

DigiCert

Certification Practices Statement

DigiCert, Inc.
Version 5.12
October 31, 2022
2801 N.
Thanksgiving Way
Suite 500

1-801-877-2100
Fax: 1-801-705-0481

Table of Contents

1.	INTRODUCTION.....	7
1.1.	OVERVIEW.....	7
1.2.	DOCUMENT NAME AND IDENTIFICATION.....	8
1.3.	PKI PARTICIPANTS.....	11
1.3.1.	Certification Authorities.....	11
1.3.2.	Registration Authorities and Other Delegated Third Parties.....	11
1.3.3.	Subscribers.....	11
1.3.4.	Relying Parties.....	12
1.3.5.	Other Participants.....	12
1.4.	CERTIFICATE USAGE.....	12
1.4.1.	Appropriate Certificate Uses.....	12
1.4.2.	Prohibited Certificate Uses.....	14
1.5.	POLICY ADMINISTRATION.....	14
1.5.1.	Organization Administering the Document.....	14
1.5.2.	Contact Person.....	14
	Revocation Reporting Contact Person.....	14
1.5.3.	Person Determining CPS Suitability for the Policy.....	15
1.5.4.	CPS Approval Procedures.....	15
1.6.	DEFINITIONS AND ACRONYMS.....	15
1.6.1.	Definitions.....	15
1.6.2.	Acronyms.....	17
1.6.3.	References.....	18
2.	PUBLICATION AND REPOSITORY RESPONSIBILITIES.....	19
2.1.	REPOSITORIES.....	19
2.2.	PUBLICATION OF CERTIFICATION INFORMATION.....	19
2.3.	TIME OR FREQUENCY OF PUBLICATION.....	19
2.4.	ACCESS CONTROLS ON REPOSITORIES.....	19
3.	IDENTIFICATION AND AUTHENTICATION.....	20
3.1.	NAMING.....	20
3.1.1.	Type of Names.....	20
3.1.2.	Need for Names to be Meaningful.....	20
3.1.3.	Anonymity or Pseudonymity of Subscribers.....	20
3.1.4.	Rules for Interpreting Various Name Forms.....	20
3.1.5.	Uniqueness of Names.....	20
3.1.6.	Recognition, Authentication, and Role of Trademarks.....	21
3.2.	INITIAL IDENTITY VALIDATION.....	21
3.2.1.	Method to Prove Possession of Private Key.....	21
3.2.2.	Authentication of Organization Identity and Domain/Email Control.....	21
3.2.2.1.	Verification of IP Address.....	25
3.2.2.2.	Wildcard Domain Validation.....	26
3.2.2.3.	Verification of Country.....	26
3.2.3.	Authentication of Individual Identity.....	27
3.2.3.1.	Authentication for Role-based Client Certificates.....	31
3.2.3.2.	Authentication of Devices with Human Sponsors.....	32
3.2.4.	Non-verified Subscriber Information.....	32
3.2.5.	Validation of Authority.....	32
3.2.6.	Criteria for Interoperation.....	33
3.3.1.	Identification and Authentication for Routine Re-key.....	33
3.4.	IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST.....	34
4.	CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS.....	35
4.1.	CERTIFICATE APPLICATION.....	35
4.1.1.	Who Can Submit a Certificate Application.....	35
4.1.2.	Enrollment Process and Responsibilities.....	35
4.2.	CERTIFICATE APPLICATION PROCESSING.....	35
4.2.1.	Performing Identification and Authentication Functions.....	35

4.2.2.	Approval or Rejection of Certificate Applications	36
4.2.3.	Time to Process Certificate Applications	37
4.3.	CERTIFICATE ISSUANCE	37
4.3.1.	CA Actions during Certificate Issuance	37
4.3.2.	Notifications to Subscriber by the CA of Issuance of Certificate	37
4.4.	CERTIFICATE ACCEPTANCE	37
4.4.1.	Conduct Constituting Certificate Acceptance.....	37
4.4.2.	Publication of the Certificate by the CA.....	37
4.4.3.	Notification of	

