with this CP/CPS. DigiCert may refuse to issue a Certificate in its sole discretion.

3.2.1 Method to Prove Possession of Private Key

DigiCert verifies possession of the private key corresponding to the public key submitted for certification by validating that the certificate request, including the CSR where applicable, is digitally signed using the associated private key and that the signature verifies successfully before issuance.

3.2.2 Authentication of Organization Identity

DigiCert maintains and regularly reviews internal policies and procedures that ensure compliance with the applicable requirements when vetting the identity of organizations for PQC TLS Pilot certificates.

3.2.2.1 Identity

3.2.2.1 Organization Validation

DigiCert verifies the identity of the applicant business or trade name using one or more sources or methods permitted by the applicable requirements, including qualified government, tax, or independent information sources, an incorporating or registration agency, a reliable data source, an attestation letter, or a site visit. Organization verification is required for certificate profiles that include the organizationName field. Address information is also verified whenever an organizationName value is present in the certificate subject.

The same documentation or source may be used to verify the applicant address, telephone number, or email address where the applicable requirements permit. DigiCert may also rely on a utility bill, bank statement, credit card statement, or other documentation that DigiCert determines to be reliable for the attribute being verified.

3.2.2.2 DBA/Tradename

DigiCert verifies that the applicant has registered its use of the assumed name with the appropriate government agency for such filings in the jurisdiction of incorporation or registration and that the filing remains valid. DigiCert may also rely on an attestation that identifies the assumed name, the filing agency, and confirmation that the filing remains valid.

3.2.2.3 Verification of Country

DigiCert verifies the subject countryName field of a certificate by verifying the address of the applicant using the methods described above, as applicable to the relevant certificate class and subject type.

3.2.2.4 Validation of Domain Authorization Control

All domains included in Certificates issued according to this CP/CPS are validated according to one of the methods described in this section.

Unless described otherwise, Random Values referred to below shall be unique in each email, fax, SMS or postal mail. The Random Value shall remain valid for use in a confirming response for no more than 30 days from its

creation.

DNSSEC validation back to the IANA DNSSEC root trust anchor must be performed on all DNS queries associated with the validation of domain authorisation or control by the Primary Network Perspective. The DNS resolver used for all DNS queries associated with the validation of domain authorisation or control by the Primary Network Perspective must:

• Perform DNSSEC validation using the algorithm defined in RFC 4035 Section 5; and
• Support NSEC3 as defined in RFC 5155; and
• Support SHA-2 as defined in RFC 4509 and RFC 5702; and
• Properly handle the security concerns enumerated in RFC 6840 Section 4.

DNSSEC validation back to the IANA DNSSEC root trust anchor MAY be performed on all DNS queries associated with the validation of domain authorization or control by Remote Network Perspectives used for Multi-Perspective Issuance Corroboration.

3.2.2.4.1 Validating the Applicant as a Domain Contact

This method is no longer allowed and DigiCert does not do this.

3.2.2.4.2. Email, Fax, SMS, or Postal Mail to Domain Contact

This method is no longer allowed and DigiCert does not do this.

3.2.2.4.3. Phone Contact with Domain Contact

This method is no longer allowed and DigiCert does not do this.

3.2.2.4.4. Constructed Email to Domain Contact

DigiCert confirms the applicant's control over a fully qualified domain name by sending an email containing a Random Value to one or more constructed addresses using admin, administrator, webmaster, hostmaster, or postmaster at an authorization domain name, and receiving a confirming response utilizing that Random Value.

Each email may confirm control of multiple FQDNs provided the authorization domain name used is valid for each FQDN. The email may be re-sent in its entirety, including reuse of the Random Value, provided the contents and recipient remain unchanged.

Where permitted by the applicable requirements, once an FQDN has been validated using this method, DigiCert may issue certificates for other FQDNs that end with all domain labels of the validated FQDN. This method is suitable for validating wildcard domain names, subject to the applicable restrictions.

By no later than March 15th, 2028, DigiCert will no longer rely on this method for the issuance of Subscriber Certificates.

DigiCert performs this validation method in accordance with Section 3.2.2.4.4 of the TLS BRs.

3.2.2.4.5. Domain Authorization Document

This method is no longer allowed and DigiCert does not do this.

3.2.2.4.6. Agreed-Upon Change to Website

This method is no longer allowed and DigiCert does not do this.

3.2.2.4.7. DNS Change

DigiCert may confirm the applicant control over an 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 domain label that begins with an underscore character.

Where a Random Value is used, DigiCert provides a value unique to the certificate request and does not use that value after 30 days. When DigiCert uses this method, it implements Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. This method is suitable for validating wildcard domain names.

Note: Once the FQDN has been validated using this method, then DigiCert may also issue Certificates for other FQDNs that end with all the domain labels of the validated FQDN.

This method is suitable for validating Wildcard Domain Names.

DigiCert performs this validation method in accordance with 3.2.2.4.7 of the TLS BRs.

3.2.2.4.8. IP Address

DigiCert does not use this method.

3.2.2.4.9. Test Certificate

This method is no longer allowed for publicly trusted TLS issuance and DigiCert does not use it.

3.2.2.4.10. TLS Using a Random Value

This method is no longer allowed for publicly trusted TLS issuance and DigiCert does not use it.

3.2.2.4.11. Any Other Method

This method is no longer allowed for publicly trusted TLS issuance.

3.2.2.4.12. Validating Applicant as a Domain Contact

DigiCert does not use this method.

3.2.2.4.13. Email to DNS CAA Contact

DigiCert may confirm the applicant control over an FQDN by sending a Random Value by email to a DNS CAA email contact and receiving a confirming response utilizing that Random Value. Each email may confirm control of multiple FQDNs where the selected contact is valid for each authorization domain name. When DigiCert performs validation using this method, it implements Multi-Perspective Issuance Corroboration as

specified in Section 3.2.2.9. To count as corroborating, a Network Perspective must observe the same challenge information (i.e. Random Value or Request Token) as the Primary Network Perspective.

This method is suitable for validating wildcard domain names, subject to the applicable restrictions.

By no later than March 15th, 2028, DigiCert will no longer rely on this method for the issuance of Subscriber Certificates.

DigiCert performs this validation method in accordance with 3.2.2.4.13 of the TLS BRs

3.2.2.4.14. Email to DNS TXT Contact

DigiCert may confirm the applicant control over an FQDN by sending a Random Value by email to a DNS TXT record email contact for the authorization domain name and receiving a confirming response utilizing that Random Value. Each email may confirm control of multiple FQDNs where the selected contact is valid for each authorization domain name. When DigiCert performs validation using this method, it implements Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. To count as corroborating, a Network Perspective must observe the same challenge information (i.e. Random Value or Request Token) as the Primary Network Perspective. This method is suitable for validating wildcard domain names, subject to the applicable restrictions.

By no later than March 15th, 2028, DigiCert will no longer rely on this method for the issuance of Subscriber Certificates.

DigiCert performs this validation method in accordance with 3.2.2.4.14 of the TLS BRs.

3.2.2.4.15. Phone Contact with Domain Contact

This method is no longer allowed for publicly trusted TLS issuance and DigiCert does not use it.

3.2.2.4.16. Phone Contact with DNS TXT Record Phone Contact

DigiCert does not use this method.

3.2.2.4.17. Phone Contact with DNS CAA Phone Contact

DigiCert does not use this method.

3.2.2.4.18. Agreed-Upon Change to Website v2

DigiCert may confirm the applicant control over an FQDN by verifying that a Request Token or Random Value is contained in the contents of a file located on the authorization domain name under /.well-known/pki-validation and retrieved over an authorized HTTP or HTTPS connection. The entire token must not appear in the request used to retrieve the file, and DigiCert must receive a successful 2xx HTTP response. Where a Random Value is used, DigiCert limits its validity to no more than 30 days. When DigiCert uses this method, it implements Multi-Perspective Issuance Corroboration.

Note: This method is not suitable for validating Wildcard Domain Names. DigiCert performs this validation method in accordance with 3.2.2.4.18 of the TLS BRs.

3.2.2.4.19. Agreed-Upon Change to Website – ACME

DigiCert may confirm the applicant control over an FQDN using the ACME HTTP challenge method defined in RFC 8555, subject to the additive requirements that DigiCert receives a successful 2xx response, the token is not used for more than 30 days from creation, any redirect handling complies with the applicable requirements, and Multi-Perspective Issuance Corroboration is implemented.

Note: This method is not suitable for validating Wildcard Domain Names. DigiCert performs this validation method in accordance with 3.2.2.4.19 of the TLS BRs.

3.2.2.4.20. TLS Using ALPN

DigiCert does not use this method.

3.2.2.4.21. DNS Labelled with Account ID – ACME

DigiCert does not use this method.

3.2.2.4.22. DNS TXT Record with Persistent Value

DigiCert may confirm the applicant's control over an FQDN by verifying the presence of a Persistent DCV TXT Record identifying the applicant at the _validation-persist label prepended to the authorization domain name being validated.

For this method, DigiCert must not use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. This prohibition overrides the Authorization Domain Name definition. CNAME records may be followed when resolving the Persistent DCV TXT Record.