9.2.	FINANCIAL RESPONSIBILITY	76
9.2.1.	Insurance Coverage	76
9.2.2.	Other Assets.....	76
9.2.3.	Insurance or Warranty Coverage for End-Entities	76
9.3.	CONFIDENTIALITY OF	

Microsoft Trusted Root Store (Program Requirements)	https://docs.microsoft.com/en-us/security/trusted-root/program-requirements
Mozilla Root Store Policy	https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/
Apple Root Store Program	https://

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

OIDs found in Certificates reliant upon CAB Forum requirements and guidelines include the designated reserved policy identifiers in the Certificate Policy extension as of September 30, 2020 as specified in section 7.1.6 of the CA/B Baseline Requirements. Certificates issued before that date include other OIDs that are designated in section 7.1.6 of this document.

1.3.1. Certification Authorities

DigiCert operates all certification authorities (CAs) that issue digital certificates. As the operator of several CAs, DigiCert performs functions associated with Public Key operations, including receiving certificate requests, issuing, revoking, rekeying, and renewing a digital Certificate, and maintaining, issuing, and publishing CRLs
www.digicert.com.

In limited circumstances, root CAs owned by DigiCert are used to issue cross Certificates to external third parties operating their own PKIs. An external Issuer CA is an unaffiliated third party that is issued a subordinate CA Certificate by DigiCert where the Private Key associated with that CA Certificate is not maintained under the physical control of DigiCert.

All external subordinate CAs are prohibited, either technically or contractually, from issuing Certificates to domain names or IP addresses that a Subscriber does not legitimately own or control (i.e. issuance for purposes of $\text{°} \text{©} \text{©} \text{©} \text{š} \text{š} \text{E} \text{; } \text{©} \text{; } \text{°}$ is prohibited), and external subordinate CAs are required to implement procedures that are at least as restrictive as those found in 1.0.1.4.3.6.2.4.38.19 Tm0 g0 G[(imp)3(l)-5(e)-5(me)-4(n)4(t)

Subscribers are not always the party identified in a Certificate, such as when Certificates are issued to an «~~ES~~»^a employees. The *Subject* of

following table provides a brief description of the appropriate uses of each. The descriptions are for guidance only and are not binding.

Certificate	Appropriate Use
DV SSL/TLS Server Certificates	Used to secure online communication where the risks and consequences of data compromise are low, including non-monetary transactions or transactions with little risk of fraud or malicious access.

1.4.2. Prohibited Certificate Uses

Certificates do not guarantee that the Subject is trustworthy, honest, reputable in its business dealings, safe to do business with, or compliant with any laws. A Certificate only establishes that the information in the

For anyone listed in section 4.9.2 of this CPS and the CA/Browser Baseline Requirements that needs assistance with revocation or an investigative report, DigiCert provides this page for reporting and submitting requests with all of the necessary information as outlined in section 4.9: <https://problemreport.digicert.com/>

If the problem reporting page is unavailable, there is a system outage, you have questions, or you believe our findings are incorrect please contact revoke@digicert.com.

Entities submitting certificate revocation requests must list their identity and explain the reason for requesting

"EV Guidelines" is defined in section 1.1.

"Key Pair" means a Private Key and associated Public Key.

"OCSP Responder" means an online software application operated under the authority of DigiCert and connected to its repository for processing certificate status requests.

"Private Key" means the key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create digital signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

"Public Key" means the key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify digital signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

"Relying Party" means an entity that relies upon either the information contained within a Certificate or a time-stamp token.

"Relying Party

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

DigiCert makes its root Certificates, revocation data for issued digital Certificates, CPs, CPSs, Relying Party Agreements, and standard Subscriber Agreements available in public repositories. DigiCert develops, implements, enforces, and annually updates this CPS to meet the compliance standards of the documents listed in Sections 1.1 and 1.6.3. These updates also describe how the latest version of the Baseline Requirements are implemented. As Baseline Requirements are updated, DigiCert reviews the changes to determine their impact on these practices. Each section impacted by the Baseline Requirements will be updated and provided to the DCPA for approval and implementation. If an SSL/TLS Server Certificate is intended to be trusted in Chrome, it is published by posting it in a Certificate Transparency log.