DigiCert must confirm the Persistent DCV TXT Record's RDATA value fulfills the following requirements:

1. The RDATA value must conform to the issue-value syntax as defined in RFC 8659, Section 4.2; and
2. The issuer-domain-name value must be one of the CA Identifier domains disclosed in Section 4.2 of this CP/CPS; and
3. The issue-value must contain an accounturi parameter, where the parameter value is a unique URI (as described by RFC 8657, Section 3) identifying the account of the Applicant which requested validation for this FQDN; and
4. The issue-value may contain a persistUntil parameter. If present, the parameter value must be a base-10 encoded integer representing a UNIX timestamp (the number of seconds since 1970-01-01T00:00:00Z ignoring leap seconds); and
5. The issue-value may contain additional parameters, but unknown parameters will be ignored.

If the persistUntil parameter is present, the DigiCert must evaluate its value. If the time of the check is after the time specified in the persistUntil parameter value, DigiCert must not use the record as evidence of the Applicant's control over the FQDN.

DigiCert implements Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9 when using this method. To count as corroborating, a Network Perspective must observe a Persistent DCV TXT Record that demonstrates the Applicant's control over the domain and contains the same accounturi parameter as the Primary Network Perspective.

The maximum reuse period for this method is 10 days.

DigiCert performs this validation method in accordance with 3.2.2.4.22 of the TLS BRs.

3.2.2.5. Authentication for an IP Address

DigiCert validates the applicant ownership or control of the IP address using at least one method permitted by the applicable requirements and DigiCert documented procedures.

3.2.2.5.1. Agreed-Upon Change to Website

Confirming the Applicant's control over the requested 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, or another path registered with IANA for the purpose of validating control of IP Addresses, on the IP Address that is accessible by DigiCert via HTTP/HTTPS over an Authorized Port.

The Request Token or Random Value must not appear in the request. If a Random Value is used, the DigiCert shall provide a Random Value unique to the certificate request and shall not use the Random Value after 30 days.

When DigiCert performs validation using this method, it implements Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. To count as corroborating, a Network Perspective must observe the same challenge information (i.e. Random Value or Request Token) as the Primary Network Perspective.

DigiCert performs this validation method in accordance with 3.2.2.5.1 of the TLS BRs.

3.2.2.5.2. Email, Fax, SMS, or Postal Mail to IP Address Contact

DigiCert does not use this method.

3.2.2.5.3. Reverse Address Lookup

DigiCert does not use this method.

3.2.2.5.4. Any Other Method

This method is no longer allowed for publicly trusted TLS issuance.

3.2.2.5.5. Phone Contact with IP Address Contact

Confirming the Applicant's control over the IP Address by calling the IP Address Contact's phone number and obtaining a response confirming the Applicant's request for validation of the IP Address. DigiCert must place the call to a phone number identified by the IP Address Registration Authority as the IP Address Contact. Each phone call shall be made to a single number. If someone other than an IP Address Contact is reached, DigiCert may request to be transferred to the IP Address Contact. In the event of reaching voicemail, DigiCert may leave the Random Value and the IP Address(es) being validated.

The Random Value must be returned to DigiCert to approve the request. The Random Value shall remain valid for use in a confirming response for no more than 30 days from its creation

By no later than March 15th, 2027, DigiCert will no longer rely on this method for the issuance of Subscriber Certificates. DigiCert performs this validation method in accordance with 3.2.2.5.5 of the TLS BRs.

3.2.2.5.6. 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 RFC 8738. When DigiCert performs validation using this method, it implements Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. To count as corroborating, a Network Perspective must observe the same challenge information (i.e. Random Value or Request Token) as the Primary Network Perspective. DigiCert performs this validation method in accordance with 3.2.2.5.6 of the TLS BRs.

3.2.2.5.7. ACME "tls-alpn-01" method for IP Addresses

DigiCert does not use this method.

3.2.2.5.8 DNS TXT Record with Persistent Value in the Reverse Namespace

DigiCert does not use this method.

3.2.2.6. Wildcard Domain Validation

Before issuing a wildcard certificate, DigiCert establishes and follows a documented procedure to determine whether the FQDN portion of any wildcard domain name is registry-controlled or a public suffix. If it is registry-controlled or a public suffix, DigiCert shall refuse issuance unless the applicant proves rightful control of the entire relevant namespace.

3.2.2.7. Data Source Accuracy

DigiCert evaluates data sources used for validation based on factors that include the age of the information provided, the frequency with which the source is updated, the data provider and the purpose for which the data was collected, the public accessibility and availability of the data, and the relative difficulty of falsifying or altering the data.

3.2.2.8. CAA Records

As part of the Certificate issuance process, DigiCert retrieves and processes CAA records in accordance with RFC 8659 for each dNSName in the subjectAltName extension that does not contain an Onion Domain Name.

Refer to Section 4.2.2.1 for additional CAA record processing requirements.

3.2.2.8.1. DNSSEC Validation of CAA Records

Refer to Section 4.2.2.1.3 for DNSSEC validation of CAA record processing requirements.

3.2.2.9. Multi-Perspective Issuance Corroboration

Multi-Perspective Issuance Corroboration is used by DigiCert to corroborate determinations made by the primary network perspective before certificate issuance, including domain validation pass/fail outcomes and CAA permission/prohibition outcomes. DigiCert may use the same or different sets of network perspectives

for domain-control checks and for CAA checks. Results obtained from one network perspective shall not be reused or cached when performing validation through subsequent network perspectives. Communications between DigiCert and a remote network perspective take place over an authenticated and encrypted channel.

DigiCert may reuse corroborating evidence for CAA record quorum compliance for a maximum of 398 days. After issuing a Certificate to a domain, remote Network Perspectives may omit retrieving and processing CAA records for the same domain or its subdomains in subsequent Certificate requests from the same Applicant for up to a maximum of 398 days.

Table: Quorum Requirements

# of Distinct Remote Network Perspectives Used	# of Allowed non-Corroborations
2-5	1
6+	2

The number of remote Network Perspectives will increase as per the schedule outlined in Section 3.2.2.9 of the TLS Baseline Requirements. By no later than 15 December 2026, DigiCert will perform MPIC using at least five (5) Network Perspectives. If these requirements and the requirements described in the Quorum Requirements Table are not satisfied, then the Certificate cannot be issued.

3.2.3. Authentication of Individual Identity

DigiCert does not issue TLS where a natural person is named in the subject.

3.2.4. Non-Verified Subscriber Information

Not Applicable.

3.2.5 Validation of Authority

DigiCert shall verify that the natural person submitting the certificate request, approving the certificate request, or otherwise acting for the applicant or subscriber is authorized to do so.

3.2.6 Criteria for Interoperation

DigiCert may provide interoperation services to certify a non-DigiCert CA, allowing it to interoperate with the DigiCert PKI.
For such interoperation services to be provided the following criteria must be met:
• DigiCert will perform due diligence on the CA;
• A formal contract must be entered into with DigiCert, which includes a ‘right to audit’ clause; and
• The CA must operate under a CPS that meets DigiCert requirements.

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. Onion Domain Validation

The Domain Name must contain at least two Domain Labels, where the rightmost Domain Label is "onion", and the Domain Label immediately preceding the rightmost "onion" Domain Label is a valid Version 3 Onion Address.

DigiCert validates the applicant control over the .onion service by using a certificate request signed with the .onion service private key and containing the required CA and applicant nonce attributes.

3.3. Identification and Authentication for Re-Key Requests

3.3.1. Identification and Authentication for Routine Re-Key

For routine re-key requests, DigiCert shall authenticate the request and determine whether existing validation information may be reused or whether fresh validation is required under the applicable requirements and DigiCert documented procedures.

3.3.2. Identification and Authentication for Re-Key After Revocation

Re-key requests are not accepted for revoked Certificates.

3.4. Identification and Authentication for Revocation Requests

All revocation requests are authenticated by DigiCert or the RA responsible for issuing the certificate. See Section 4.9 for detailed certificate revocation procedures.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Either the applicant or an individual authorized to request certificates on behalf of the applicant may submit certificate requests. Applicants are responsible for any data that they or their agents supply to DigiCert.

4.1.2 Enrolment Process and Responsibilities

Applicants shall provide complete and accurate information required for the generation and issuance of certificates. By agreeing to the applicable agreement, terms of use, and privacy documentation, the applicant also agrees to the underlying policy documents governing the relevant certificate service. If required information is missing, incomplete, inaccurate, or produces an adverse validation result, DigiCert may reject the application. DigiCert does not issue certificates to entities that are prohibited by applicable sanctions, denied-party restrictions, or other legal or policy constraints. An internal database of previously revoked

Certificates and previously rejected Certificate requests are maintained which may be used to identify subsequent suspicious Certificate requests.

4.2. Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

After receiving a certificate application, DigiCert or an authorized RA shall perform the identification and authentication steps applicable to the requested certificate class and profile. DigiCert implements procedures that identify and require additional verification activity for high-risk certificate requests before approval, as reasonably necessary to ensure that such requests are properly verified. If a delegated third party fulfills any portion of DigiCert obligations under this section, DigiCert shall verify that the delegated third-party process provides at least the same level of assurance as DigiCert own process.

Subject Identity Information that has been validated according to Section 3.2 of this document may be reused for up to 398 days. Domain name and IP address validation data may be reused for up to 200 days for certificates issued before 15 March 2027; up to 100 days for certificates issued on or after 15 March 2027 and before 15 March 2029; and up to 10 days for certificates issued on or after 15 March 2029.

4.2.1.1 Requirements for Re-use of Existing Documentation

Except for reissuance of an EV TLS for existing Subscribers, the age of all data used to support issuance (before revalidation is required) shall not exceed the limits described below. The period specified shall begin to run on the date the information was collected.

OV TLS
Subject identity validation may not be relied upon for OV TLS Certificates if the validation was collected more than 398 days prior.

Domain Validation
Domain validation may be re-used for 200 days unless otherwise specified in Section 3.2.2.4.

Certificates issued on or after March 15, 2027 may not rely on existing domain validation older than 100 days.

Certificates issued on or after March 15, 2029 may not rely on existing domain validation older than 10 days.

4.2.2. Approval or Rejection of Certificate Applications

DigiCert shall approve a certificate application only after successful completion of all applicable validation checks.

DigiCert may reject or refuse to issue any Certificate at its sole discretion. Rejected Applicants may re-apply.

DigiCert shall not issue Certificates containing Internal Names or Reserved IP Addresses, as such names cannot be validated according to Section 3.2.2.4 or Section 3.2.2.5. DigiCert shall not issue Certificates containing Domain Names that end in an IP Reverse Zone Suffix.

4.2.2.1 CAA Record Processing

DigiCert checks DNS records for the existence of a CAA record for each dNSName in the subjectAltName extension of the certificate to be issued. DigiCert processes the issue, issuewild, and iodef CAA property tags

as specified in RFC 8659.

Certificates passing the CAA check are issued within the Time to Live (TTL) of the CAA record, or eight (8) hours, whichever is greater. DigiCert does not dispatch reports of issuance requests to the contact(s) listed in an "iodef" property tag.

DigiCert treats a record-lookup failure as permission to issue if the failure is outside DigiCert infrastructure, the lookup has been retried at least once, and DigiCert has confirmed that the domain is “Insecure” as defined in RFC 4035 Section 4.3

The CA identifiers that DigiCert recognizes are:
digicert.com;
digicert.ne.jp;
cybertrust.ne.jp;
symantec.com;
thawte.com;
geotrust.com;
quovadisglobal.com;
rapidssl.com;
digitalcertvalidation.com;
volusion.digitalcertvalidation.com;
stratossl.digitalcertvalidation.com;
intermediatecertificate.digitalcertvalidation.com;
1and1.digitalcertvalidation.com;
amazon.com;
amazontrust.com;
awstrust.com;
amazonaws.com;
www.digicert.com;
pkioverheid.nl.

4.2.2.1.1 CAA Multi-Perspective Issuance Corroboration

Some methods relied upon for validating the Applicant’s ownership or control of the subject domain(s) or IP address(es) to be listed in a certificate require CAA records to be retrieved and processed from additional remote Network Perspectives before Certificate issuance. To corroborate the Primary Network Perspective, a remote Network Perspective’s CAA check response must be interpreted as permission to issue, regardless of whether the responses from both Perspectives are byte-for-byte identical. Additionally, DigiCert may consider the response from a remote Network Perspective as corroborating if one or both of the Perspectives experience an acceptable CAA record lookup failure, as defined in Section 4.2.2.1.

4.2.2.1.2 CAA Parameters

By no later than March 15th 2027, DigiCert will process the accounturi and validationmethods parameters as specified in RFC 8657.

4.2.2.1.3 DNSSEC Validation of CAA Records

DigiCert performs DNSSEC validation back to the IANA DNSSEC root trust anchor on DNS queries associated with CAA record lookups performed by the primary network perspective where the applicable requirements require such validation. DNSSEC validation errors cannot be treated as permission to issue.

The DNS resolver used for all DNS queries associated with CAA record lookups performed by the Primary Network Perspective must:
• perform DNSSEC validation using the algorithm defined in RFC 4035, Section 5; and
• support NSEC3 as defined in RFC 5155; and
• support SHA-2 as defined in RFC 4509 and RFC 5702; and
• properly handle the security concerns enumerated in RFC 6840, Section 4.

4.2.3. Time To Process Certificate Applications

Reasonable efforts are made to confirm Certificate Application information and issue a Certificate. To avoid delays, it is the responsibility of the Applicant to provide the necessary details and documentation in a timely manner.

4.3. Certificate Issuance

DigiCert shall issue a certificate only after completion of all applicable validation, authorization, and technical checks.

4.3.1. CA Actions During Certificate Issuance

Certificate issuance is governed by the practices described in this CP/CPS and any requirements imposed by applicable standards and supervisory frameworks. DigiCert maintains documented controls governing issuance authorization, issuance event logging, separation of duties where applicable, and generation of final certificate content.

4.3.1.1. Manual authorization of certificate issuance for Root CAs

Certificate issuance by a root CA requires at least two individuals authorized by DigiCert, one of whom deliberately commands the root CA to perform a certificate signing operation. Databases and CA processes occurring during certificate issuance are protected against unauthorized modification.

4.3.1.2. Linting of to-be-signed Certificate content

DigiCert implements a linting process to test the technical conformity of each to-be-signed certificate artifact before signing it.

4.3.1.3. Linting of issued Certificates

DigiCert may use a Linting process to test issued Certificates as part of self-audit, quality-control, and continuous-improvement processes to verify technical accuracy independently of earlier pre-issuance linting.

4.3.2. Notification To Subscriber by the CA of Issuance of Certificate

DigiCert delivers instructions via email to the mailbox address designated by the Certificate Requester during the application process but may use other methods deemed at least equally secure.

4.4. Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

A Certificate is deemed accepted when the Subscriber downloads, installs, or uses the Certificate, or otherwise fails to object to the Certificate within the period stated in the applicable agreement. Subscribers must review Certificate contents and promptly request revocation if any information is inaccurate.

4.4.2. Publication of the Certificate by the CA

DigiCert publishes end-entity certificates by delivering them to the Subscriber.

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

RAs and other entities involved in the enrolment process may be informed of issuance.

4.5. Key Pair and Certificate Usage

4.5.1. Subscriber Private Key and Certificate Usage

Certificates shall be used lawfully and in accordance with this CP/CPS and the applicable Subscriber Agreement. Subscribers are obligated 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 only in accordance with their intended purpose.

4.5.2. Relying Party Public Key and Certificate Usage

A party seeking to rely on a certificate issued within the DigiCert PKI agrees to and accepts the Relying Party Agreement.

4.6. Certificate Renewal

4.6.1. Circumstance For Certificate Renewal

DigiCert may renew a certificate if the associated key has not reached the end of its validity period, the Subscriber and attributes are consistent, and the associated private key remains uncompromised. DigiCert allows for renewal through its automation tools, GUIs and API.

4.6.2. Who May Request Renewal

Only the Certificate Subject or an authorized representative of the Certificate Subject may request renewal of the Subscriber certificates.

4.6.3. Processing Certificate Renewal Requests

Renewal application requirements and procedures are the same as those used during the original certificate issuance, but DigiCert may use previously collected information that is still within the limits of reuse allowed by the relevant requirements. DigiCert will revalidate any information that is older than the periods specified in applicable standards for the relevant certificate policy and may refuse to renew a certificate if it cannot verify rechecked information.

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

4.7.1. Circumstance For Certificate Re-Key

Certificates may be re-keyed upon request. If the prior certificate is replaced and should no longer be used or relied upon, DigiCert revokes the prior certificate using the appropriate CRLReason. Where simultaneous validity is permitted by applicable requirements and agreement, DigiCert may leave the prior certificate valid until expiration or separate revocation.

4.7.2. Who May Request Certification of a New Public Key

DigiCert will accept re-key requests from the Subject of the certificate, an authorized representative for an organizational certificate, or the nominating RA. DigiCert may initiate a certificate re-key at the request of the Certificate Subject or at DigiCert own discretion.

4.7.3. Processing Certificate Re-Keying Requests

If the identity and domain information in a certificate have not changed, DigiCert may issue a re-key certificate based on a newly provided CSR and may re-use existing verification and authentication information in accordance with Section 3.3 unless DigiCert believes that the information has become inaccurate.

Re-keying MAY be required following changes to PQC algorithms, implementations, Microsoft requirements, identified cryptographic weakness, or interoperability requirements.

4.7.4. Notification of New Certificate Issuance to Subscriber

See Section 4.3.2.

4.7.5. Conduct Constituting Acceptance of a Re-Key Certificate

See Section 4.4.1.

4.7.6. Publication Of the Re-Key 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

DigiCert may modify a certificate where the changed information has been revalidated and the resulting certificate remains compliant with the applicable product profile, Microsoft Requirements, and this CP/CPS.

4.8.2. Who May Request Certificate Modification

See Section 4.1.1.

4.8.3. Processing Certificate Modification Requests

After receiving a request for modification, DigiCert verifies any information that will change in the modified certificate. DigiCert will only issue the modified certificate after completing the verification process on all modified information.

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

4.9.1. Circumstances For Revocation

Revocation of a PQC certificate permanently ends the operational period of the certificate prior to the certificate reaching the end of its stated validity period.

Prior to revoking a certificate, DigiCert verifies that a revocation request was initiated by an entity entitled to request revocation under Section 4.9.2. Other parties may submit Certificate Problem Reports to DigiCert to report reasonable cause to revoke the certificate

4.9.1.1. Reasons for Revoking a Subscriber Certificate

Circumstances for revocation within 24 hours
DigiCert will revoke a Certificate within 24 hours after receipt and use the corresponding CRLReason in

accordance with Section 7.2, confirming one or more of the following occurred:

1. The Subscriber requests in writing that DigiCert revoke the Certificate but does not specify a reason (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);
2. The Subscriber notifies DigiCert that the original Certificate request was not authorized and does not retroactively grant authorisation (CRLReason #9, privilegeWithdrawn);
3. DigiCert obtains evidence that the Subscriber's Private Key in the Certificate suffered a Key Compromise (CRLReason #1, keyCompromise);
4. DigiCert is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key in the Certificate (including but not limited to those identified in Section 6.1.1.1) (CRLReason #1, keyCompromise);
5. DigiCert obtains evidence that the validation of domain authorisation or control for any FQDN or IP address in the Certificate should not be relied upon, including cases where the CA failed to perform CAA checking correctly or where issuance was not permitted according to Section 4.2.2.1 (CRLReason #4, superseded).
6. Microsoft directs DigiCert to discontinue or replace an affected certificate.