~ ¥¥ | ®

3. IDENTIFICATION AND AUTHENTICATION

3.1.1. Type of Names

For TLS and s/MIME Certificates are

3.1.6. Recognition, Authentication, and Role of Trademarks

For publicly-trusted TLS/SSL and EV SSL Certificates, DigiCert implements a process that prevents Certificates from including a name, DBA, tradename, trademark,

IV and OV SSL/TLS Server,
Object Signing, and Device
Certificates
(excluding device
Certificates issued under
the Grid-only arc)

DigiCert validates right to use or control the Domain
Name(s) and the country code that will be listed in the Certificate
using the DV SSL/TLS

Before issuing an SSL/TLS Server Certificate with a domain name that has not been previously verified as within the scope of an & - or other Delegated Third Party - allowed domain names, DigiCert establishes that the RA or Delegated Third Party has the right to use the Domain Name by independently verifying the authorization with the domain owner, as described and allowed by the above.

DigiCert uses a documented internal process to check the accuracy of information sources and databases to data source as a Reliable Data Source, DigiCert evaluates the source for its reliability, accuracy, and resistance to alteration or falsification. For SSL/TLS, EV, EVCS, and other Certificates under the requirements of the CA/Browser Forum, the criteria in sections BR 3.2.2.7 and EVG 11.11.5 are included in the process to determine the database and information sources.

For Legal Entity Identifier (LEI) numbers listed in Certificates, DigiCert may include the value after verification, through the appropriate mechanism, such as mechanisms provided by Global Legal Entity Identifier Foundation (GLEIF), that the LEI is associated with entity information provided. LEI lookups are treated as information from a source described above, but not currently relied upon as a primary source of information for verification. Instead, this information is treated as additional correlation of identity information found in the certificate and provided in the certificate for the convenience and use of data researchers and the legal entities operating the certificates.

Before issuing a certificate with a wildcard character (*) in a CN or subjectAltName of type DNS-ID, DigiCert follows a documented procedure that determines if the wildcard character occurs in the first label position to further explanation).

If a wildcard would fall within the label immediately to the left of a registry-controlled /1 or public suffix, DigiCert refuses issuance unless the applicant proves its rightful control of the entire Domain Namespace. (e.g. to Example Co.).

For EV Certificates, DigiCert may include a Wildcard Domain Name in the Subject Alternative Name extension and Subject -most Domain Label of the FQDN portion of the Wildcard Domain Name and the inclusion of the Wildcard Domain Name complies with Section 3.2.2.6 of the CA/Browser Forum Baseline Requirements. In all other cases, DigiCert will not include a Wildcard Domain Name in the Subject Alternative Name extension or Subject Common Name field of an EV Certificate.

For publicly-trusted TLS, if the Applicant requests a Certificate that will contain Subject Identity Information comprised only of the countryName field, then DigiCert or the RA verifies the country associated with the Subject using a verification process meeting the requirements of

3.2.3.

<p>Adobe Document Signing Certificates for Individuals</p>	<p>In-person appearance before a person performing identity proofing for a Registration Authority or a Trusted Agent per section ICA5(a) of the AATL 2.0 requirements. This can be performed either physically or digitally per the stated standards.</p> <p>RAs must retain sufficient information about the signatory's identity to identify the signatory.</p>
<p>Adobe Document Signing Certificates for Organizations</p>	<p>In-person appearance (either physically or digitally) before a person performing identity proofing for a Registration Authority or a Trusted Agent; and</p> <p>Evidence of association with, and proofs of entitlement to represent, that organization per methods described for Applicants for a Level 2, 3, or 4 Client Certificate.</p> <p>RAs must retain sufficient information about the signatory's identity to identify the signatory.</p>
<p>Level 1 Client Certificates Personal (email Certificates)</p>	<p>As specified in Section 3.2.2 (no identity verification other than control of the email address listed in the Certificate).</p>
<p>Level 1 Client Certificates Enterprise (email certificates)</p>	<ol style="list-style-type: none"> For a certificate capable of being used for digitally signing or encrypting email messages, DigiCert takes reasonable measures to verify that the Applicant submitting the request controls the email account associated with the email address referenced in the certificate or has been authorized by the email account holder to act on their behalf. DigiCert may rely on validation performed for an Authorization Domain Name (as specified in the Baseline Requirements and section 3.2.2 of this CPS) as being valid for subdomains of that Authorization Domain Name.