Circumstances for revocation within 5 days

Apart from Short-lived Subscriber Certificates, DigiCert may revoke a Certificate within 24 hours and will revoke a Certificate within 5 days after receipt and use the corresponding CRL Reason confirming that one or more of the following occurred:

1. DigiCert obtains evidence that the Certificate was misused and/or used outside the intended purpose as indicated by the relevant agreement (CRLReason #9, privilegeWithdrawn);
2. The Subscriber breached a material obligation under the CP/CPS or the relevant agreement (CRLReason #9, privilegeWithdrawn);
3. DigiCert confirms any circumstance indicating that use of a FQDN or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name registrant and the Applicant has terminated, or the Domain Name registrant has failed to renew the Domain Name) (CRLReason #5, cessationOfOperation);
4. DigiCert confirms that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate FQDN (CRLReason #9, privilegeWithdrawn);
5. DigiCert confirms a material change in the information contained in the Certificate (CRLReason #9, privilegeWithdrawn);
6. DigiCert determines or confirms that any of the information appearing in the Certificate is inaccurate (CRLReason #9, privilegeWithdrawn);
7. DigiCert right to issue Certificates under Microsoft PQC Pilot requirements expires or is revoked or terminated, unless DigiCert has made arrangements to continue maintaining the CRL Repository for a reason that is not otherwise required to be specified by this Section 4.9.1 (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL;
8. Revocation is required by this CP/CPS for a reason that is not otherwise required to be specified by this Section 4.9.1 (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL;
9. DigiCert 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);

Other Revocation Considerations

1. DigiCert shall maintain the capability to revoke any PQC TLS Pilot Certificate at its sole discretion;
2. The certificate is used outside the authorized Pilot scope;
3. An algorithm or parameter set is no longer considered suitable;
4. Microsoft directs DigiCert to discontinue or replace an affected certificate .

4.9.1.2. Reasons for Revoking a Subordinate CA Certificate

DigiCert will revoke an Issuing CA Certificate within seven (7) days after receipt and confirming one or more of the following occurred:

1. The Issuing CA requests revocation in writing;
2. The Issuing CA notifies DigiCert that the original Certificate request was not authorized and does not retroactively grant authorization;
3. DigiCert obtains evidence that the Issuing CA's Private Key corresponding to the Public Key in the Certificate suffered a key compromise;
4. DigiCert obtains evidence that the CA Certificate was misused and/or used outside the intended purpose as indicated by the relevant agreement;
5. DigiCert confirms that the CA Certificate was not issued in accordance with or that Issuing CA has not complied with the CP/CPS;
6. DigiCert determines that any of the information appearing in the CA Certificate is inaccurate or misleading;
7. DigiCert or the Issuing CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the CA Certificate;
8. DigiCert's or the Issuing CA's right to issue Certificates expires or is revoked or terminated, unless DigiCert has made arrangements to continue maintaining the CRL Repository;
9. Revocation is required by the DigiCert CP/CPS; or
10. The technical content or format of the CA Certificate presents an unacceptable risk to Application Software Vendors or Relying Parties.

In the event that an Issuing CA determines that its Certificates or the DigiCert PKI could become compromised and that revocation of Certificates is in the interests of the PKI, following remedial action, DigiCert may authorize the reissue of Certificates to Subscribers at no charge, unless the actions of the Subscribers were in breach of the DigiCert CP/CPS or other contractual documents.

4.9.2. Who Can Request Revocation

Any appropriately authorized party may request revocation of a Certificate. This may include a recognized representative of a Subscriber or the RA, the party that purchased the Certificate on behalf of a Subscriber, and the party that manages the Portal account to which the Certificate is tied. DigiCert may revoke a Certificate at its sole discretion, without receiving a request and without reason.

Third parties may request Certificate revocation for problems related to fraud, misuse, or compromise. Certificate revocation requests must identify the entity requesting revocation and specify the reason for revocation. DigiCert provides Anti-Malware Organizations, Subscribers, Relying Parties, Application Software Vendors, 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 at https://problemreport.digicert.com/ and other resources listed in Section 1.5.2.1.

4.9.3. Procedure for Revocation Request

DigiCert processes a revocation request as follows:

1. DigiCert logs the request or problem report and the reason for requesting revocation based on the list in Section 4.9.1, including contact information for 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, email, etc.).
3. If the request is authenticated as originating from the Subscriber or an authorized party, DigiCert revokes the Certificate based on the timeframes listed in 4.9.1 as listed for the reason for revocation.
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 24x7 ability to internally respond to revocation requests and Certificate problem reports at https://problemreport.digicert.com/ and other resources listed in Section 1.5.2.1. Subscribers may also revoke their Certificates via the DigiCert Portal.

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 depend on the reasons for revocation as described in this section.

4.9.5. Time Within Which CA Must Process the Revocation Request

Within 24 hours after receiving a Certificate problem report or revocation request, DigiCert investigates the facts and circumstances involved with the report and will provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate problem report.

After reviewing the facts and circumstances, DigiCert works with the Subscriber and any entity reporting the Certificate problem report or other revocation-related notice to establish whether or not the Certificate will be revoked, and if so, a date which DigiCert will revoke the Certificate. The period from receipt of the Certificate problem report or revocation-related notice to published revocation must not exceed the time frame set forth in Section 4.9.1. The date selected by DigiCert will consider the following criteria:

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);
2. The number of Certificate problem reports received about a particular Certificate or Subscriber;
3. 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 she didn't receive the goods she ordered); and
4. Relevant legislation.

The time used for the provision of revocation services is synchronized with UTC at least every 24 hours. 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.

4.9.6. Revocation Checking Requirement 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 responder listed in the certificate.

4.9.7. CRL Issuance Frequency

Subscriber Certificates
Updated CRLs are issued at least once every seven (7) days, and the value of the nextUpdate field is not more than ten (10) days beyond the value of the thisUpdate field. A new CRL is published within 24 hours of revoking a Certificate.

Subordinate CA
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.

4.9.8. Maximum Latency For CRL

No stipulation.

4.9.9. On-Line Revocation/Status Checking Availability

No stipulation.

4.9.10. On-line Revocation Checking Requirements

No stipulation.

4.9.11. Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12. Special Requirements Re Key Compromise

DigiCert uses commercially reasonable efforts to notify potential Relying Parties if it discovers or suspects the compromise of a Private Key. Reports to DigiCert of key compromise must include:

- 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.
- A valid email address so that you can receive confirmation of your problem report and associated Certificate revocations.

DigiCert will select the CRLReason code “keyCompromise” (value 1) upon discovery of such reason or as required by an applicable CP/CPS. Should a CA Private Key become compromised, the CA and all Certificates issued by that CA shall be revoked. DigiCert provides additional instructions and support for keyCompromise at https://problemreport.digicert.com/and other resources as indicated in Section 1.5.2.1 of this CP/CPS.

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.

4.9.13. Circumstances for Suspension

Suspension is not supported under this CP/CPS.

4.9.14. Who Can Request Suspension

Suspension is not supported under this CP/CPS.

4.9.15. Procedure For Suspension Request

Suspension is not supported under this CP/CPS.

4.9.16. Limits On Suspension Period

Suspension is not supported under this CP/CPS.

4.10. Certificate Status Services

4.10.1. Operational Characteristics

For Subscriber Certificates, revocation status information may be removed after certificate expiry where permitted by Applicable Requirements. Revocation information is retained and published as required by applicable standards, root-program policy, and this CP/CPS.

4.10.2. Service Availability

Certificate status services are available 24/7. DigiCert operates and maintains its CRL capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

DigiCert also maintains a continuous 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 Master Services Agreement to expire without renewal. Some terms of the Master Services Agreement and this CP/CPS may survive termination of the subscription service.

4.12. Key Escrow and Recovery

Key Escrow is not supported under this CP/CPS.

4.12.1. Key Escrow and Recovery Policy and Practices

Key Escrow is not supported under this CP/CPS.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

Key Escrow is not supported under this CP/CPS.

5. Facility, Management, and Operational Controls

This Section of the CP/CPS provides a high-level description of the security policies, physical and logical access control mechanisms, service levels, and personnel policies used by DigiCert to provide trustworthy and reliable CA operations.

5.1. Physical Controls

DigiCert manages and implements appropriate physical security controls to restrict access to the hardware and software used in connection with CA operations.

5.1.1. Site Location and Construction

DigiCert performs its CA operations from secure datacenters. The datacenters are equipped with logical and physical controls that make DigiCert's CA operations inaccessible to non-trusted personnel. DigiCert operates under a security policy designed to detect, deter, and prevent unauthorized access to the CA operations.

5.1.2. Physical Access

DigiCert permits entry to its secure datacenters only to security-cleared and authorized personnel, whose movements within the facility are logged and audited. Physical access is controlled by dual-factor authentication using a combination of physical access cards and biometric readers.

5.1.3. Power And Air-Conditioning

The datacenter has 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

The cabinets housing the CA systems are designed to prevent and protect against water exposure.