Level 3 Client Certificates

In-person proofing⁴ before an RA, Trusted Agent, or an entity certified by a state, federal, or national entity that is authorized to confirm identities⁵. The information must be collected and stored in a secure manner. Required identification consists of one unexpired Federal/National Government-issued Picture I.D. (e.g. a passport), a REAL ID, or two unexpired Non-

DigiCert issues Level 1, 2, 3 or 4 Client Certificates for use on computing or network devices, provided that the entity owning the device is listed as the subject. In all cases, the device has a human sponsor who provides:

- Equipment

An organization may limit who is authorized to request Certificates by sending a request to DigiCert. A request to limit authorized individuals is not effective until approved by DigiCert. DigiCert will respond to an

3.2.6. Criteria for

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

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 the Applicant or an agent of the Applicant supplies to DigiCert.

EV Certificate requests must be submitted by an authorized Certificate Requester and approved by a Certificate Approver. The certificate request must be accompanied by a signed (in writing or electronically) Subscriber Agreement from a Contract Signer.

DigiCert does not issue Certificates to entities on a government denied list maintained by the United States or that is located in a country with which the laws of the United States prohibit doing business.

In accordance with Section 5.5.2, DigiCert maintains an internal database of all previously revoked Certificates and previously

4.2.3. Time to Process Certificate Applications

within a reasonable time frame.

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

Renewed Certificates are considered accepted 30 days after the ~~CA's~~ renewal, or earlier upon use of the Certificate when evidence exists that the Subscriber used the Certificate.

4.6.6. Publication of the Renewal Certificate by the CA

DigiCert publishes a renewed Certificate by delivering it to the Subscriber. All renewed CA Certificates are

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

RAs may receive notification of a ~~CA's~~ renewal if the RA was

4.8.1. Circumstances for Certificate Modification Modifying a

the Certificate suffered a key compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of the CAB forum baseline requirements or any section of the Mozilla Root Store policy;

4. DigiCert obtaint

If DigiCert deems appropriate, DigiCert may forward the revocation reports to law enforcement. DigiCert maintains a continuous 24/7 ability to internally respond to any high priority revocation requests and certificate problem reports on the following website: <https://www.digicert.com/certificate-revocation.htm> and other resources as indicated in section 1.5.2 of this CPS.

4.9.4. Revocation Request Grace Period

Subscribers are required to request revocation within one day after detecting the loss or compromise of the Private Key. DigiCert may grant and extend revocation grace periods on a case-by-case basis. DigiCert reports the suspected compromise of its CA Private Key and requests revocation to both the policy authority and operating authority of the superior issuing CA within one hour of discovery.

4.9.5. Time within which CA Must Process the Revocation Request

DigiCert will revoke a CA Certificate within one hour after receiving clear instructions from the DCPA.

Within 24 hours after receiving a Certificate problem report or a revocation request, DigiCert investigates the facts and circumstances involved with the report and will provide a preliminary report on

DigiCert updates and reissues CRLs at least (i) once every twelve months and (ii) 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.

For all other Certificates in this CPS:

DigiCert uses its offline root CAs to publish CRLs for its inter

DigiCert may monitor the OCSP responder for requests for $\pm^a \pm^-_i \dot{Y}$ serial numbers as part of its security response procedures.

there was a corresponding Certificate that matches the Precertificate [RFC6962]. A certificate serial number within an OCSP request is one of the following three options:

1. $\dot{S}^- \dot{Y}^a$ if a Certificate with that serial number has been issued by the Issuing CA, using any current or previous key associated with that CA subject; or
2. $\dot{R}^-_i \dot{Y}$ if a Precertificate [RFC6962] with that serial number has been issued by (a) the Issuing CA; or (b) a Precertificate Signing Certificate [RFC6962] associated with the Issuing CA; or
3. $\pm^a \pm^-_i \dot{Y}$

DigiCert sets the maximum time period an EPCS certificate may be in suspension to 30 days. If the Certificate remains in suspension throughout the period, the requestor has until the 30th day to confirm unsuspension or it will be revoked. DigiCert will maintain an internal policy and procedure to manually or programmatically review the certificate suspensions in this period in order to ensure the certificates do not pass the timeframe stated.

If the subscriber has not removed the certificate from hold (suspension) within that period, the certificate will

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1.1. Site Location and Construction

DigiCert performs its CA and TSA operations from secure data centers. The data centers are equipped with state-of-the-art security measures and are staffed by highly trained and vetted personnel. DigiCert operates under a security policy designed to detect, deter, and prevent unauthorized access to DigiCert's operations.

5.1.2. Physical Access

Systems providing online certificate issuance (e.g. Issuer CAs) are located in secure data centers. DigiCert protects such online equipment (including certificate status servers) through physical access controls, including restricted access to the facility, secure entry procedures, and physical security measures.

5.1.3. Power and Air Conditioning

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

5.1.4. Water Exposures

The cabinets housing DigiCert's CA and TSA systems are designed to prevent and protect against water exposure.

5.1.5. Fire Prevention and Protection

The data centers are equipped with fire suppression mechanisms.

5.1.6. Media Storage

DigiCert protects its media from accidental damage, environmental hazards, and unauthorized physical access. Backup files are created on a daily basis. Backup files are maintained separately from data operations facility.

5.1.7. Waste Disposal

All unnecessary copies of printed sensitive information are 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

DigiCert makes regular backup copies of any information necessary to recover from a system failure. Backup copies of CA Private Keys and activation data are stored for disaster recovery purposes off-site and are accessible only by trusted personnel.

5.1.9. Certificate Status Hosting, CMS and External RA Systems

All physical control requirements under Section 5.1 apply equally to any Certificate Status Hosting, CMS, or external RA system.

5.2.1. Trusted Roles

Personnel acting in trusted roles include CA, TSA, 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 PKI or TSA operations. A list of personnel appointed to trusted roles is maintained and reviewed annually.

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. Administrators do not issue Certificates to Subscribers.

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

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.

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 CPS or an & " Registration Practices Statement.

RA Administrators are responsible for the RA software.

5.2.2. Number of Persons Required per Task

DigiCert requires that at least two people acting in a trusted role take action for the most sensitive tasks, such as activating Private Keys, generating a CA Key Pair, or backing up a DigiCert Private Key. The Internal Auditor may serve to fulfill the requirement of multiparty control for physical access to the CA system but not logical access. Physical access to the CAs does not constitute a task as defined in this section but is defined in section 5.1.

5.2.3. Identification and Authentication for each Role

All personnel are required to authenticate themselves to CA, TSA, and RA systems before they are allowed access to systems necessary to perform their trusted roles.

5.2.4. Roles Requiring Separation of Duties

Roles requiring a separation of duties include:

1. Those performing authorization functions such as the verification of information in certificate applications and approvals of certificate applications and revocation requests,
2. Those performing backups, recording, and record-keeping functions;
3. Those performing audit, review, oversight, or reconciliation functions; and
4. Those performing duties related to CA/TSA key management or CA/TSA administration.