5.1.5. Fire Prevention and Protection

The datacenter is equipped with fire suppression mechanisms.

5.1.6. Media Storage

Media is protected from accidental damage, environmental hazards, unauthorized physical access, and from obsolescence/deterioration during the period that records are required to be retained. Backup files are created daily and are maintained either within the service operations area or in a secure off-site storage area.

5.1.7. Waste Disposal

Printed sensitive information is shredded on-site before disposal. All electronic media are physically destroyed or are overwritten multiple times to prevent the recovery of the data.

5.1.8. Off-Site Backup

An off-site location is used for the storage and retention of backup software and data. The off-site storage is available to authorized personnel 24x7 for the purpose of retrieving software and data; and has appropriate levels of physical security in place (i.e., software and data are stored in fire rated safes and containers which are located behind access-controlled doors in areas accessible only by authorized personnel).

5.2. Procedural Controls

5.2.1. Trusted Roles

Personnel acting in trusted roles include CA and RA system administration personnel, and personnel involved with identity vetting and the issuance and revocation of Certificates. The 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 operations. A list of personnel appointed to trusted roles is maintained and reviewed annually.

5.2.1.1. CA Administrators

The CA Administrator installs and configures the CA software, including key generation, key backup, and key management. The CA Administrator performs and securely stores regular system backups of the CA system. CA Administrators do not issue Certificates to Subscribers.

5.2.1.2. Registration Officers –Validation and Vetting Personnel

The Registration Officer role is responsible for issuing and revoking Certificates.

5.2.1.3. System Administrators/ System Engineers (Operator)

The System Administrator/System Engineer installs and configures system hardware, including servers, routers, firewalls, and network configurations. The System Administrator/System Engineer also keeps critical systems updated with software patches and other maintenance needed for system stability and recoverability.

5.2.1.4. Internal Auditors

Internal Auditors are responsible for reviewing, maintaining, and archiving audit logs and performing or overseeing internal compliance audits to determine if DigiCert is operating in accordance with this CP/CPS and the relevant requirements.

5.2.1.5. RA Administrators

RA Administrators are responsible for the RA certificate management systems.

5.2.1.6. Security Officers

The Security Officer is responsible for administering and implementing security practices.

5.2.2. Number Of Persons Required Per Task

DigiCert applies dual control, multi-person control, or equivalent segregation measures for sensitive operations where appropriate to the risk, including activating CA Private Keys, generating a CA Key Pair, or creating a backup of a CA Private Key and other high-impact certificate system functions.

The Internal Auditor may serve to fulfil the requirement of multiparty control for physical access to the CA system but not logical access.

5.2.3. Identification and Authentication for Each Role

Persons filling trusted roles must undergo an appropriate security screening procedure commensurate to their role and access privileges are configured using the “least privileges” principle for the role. All personnel are required to authenticate themselves to systems before they are allowed access to 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 identifies roles and activities that require separation of duties and implements those controls to reduce the risk of error, fraud, or unauthorized action.

5.3. Personnel Controls

5.3.1. Qualifications, Experience, and Clearance Requirements

The DCPA is responsible and accountable for DigiCert PKI operations and ensures compliance with this CP/CPS. Prior to the engagement of any person in the Certificate management process, DigiCert verifies the identity and trustworthiness of such person. DigiCert determines that all individuals assigned to trusted roles perform their prospective job responsibilities competently and satisfactorily as required.

5.3.2. Background Check Procedures

DigiCert verifies the identity of each individual appointed to a trusted role and performs a background check prior to allowing such person to act in a trusted role. DigiCert's human resources department verifies the individual's identity using government-issued photo identification (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 a combination of the following as required; verification of individual identity, employment history, education, character references, social security number, previous residences, driving records, professional references, and criminal background. Criminal history reviews shall be conducted in accordance with applicable laws.These procedures are subject to any limitations on background checks imposed by local law. To the extent one of the requirements imposed by this Section cannot be met by DigiCert due to a prohibition or limitation in local law, DigiCert utilizes a substitute investigative technique permitted by law that provides substantially similar information, including but not limited to obtaining a background check performed by the applicable governmental agency.

5.3.3. Training Requirements

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

1. Basic 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

A record of all trainings is maintained. Registration Officers must have the minimum skills required to perform the validation process and must demonstrate those skills by passing an exam validating and approving the issuance of the corresponding certificates.

5.3.4. Retraining Frequency and Requirements

Personnel must maintain their skill levels 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

Not applicable.

5.3.6. Sanctions for Unauthorized Actions

DigiCert employees and agents failing to comply with this CP/CPS, whether through negligence or malicious intent, are subject to internally maintained processes specifying guidance on administrative or disciplinary actions, up to and including termination of employment or agency and criminal sanctions.

5.3.7. Independent Contractor Requirements

Independent contractors who are assigned to perform trusted roles are subject to the duties and requirements specified for such roles in this Section 5.3 and are subject to sanctions stated above in Section 5.3.6.

5.3.8. Documentation Supplied to Personnel

Personnel are supplied with the documentation, policies, procedures, and guidance needed to perform their assigned roles correctly and securely.

5.4. Audit Logging Procedures

5.4.1. Types of Events Recorded

DigiCert records details of the actions taken to process a PQC Pilot Certificate request and to issue a Certificate, including all information generated and documentation received in connection with the Certificate request. DigiCert logs the following events:

- CA Certificate and key lifecycle management events:
    - PQC key generation, backup, storage, recovery, archival, and destruction.
    - Certificate requests, renewal, re-key requests, and revocation.
    - Approval and rejection of Certificate requests.
    - Cryptographic configuration changes.
    - Generation of Certificate Revocation Lists (CRLs).
    - Introduction of new PQC Pilot Certificate Profiles and retirement of existing profiles.
- Subscriber Certificate lifecycle management events, including:
    - Certificate requests, renewal, re-key requests, and revocation.
    - All verification activities stipulated in the Applicable Requirements and this CP/CPS. Records include, at a minimum:
        - The information being validated.
        - The Authorization Domain Name (ADN) used.
        - The validation method used.
    - Approval and rejection of Certificate requests.
    - Issuance of Certificates.
    - Generation of Certificate Revocation Lists (CRLs).
    - Multi-Perspective Issuance Corroboration (MPIC) attempts from each Network Perspective, minimally recording:
        - An identifier that uniquely identifies the Network Perspective used.
        - The attempted domain name and/or IP address.
        - The result of the attempt (for example, "domain validation pass/fail" or "CAA permission/prohibition").
    - Multi-Perspective Issuance Corroboration quorum results for each attempted domain name or IP address represented in a Certificate request (for example, "3/4", meaning that three (3) out of four (4) attempted Network Perspectives corroborated the determinations made by the Primary Network Perspective).
- 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 PKI System.
    - System crashes, hardware failures, and other anomalies.
    - Relevant firewall and router activities.
    - Entries to and exits from the CA facility.

- DigiCert event logs include at least the following:

    - Date and time of the record.
    - Identity of the entity making the journal record (when applicable).
    - Details of the record.

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

At least once every 31 days, personnel in a Trusted Role review the logs generated by DigiCert's systems, makes system and file integrity checks, and conducts a vulnerability assessment.

The administrator may perform the checks using automated tools. During these checks, the administrator (1) checks whether anyone has tampered with the log, (2) scans for anomalies or specific conditions, including any evidence of malicious activity, and (3) if necessary, prepares a written summary of the review.

Any anomalies or irregularities found in the logs are investigated. The summaries may include recommendations to DigiCert's operations management committee and are made available to auditors upon request. DigiCert documents any actions taken because of a review.

5.4.3. Retention Period for Audit Log

Audit logs relating to the Certificate lifecycle are retained for a period no less than two (2) years for TLS Certificates:

- CA Certificate and key lifecycle management event records must be retained until the later of:
- Destruction of the CA Private Key; or
- Revocation or expiration of the final CA Certificate in the set of Certificates that:
    - Have an X.509v3 `basicConstraints` extension with the `cA` field set to `TRUE`;
- Subscriber Certificate lifecycle management event records must be retained until the Subscriber Certificate expires.

- Security event records must be retained after the event occurred.

Audit logs are made available to auditors upon request.

5.4.4. Protection of Audit Log

Audit logs are protected against unauthorized access, alteration, deletion, and destruction through technical, procedural, and administrative controls for the duration of the retention period for audit logs. The audit logs 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 daily. Audit logs are backed up on a weekly basis to an offsite location.

5.4.6. Audit Collection System (Internal vs. External)

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

5.4.7. Notification to Event-Causing Subject

DigiCert does not ordinarily provide routine notification to the subject of an event solely because the event was logged, except where notification is required by policy, contract, law, or incident-handling procedure.

5.4.8. Vulnerability Assessment

DigiCert performs monthly vulnerability scans on its PKI systems and infrastructure. Identified vulnerabilities are rated and addressed based on the Common Vulnerability Scoring System (CVSS).

DigiCert's audit log monitoring tools alert the appropriate personnel of any events, such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses.

DigiCert performs annual risk assessments that identify and assess reasonably foreseeable threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate data or Certificate issuance process. DigiCert also routinely assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that DigiCert has in place to control risks identified in risk assessments. DigiCert's Internal Auditors review the security audit data checks for continuity.

Based on the risk assessment, DigiCert develops, implements, and maintains a security plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to manage and control the risks identified during the risk assessment, commensurate with the sensitivity of the Certificate data and management processes.

5.5. Records Archival

5.5.1. Types of Records Archived

DigiCert archives records related to the security of their Certificate Systems, Certificate Management Systems, Root CA Systems, and Delegated Third Party Systems, including event records and documentation related to their verification, issuance, and revocation of Certificate requests and Certificates.

DigiCert archives records relating to:
• CA Certificate and key lifecycle management event records;
• Subscriber Certificate lifecycle management event records and
• Security event records.

DigiCert retains the following information in its archives (as such information pertains to DigiCert's CA operations):

1. Accreditations of DigiCert;
2. CP/CPS versions;
3. Contractual obligations and other agreements concerning the operation of the CA;
4. System and equipment configurations, modifications, and updates;
5. Rejection or acceptance of a Certificate request;
6. Certificate issuance, rekey, renewal, and revocation requests;
7. Sufficient identity authentication data to satisfy the identification requirements of Section 3.2, including information about telephone calls made for verification purposes;
8. Any documentation related to the receipt or acceptance of a Certificate or token;
9. Subscriber Agreements;
10. Issued Certificates;
11. A record of Certificate re-keys;
12. Data or applications necessary to verify an archive's contents;
13. Compliance auditor reports;
14. Changes to DigiCert audit parameters;
15. Any attempt to delete or modify audit logs;
16. CA Key generation and destruction;
17. Access to Private Keys for key recovery purposes;
18. Export of Private Keys;
19. Approval or rejection of a revocation request;
20. Appointment of an individual to a trusted role;
21. Destruction of a cryptographic module;
22. Certificate compromise notifications;
23. Remedial action taken as a result of violations of physical security; and
24. Violations of the CP/CPS.

5.5.2. Retention Period for Archive

Audit logs relating to the Certificate lifecycle are retained as archive records for a period of no less than two (2) years, starting from the destruction of the CA Private Key, or revocation, or expiration of the Certificate.

For at least two (2) years, DigiCert retains the following:

1. All archived documentation related to the security of Certificate Systems, Certificate Management Systems, Root CA Systems and Delegated Third Party Systems; and
2. All archived documentation relating to the verification, issuance, and revocation of certificate requests and Certificates after the later occurrence of:

a. such records and documentation were last relied upon in the verification, issuance, or revocation of certificate requests and Certificates; or
b. the expiration of the Subscriber Certificates relying upon such records and documentation.

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 backed up at least annually, 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

Towards the end of the CA Private Key's lifetime, DigiCert ceases using its expiring CA Private Key to sign Certificates (well in advance of expiration) and uses the old Private Key only to sign CRLs associated with that key. A new CA signing Key Pair is commissioned and all subsequently issued Certificates and CRLs are signed with the new private signing key. Both the old and the new Key Pairs may be concurrently active.

5.7. Compromise and Disaster Recovery

5.7.1. Incident and Compromise Handling Procedures

5.7.1.1. Incident Response and Disaster Recovery Plans

DigiCert maintains internal incident response procedures to guide personnel in response to security incidents, natural disasters, and similar events that may give rise to system compromise. These procedures include notification to Application Software Vendors, Subscribers, and Relying Parties as appropriate in the event of a disaster, security compromise, or business failure.

DigiCert reviews, tests, and updates its incident response plans and procedures on a periodic basis.

5.7.1.2. Mass Revocation Plans

DigiCert maintains a mass revocation plan to ensure a rapid, consistent, and reliable response to large-scale certificate revocation events. The Mass Revocation Plan is tested, reviewed, and updated at least annually. Lessons learned during testing are incorporated into the plan to ensure preparedness in an evolving environment.The Mass Revocation Plan is made available to DigiCert's auditors upon request.

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

DigiCert makes system backups on a weekly basis and maintains backup copies of its CA Private Keys, which are stored in a secure, separate location.

If it is discovered that any computing resources, software, or data operations have been compromised, DigiCert assesses the threats and risks that the compromise presents to the integrity or security of its operations or those of affected parties. If continuing an operation could pose a significant risk to Relying Parties or Subscribers, DigiCert suspends such operation until it determines that the risk is mitigated.

5.7.3. Entity Private Key Compromise Procedures

If DigiCert suspects that one of its CA Private Keys has been compromised, a response team will be convened to assess the incident and take appropriate action.

DigiCert maintains procedures for suspected or confirmed compromise of CA or other entity private keys, including investigation, issuance suspension where appropriate, revocation, notification, and recovery actions.

5.7.4. Business Continuity Capabilities After a Disaster

To maintain the integrity of its services, DigiCert implements data backup and recovery procedures as part of its Business Continuity Management Plan (BCMP). Stated goals of the BCMP are to ensure that Certificate status services be only minimally affected by any disaster involving DigiCert's primary facility and that DigiCert be capable of maintaining other services or resuming them as quickly as possible following a disaster.

DigiCert periodically reviews, tests, and updates the BCMP and supporting procedures.

5.8. CA or RA Termination

- Unless otherwise addressed in an applicable agreement between DigiCert and a counterparty, before terminating its CA or RA activities, DigiCert may:

    1. Notify relevant government and certification bodies as required under applicable laws and regulations.
    2. Provide notice of the termination by:
        - Sending email notifications to customers and Application Software Vendors; and
        - Posting notice on the DigiCert website.
    3. Transfer all responsibilities to a qualified successor entity.

- Unless otherwise addressed in an applicable agreement between DigiCert and a counterparty, if a qualified successor entity does not exist, DigiCert may:

    1. Transfer those functions capable of being transferred to a reliable third party and arrange for the preservation of all relevant records with:
        - A reliable third party; or
        - A government, regulatory, or legal body with appropriate authority.
    2. Revoke all Certificates that remain unrevoked and unexpired as of the date specified in the termination notice and publish final Certificate Revocation Lists (CRLs).
    3. Destroy all Private Keys.
    4. Make any other arrangements necessary to ensure compliance with this CP/CPS.

- Arrangements have been made to cover the costs associated with fulfilling these requirements in the event that DigiCert becomes bankrupt or is otherwise unable to meet these obligations.

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

DigiCert CA Key Pairs are generated by multiple trusted individuals acting in trusted roles and using a cryptographic hardware device as part of scripted key generation ceremony in the environments described in Section 5.1 and logged in accordance with Section 5.4.

6.1.1.2. RA Key Pair Generation

No stipulation.

6.1.1.3. Subscriber Key Pair Generation

DigiCert never creates key pairs for TLS Certificates.

DigiCert will reject a Certificate request if any of the following conditions are identified:

1. The Key Pair does not meet the requirements specified in Section 6.1.5 and/or Section 6.1.6.
2. There is clear evidence that the method used to generate the Private Key was flawed.
3. DigiCert is aware of a demonstrated or proven method that exposes the Applicant's Private Key to compromise.
4. DigiCert has previously been notified that the Applicant's Private Key has suffered a Key Compromise.

6.1.2. Private Key Delivery to Subscriber

DigiCert does not generate private keys for TLS Certificates.

6.1.3. Public Key Delivery to Certificate Issuer

Not Applicable.

6.1.4. CA Public Key Delivery to Relying Parties

Not Applicable.

6.1.5. Key Sizes

- Root certificates MUST use ML-DSA-87.
- ML-DSA-44 and ML-DSA-65 MAY be used for Subordinate CA or leaf certificates.

6.1.6. Public Key Parameters Generation and Quality Checking

DigiCert validates the key and associated parameters submitted in each certificate request before issuance.

6.1.7. Key Usage Purposes (As Per X.509 V3 Key Usage Field)

Key usage bits and extended key usages are specified in the profiles.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic Module Standards and Controls

The PQC TLS Pilot does not specify the use of HSMs.

6.2.2. Private Key (N out of M) Multi-Person Control

DigiCert's authentication mechanisms are protected securely when not in use and may only be accessed by actions of multiple trusted persons. Backups of CA Private Keys are securely stored and require two-person access. Re-activation of a backed-up CA Private Key (unwrapping) requires the same security and multi-person control as when performing other sensitive CA Private Key operations.

6.2.3. Private Key Escrow

DigiCert does not escrow its CA signature keys.

6.2.4. Private Key Backup

The PQC TLS Pilot does not specify the use of HSMs.

When keys are transferred to other media for backup and disaster recovery purposes, the keys are transferred and stored in an encrypted form. The Key Pairs are backed up by multiple trusted individuals using a cryptographic hardware device as part of scripted key backup process.

6.2.5. Private Key Archival

DigiCert does not archive CA Certificate 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 entity, then DigiCert will mandate revocation of all certificates that include the Public Key corresponding to the communicated Private Key.

6.2.7. Private Key Storage on Cryptographic Module

No stipulation.

6.2.8. Method of Activating Private Key

Activation data entry is protected from disclosure.

6.2.9. Method of Deactivating Private Key

No stipulation.

6.2.10. Method of Destroying Private Key

No stipulation.

6.2.11. Cryptographic Module Rating

No stipulation.

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival

Not Applicable.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

Certificate Type	Maximum Validity
Root Certificates	1 year
Subordinate CA Certificates	1 year
Leaf Certificates	90 days

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

No stipulation.

6.4.2. Activation Data Protection

Activation data is protected against unauthorized disclosure, modification, and use.

6.4.3. Other Aspects of Activation Data

DigiCert maintains procedures governing activation-data lifecycle matters, including change, recovery where permitted, and destruction.

6.5. Computer Security Controls

DigiCert has a formal Information Security Policy that documents the policies, standards and guidelines relating to information security. This Information Security Policy has been approved by the DCPA and is communicated to all employees.