To accomplish this separation of duties, DigiCert specifically designates individuals to the trusted roles defined in Section 5.2.1 above. Individuals designated as Registration Officer or Administrator may perform Operator duties, but an Internal Auditor must identify and authenticate individuals acting in trusted roles, restrict an individual from assuming multiple roles at the same time.

5.3.1. Qualifications, Experience, and Clearance Requirements

The DCPA is responsible and accountable for PKI operations and ensures compliance with this CPS and the CP. Prior to the engagement of any person in the Certificate Management Process, whether as an employee, agent, or an independent contractor, DigiCert verifies the identity and trustworthiness of such person.

Management and operational support personnel involved in time-stamp operations possess experience with information security and risk assessment and knowledge of time-stamping technology, digital signature technology, mechanisms for calibration of time stamping clocks with UTC, and security procedures. 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 employee appointed to a trusted role and performs a background check

5.4.1. Types of Events Recorded

DigiCert logs all actions that are initiated by operators to establish the accountability of the operators who initiate such actions.

DigiCert enables all essential event auditing capabilities of its CA and TSA applications in order to record the events that occur during the operation of the applications. DigiCert uses manual procedures to satisfy the requirements.

For each event, DigiCert records the relevant (i) date and time, (ii) type of event, (iii) success or failure, and (iv) user or system that caused the event or initiated the action. DigiCert records the precise time of any significant TSA events. All event records are available to auditors as proof of the events that occurred and are maintained to the standard per the requirements of the relevant policies and programs.

DigiCert records at least the following events:

1. CA Certificate and key lifecycle events, including:
 - a. Key generation, backup, storage, recovery, archival, and destruction
 - b. Certificate requests, renewal, and re-key requests, and revocation;
 - c. Approval and rejection of certificate requests
 - d. Cryptographic device lifecycle management events;
 - e. Generation of Certificate Revocation Lists;
 - f. Signing of OCSP responses (as described in sections 4.9 and 4.10);
 - g. Introduction of new Certificate Profiles and retirement of 1 197.21 43E8[()] TJETQq0.0WETQq0.00000912 0 6

conditions, including any evidence of malicious activity, and (3) (if necessary) prepares a written summary

and other arrangements that DigiCert has in place to counter such threats.

~ ¥¥ ; ® - 7ª °; ® S''' ±ÿ¥«® ·® 2¥³ °¤; ¨; œ®µ'š±ÿ¥ÿš°š'œ; oš' ¤®œª °¥ ±¥µ ~ ¥¥ ; ® - 'š±ÿ¥'''« E' monitoring

Towards the end of a CA Private Key's lifetime, DigiCert ceases using the expiring CA Private Key to sign Certificates and uses the old Private Key only to sign CRLs and OCSP responder Certificates. 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. This key changeover process

6.1.3. Public Key Delivery to Certificate Issuer

Not Applicable.

6.1.4. CA Public Key Delivery to Relying Parties

DigiCert's Public Keys are provided to Relying Parties as specified in a certificate validation or path discovery policy file, as trust anchors in commercial browsers and operating system root store, and/or as roots signed by other CAs. All accreditation authorities supporting DigiCert Certificates and all application

DigiCert may also distribute Public Keys that are part of an updated signature Key Pair as a self-signed Certificate, as a new CA Certificate, or in a key roll-over Certificate. Relying Parties may obtain DigiCert's self-

Adobe Signing

FIPS 140

DigiCert never leaves its HSM devices in an active unlocked or unattended state.

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

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

DigiCert may voluntarily retire its CA Private Keys before the periods listed above to accommodate key changeover processes. DigiCert may also retire its CA Private Keys before their expiration period if the key identification requirements specified in Section 3.1.1.

6.4.1. Activation Data Generation and Installation

DigiCert activates the cryptographic module containing its CA Private Keys according to the specifications of the hardware manufacturer. For roots and public issuing CAs, this method has been evaluated as meeting the requirements of FIPS 140-2 Level 3. The cryptographic hardware is held under two-person control as explained in Section 5.2.2 and elsewhere in this CPS. DigiCert will only transmit activation data via an appropriately protected channel and at a time and place that is distinct from the delivery of the associated cryptographic module.