6.5.1. Specific Computer Security Technical Requirements

DigiCert applies specific technical security requirements for in-scope systems, including access control, authentication, hardening, monitoring, malware defenses, secure administration, vulnerability management, and network protection appropriate to the system function and risk.

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.

6.5.2. Computer Security Rating

DigiCert designs, operates, and assesses its computer security environment in accordance with the applicable audit criteria, policy requirements, and risk-management expectations.

6.6. Life Cycle Technical Controls

6.6.1. System Development Controls

DigiCert maintains controls governing design, acquisition, development, testing, approval, and deployment of systems used in support of certificate services.
When Linting software developed by 3rd parties is used, DigiCert monitors for updates to ensure that it can be implemented within 3 months of the release.

6.6.2. Security Management Controls

DigiCert has mechanisms in place to control and continuously monitor the security-related configurations of its CA systems. The maximum interval between consecutive checks of CA systems for compliance, integrity, and security is six (6) months. When loading software onto a CA system, DigiCert verifies that the software is the correct version and is supplied by the vendor free of any modifications.

6.6.3. Life Cycle Security Controls

DigiCert applies security controls throughout the system life cycle, from initial design through decommissioning.

6.7. Network Security Controls

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

6.8. Time-stamping

No stipulation.

7. Certificate, CRL, and OCSP Profiles

DigiCert meets the technical requirements set forth in this CP/CPS.

7.1. Certificate Profile

7.1.1. Version Number(s)

Certificates issued under this CP/CPS are X.509 version 3 Certificates.

7.1.2. Certificate Extensions

PQC root certificates MUST include the EKU extension and MUST mark the EKU extension as critical.

The EKU extension MUST contain only the EKU OID or OIDs corresponding to the approved TLS authentication use case for that root:
• Server Authentication only: serverAuth (1.3.6.1.5.5.7.3.1)
• Client Authentication only: clientAuth (1.3.6.1.5.5.7.3.2)
• Server Authentication combined with Client Authentication:
o serverAuth (1.3.6.1.5.5.7.3.1)
o clientAuth (1.3.6.1.5.5.7.3.2)

7.1.3. Algorithm Object Identifiers

Certificates are signed using the algorithms allowed by the PQC Pilot Program.

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 and/or any other indication that the value or field is absent, incomplete, or not applicable.

7.1.5. Name Constraints

DigiCert may use nameConstraints when appropriate.

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.

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

7.1.7. Usage Of Policy Constraints Extension

Not applicable.

7.1.8. Policy Qualifiers Syntax and Semantics

Not applicable.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2. CRL Profile

7.2.1. Version number(s)

CRLs must be version 2 CRLs that conform to RFC5280.

7.2.2. CRL and CRL Entry Extensions

Where a reasonCode extension is present, DigiCert sets the reasonCode to the reason that most accurately reflects the revocation circumstance described in Section 4.9.1 and Section 7.2.2.1.

If a CRL entry is for a Root CA or Subordinate CA Certificate, the reasonCode extension shall be present and must not be unspecified (0) or certificateHold(6).

Code	Description	TLS Permitted
0	Unspecified; if permitted, the `reasonCode` extension should just be omitted.	Yes, but not for CA certificates
1	`keyCompromise`	Yes
2	`cACompromise`	Yes
10	`aACompromise`	No
9	`privilegeWithdrawn`	Yes
5	`cessationOfOperation`	Yes
3	`affiliationChanged`	Yes
4	`superseded`	Yes
6	`certificateHold`	No
7	Value 7 is not used	No
8	`removeFromCRL`	No

7.2.2.1. 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 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 in the Certificate; or
• The Certificate Subscriber requests that DigiCert revoke the Certificate for this reason, with the scope of revocation being described below.

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 authorisation.

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 authorisation 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 this CP/CPS or Microsoft's PQC Pilot Program. 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 authorisation or compliance issues other than those related to keyCompromise or privilegeWithdrawn.

Otherwise, the superseded CRLReason is not used.

7.3. OCSP Profile

OCSP services are onot provided for the PQC TLS Pilot.

7.3.1. Version Number(s)

Not applicable.

7.3.2. OCSP Extensions

Not applicable.

8. Compliance Audit and Other Assessments

The operation of the PQC TLS Pilot hierarchy and its corresponding certificate issuance are not included in an independent compliance audit.

8.1. Frequency or Circumstances of Assessment

No stipulation.

8.2. Identity/Qualifications of Assessor

No stipulation.

8.3. Assessor’s relationship to assessed Entity

No stipulation.

8.4. Topics Covered by Assessment

No stipulation.

8.5. Actions Taken as a Result of Deficiency

No stipulation.

8.6. Communication of Results

No stipulation.

8.7. Self-Audits

No stipulation.

9. Other Business and Legal Matters

9.1. Fees

9.1.1. Certificate Issuance or Renewal Fees

DigiCert charges fees in connection with verification, certificate issuance and renewal. DigiCert may change its pricing for future purchases 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

DigiCert or Issuing CAs under the DigiCert hierarchy may establish a refund policy, details of which may be contained in relevant contractual agreements.

9.2. Financial Responsibilities

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

DigiCert keeps the following types of information confidential and maintains reasonable controls to prevent the exposure of such records to non-trusted personnel.

- Private Keys;
- Activation data used to access Private Keys or to gain access to the CA system;
- Business continuity, incident response, contingency, and disaster recovery plans;
- Other security practices used to protect the confidentiality, integrity, or availability of information;
- Information held by DigiCert as private information in accordance with Section 9.4;
- Audit logs and archive records; and
- 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).

Any personal or corporate information held by Issuing CAs related to a Subscriber's application and the issuance of Certificates is considered confidential and will not be released without the prior consent of the relevant holder, unless required otherwise by law or to fulfil the requirements of this CP/CPS.

9.3.2. Information Not Within the Scope of Confidential Information

Information appearing in Certificates or stored in the Repository is considered public and not within the scope of confidential information, unless statutes or special agreements so dictate.

9.3.3. Responsibility to Protect Confidential Information

DigiCert 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 collects and processes personal information in accordance with its internal Data Privacy Framework Policy and the privacy notices posted on its website, including its Global Privacy Notice and Remote Identity Verification Policy. Additional privacy information is available at https://www.digicert.com/privacy-center.

9.4.2. Information Treated as Private

DigiCert treats all personal information related to a Certificate or CRL as confidential information. DigiCert protects all confidential information using industry-recommended safeguards and in accordance with applicable data protection laws.

9.4.3. Information Deemed Not Private

Publicly available information related to certificates and CRLs are not considered confidential. This CP/CPS is a public document and therefore is not treated as confidential.

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 of applicable data protection laws. All sensitive information is securely stored and protected against unauthorized disclosure.

9.4.5. Notice And Consent to Use Private Information

In the course of enrolling for a Certificate or using a certificate service, individuals are provided with notices describing how their personal information will be processed by and on behalf of DigiCert and, where necessary, DigiCert obtains consent to process such information. Personal information is used as explained during the registration process. Individuals to whom the information belongs have the opportunity to decline having their personal information used for particular purposes, like direct marketing. They have also agreed to let certain information appear in publicly accessible directories and be communicated to others.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

If required by a legitimate and lawful judicial order or regulation that complies with requirements of this CP/CPS, DigiCert may disclose private information without notice.

9.4.7. Other Information Disclosure Circumstances

No stipulation.

9.5. Intellectual Property Rights

DigiCert, Inc owns the intellectual property rights in DigiCert's services, including the Certificates, trademarks and the Proprietary Marks used in providing the services, and this CP/CPS.

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.

For the avoidance of doubt, external documents or electronic records signed or protected using DigiCert Certificates are not considered to be DigiCert documents for the purposes of this Section, nor is DigiCert responsible for the content of those documents or records.

9.6. Representations and Warranties

9.6.1. CA Representations and Warranties

By issuing a Certificate, DigiCert represents and warrants that, during the period when the Certificate is valid, DigiCert has complied with this CP/CPS in issuing and managing the Certificate to the parties listed below:
• The party to the relevant Master Services Agreement and Terms of Use;
• All Relying Parties who reasonably rely on a Valid Certificate; and
• All Application Software Vendors with whom DigiCert has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Vendor.

DigiCert discharges its obligations by:
• DigiCert complies, in all material aspects, with this CP/CPS, and all applicable laws and regulations;
• DigiCert publishes and updates CRLs responses on a regular basis;
• All Certificates issued under this CP/CPS will be verified in accordance with this CP/CPS and meet the minimum requirements found herein; and
• DigiCert will maintain a Repository of public information on its website.

DigiCert hereby warrants (i) it has taken reasonable steps to verify that the information contained in any Certificate is accurate at the time of issue (ii) Certificates shall be revoked if DigiCert believes or is notified that the contents of the Certificate are no longer accurate, or that the Private Key associated with a Certificate has been compromised in any way.

DigiCert makes no other warranties, and all warranties, express or implied, statutory or otherwise, are excluded to the greatest extent permissible by applicable law, including without limitation all warranties as to merchantability or fitness for a particular purpose.

9.6.2. RA Representations and Warranties

RAs represent and warrant that:
• The RA's Certificate issuance and management services conform to the applicable CP/CPS and applicable CA or RA Agreements;
• Information provided by the RA does not contain any false or misleading information;
• Reasonable steps are taken to verify that the information contained in any Certificate is accurate at the time of issue;
• Translations performed by the RA are an accurate translation of the original information;
• All Certificates requested by the RA meet the requirements of this CP/CPS and RA Agreement; and

• The RA will request that Certificates be revoked by DigiCert if they believe or are notified that the contents of the Certificate are no longer accurate, or that the key associated with a Certificate has been compromised in any way.

DigiCert's RA Agreement 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 Master Services Agreement or Terms of Use, that the Applicant make the commitments and warranties in this Section for the benefit of DigiCert and all Relying Parties and Application Software Vendors. This may take the form of either:
• The Applicant's agreement to the Master Services Agreement with DigiCert; or
• 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:
• Securely generate its Private Keys and protect its Private Keys from compromise, and exercise sole and complete control and use of its Private Keys;
• Provide accurate and complete information when communicating with DigiCert, and to respond to DigiCert's instructions concerning Key Compromise or Certificate misuse;
• Confirm the accuracy of the Certificate data prior to installing or using the Certificate;
• Promptly (a) 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 included in the Certificate, and (b) request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate;
• Ensure that individuals using Certificates on behalf of an organization have received security training appropriate to the Certificate;
• Use the Certificate only for authorized and legal purposes, consistent with the Certificate purpose, this CP/CPS, and the Master Services Agreement, including only installing TLS Server Certificates on servers accessible at the Domain listed in the Certificate; and
• Promptly cease using the Certificate and related Private Key after the Certificate's expiration or revocation, or in the event that DigiCert notifies the Subscriber that the DigiCert PKI has been compromised.

Subscriber Agreements may include additional representations and warranties.

9.6.4. Relying Party Representations and Warranties

Relying parties are required to act in accordance with this CP/CPS and the Relying Party Agreement. A Relying Party must exercise reasonable reliance as set out in this Section.

• Prior to relying on the Certificate or other authentication product or service, Relying Parties are obliged to check all status information provided by DigiCert related to the Certificate or other authentication product or service to confirm that the information was still valid and that the product or service had not expired or been revoked. For Certificates, this includes checking to ensure that each Certificate in the Certificate Chain is valid,

unexpired, and non-revoked (by using any CRL or OCSP information available).
• Prior to relying on an authentication product or service, Relying Parties must gather sufficient information to make an informed decision about the proper use of the authentication product or service and whether intended reliance on the authentication product or service was reasonable in light of the circumstances.
• This includes evaluating the risks associated with their intended use and the limitations associated with the authentication product or service provided by DigiCert.
• Relying Parties' reliance on the authentication product or service is reasonable based on the circumstances. Relying Parties' reliance will be deemed reasonable if:
• The attributes of the Certificate relied upon and the level of assurance in the Identification and Authentication provided by the Certificate are appropriate in all respects to the level of risk and the reliance placed upon that Certificate by the Relying Party;
• The Relying Party has, at the time of that reliance, used the Certificate for purposes appropriate and permitted by the CP/CPS and under the laws and regulations of the jurisdiction in which the Relying Party is located;
• The Relying Party has, at the time of that reliance, acted in good faith and in a manner appropriate to all the circumstances known, or circumstances that ought reasonably to have been known, to the Relying Party;
• The Relying Party has, at the time of that reliance, verified the Digital Signature, if any;
• The Relying Party has, at the time of that reliance, verified that the Digital Signature, if any, was created during the operational term of the Certificate being relied upon;
• The identity of the Subscriber is displayed correctly by utilizing trusted application software; and
• Any alterations arising from security changes are identified by utilising trusted application software.

If the circumstances indicate a need for additional assurances, it is Relying Parties' responsibility to obtain such assurances. A Relying Party shall make no assumptions about information that does not appear in a Certificate. Relying Party Agreements may include additional representations and warranties.

9.6.5. Representations And Warranties of Other Participants

Participants within the DigiCert PKI represent and warrant that they accept and will perform any and all duties and obligations as specified by this CP/CPS.

9.7. Disclaimers of Warranties

OTHER THAN AS PROVIDED IN SECTION 9.6.1, THE CERTIFICATES ARE PROVIDED "AS IS" AND "AS AVAILABLE" AND TO THE MAXIMUM EXTENT PERMITTED BY LAW, DIGICERT DISCLAIMS ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT.

DIGICERT DOES NOT WARRANT THAT ANY CERTIFICATE WILL MEET SUBSCRIBER'S OR ANY OTHER PARTY'S EXPECTATIONS OR THAT ACCESS TO THE CERTIFICATES WILL BE TIMELY OR ERROR-FREE.

DIGICERT does not guarantee the accessibility of any Certificates and may modify or discontinue offering any Certificates at any time.

Subscriber's sole remedy for a defect in the Certificates is for DIGICERT to use commercially reasonable efforts, upon notice of such defect from Subscriber, to correct the defect, except that DIGICERT has no obligation to correct defects that arise from (i) misuse, damage, modification or damage of the Certificates or combination of the Certificates with other products and services by parties other than DIGICERT, or (ii) Subscriber's breach of any provision of the Master Services Agreement.

9.8. Limitations of Liability

This section does not limit a party's liability for: (i) death or personal injury resulting from the negligence of a party; (ii) gross negligence, willful misconduct or violations of applicable law, or (iii) fraud or fraudulent statements made by a party to the other party in connection with this CP/CPS.

TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW AND NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY OR LIMITATION OF LIABILITY: (A) DIGICERT AND ITS AFFILIATES, SUBSIDIARIES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, PARTNERS AND LICENSORS (THE DIGICERT ENTITIES) WILL NOT BE LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES (INCLUDING ANY DAMAGES ARISING FROM LOSS OF USE, LOSS OF DATA, LOST PROFITS, BUSINESS INTERRUPTION, OR COSTS OF PROCURING SUBSTITUTE SOFTWARE OR SERVICES) ARISING OUT OF OR RELATING TO THIS CP/CPS OR THE SUBJECT MATTER HEREOF; AND (B) THE DIGICERT ENTITIES' TOTAL CUMULATIVE LIABILITY ARISING OUT OF OR RELATING TO THIS CP/CPS OR THE SUBJECT MATTER HEREOF WILL NOT EXCEED THE AMOUNTS PAID BY OR ON BEHALF OF SUBSCRIBER TO DIGICERT IN THE TWELVE MONTHS PRIOR TO THE EVENT GIVING RISE TO SUCH LIABILITY, REGARDLESS OF WHETHER SUCH LIABILITY ARISES FROM CONTRACT, INDEMNIFICATION, WARRANTY, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE, AND REGARDLESS OF WHETHER DIGICERT HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

NO CLAIM, REGARDLESS OF FORM, WHICH IN ANY WAY ARISES OUT OF THIS CP/CPS, MAY BE MADE OR BROUGHT BY SUBSCRIBER OR SUBSCRIBER'S REPRESENTATIVES MORE THAN ONE (1) YEAR AFTER THE BASIS FOR THE CLAIM BECOMES KNOWN TO SUBSCRIBER.

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 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 (i) a valid and trustworthy Certificate as not valid or trustworthy or (ii) displaying as trustworthy (a) an Certificate that has expired or (b) a revoked 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 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 Master Services 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 Master Services 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 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 are effective as of the date stipulated in this document 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 force until it is replaced by a newer version.

9.10.3. Effect Of Termination and Survival

The conditions and effect resulting from termination of this CP/CPS will be communicated via the DigiCert website upon termination. That communication will outline the provisions that may survive termination of this CP/CPS and remain in force. The responsibilities for protecting business confidential and private personal information shall survive termination, and the Terms and Conditions for all existing Certificates shall remain valid for the remainder of the validity periods of such Certificates.

9.11. Individual Notices and Communications with Participants

DigiCert accepts notices related to this CP/CPS at the locations specified in Section 1.5. Notices are deemed effective after the sender receives a valid and digitally signed acknowledgment of receipt from DigiCert.

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

9.12. Amendments

9.12.1. Procedure For Amendment

Amendments to this CP/CPS are made and approved by the DCPA at least annually. Notification of the amendments are made by posting an updated version of the CP/CPS to the 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

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

• Arbitration: In the event a dispute is allowed or required to be resolved through arbitration, the parties will maintain the confidential nature of the existence, content, or results of any arbitration hereunder, except as may be necessary to prepare for or conduct the arbitration hearing on the merits, or except as may be necessary in connection with a court application for a preliminary remedy, a judicial confirmation or challenge to an arbitration award or its enforcement, or unless otherwise required by law or judicial decision.
• Class Action and Jury Trial Waiver: THE PARTIES EXPRESSLY WAIVE THEIR RESPECTIVE RIGHTS TO A JURY TRIAL FOR THE PURPOSES OF LITIGATING DISPUTES HEREUNDER. Each party agrees that any dispute must be brought in the respective party's individual capacity, and not as a plaintiff or class member in any purported class, collective, representative, multiple plaintiffs, or similar proceeding ("Class Action"). The parties expressly waive any ability to maintain any Class Action in any forum in connection with any dispute. If the dispute is subject to arbitration, the arbitrator will not have authority to combine or aggregate similar claims or conduct any Class Action nor make an award to any person or entity not a party to the arbitration. Any claim that all or part of this Class Action waiver is unenforceable, unconscionable, void, or voidable may be determined only by a court of competent jurisdiction and not by an arbitrator.

9.14. Governing Law

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

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

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

9.16. 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 contract 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, the Master Services Agreement and Relying Party Agreements shall include a force majeure clause protecting DigiCert.

9.17. OTHER PROVISIONS

No stipulation.