All DigiCert personnel and Subscribers are instructed

RAs must logically separate access to these systems and this information from other components. This separation prevents access except through defined processes. RAs must use firewalls to protect the network from internal and external intrusion and limit the nature and source of activities that may access such systems and information. RAs must require the use of passwords with a minimum character length and a combination of alphanumeric and special characters.

CA systems are configured to:

1. authenticate the identity of users before permitting access to the system or applications;
2. manage the privileges of users

DigiCert and RA functions are performed using networks secured in accordance with the standards documented in the DigiCert CP to prevent unauthorized access, tampering, and denial-of-service attacks. Communications of sensitive information shall be protected using point-to-point encryption for confidentiality and digital signatures for non

sha384WithRSAEncryption	[iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12]
sha512WithRSAEncryption	[iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha512WithRSAEncryption(13)]
ecdsa-with-SHA256 ⁹	[iso(1) member-body(2) us(840) ansi-X9-62 (10045)]

7.1.8 Policy Qualifiers Syntax and Semantics

DigiCert includes brief statements in Certificates about the limitations of liability and other terms associated with the use of a Certificate in the Policy Qualifier field of the Certificates Policy extension. Those Certificates may contain a CPS pointer qualifier that points to the applicable Relying Party Agreement or the applicable CPS.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

For revoked issuing CAs, the CRLReason indicated cannot be unspecified (0) or certificateHold(6). If the reason for revocation is unspecified, DigiCert will omit the reasonCode entry extension, when technically not capable of issuance.

If a reasonCode CRL entry extension is present, the CRLReason must indicate the most appropriate reason for revocation of the certificate. DigiCert specifies the following reason codes from RFC 5280, section 5.3.1 as appropriate for most instances when used in accordance with the practices in this section and this CPS:

- unspecified (0)¹¹
-

- the certificate subscriber has requested that their certificate be revoked for this reason; or
- DigiCert revoked the certificate due to domain authorization or compliance issues other than those related to keyCompromise or privilegeWithdrawn.

Otherwise, the superseded CRLReason must not be used.

7.2.1 Version number(s)

DigiCert issues version 2 CRLs that may contain the following fields per requirements:

Field	Value
Issuer Signature Algorithm	sha-1WithRSAEncryption [1 2 840 113549 1 1 5] OR sha-256WithRSAEncryption [1 2 840 113549 1 1 11]; sha-384WithRSAEncryption [1 2 840 113549 1 1]; sha-512WithRSAEncryption [1 2 840 113549 1 1 13]; ecdsa-with-sha256 [1 2 840 10045 4 3 2]; OR ecdsa-with-sha384 [1 2 840 10045 4 3 3].
Issuer Distinguished Name	Full subject DN of the issuing CA
thisUpdate	CRL issue date in UTC format
nextUpdate	Date

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The practices in this CPS are designed to meet or exceed the requirements of generally accepted industry standards, including the latest versions of the WebTrust Programs for Certification Authorities as required by the Mozilla Root Store policy and other programs listed in section 1.1 and 1.6.3.

DigiCert receives an annual period in time audit by an independent external auditor to assess DigiCert's compliance with this CPS, referenced requirements, any applicable CPs, and the WebTrust for CA programs criteria.

WebTrust auditors must meet the requirements of Section 8.2 of the CA/Browser Baseline Requirements and section 3.1 of the Mozilla Root Store policy where applicable.

~ ¥¥ ; ® ~ WebTrust / Federal PKI auditor does not have a financial interest, business relationship, or course of dealing that could

On at least a quarterly basis, DigiCert performs regular internal audits against a randomly selected sample of at least three percent of its SSL/TLS Server Certificates and EV Code Signing Certificates issued since the last internal audit. Self-audits on server and code signing Certificates are performed in accordance with Guidelines adopted by

9. OTHER

9.5.1. Property Rights in Certificates and Revocation Information


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 referenced in the Certificate. DigiCert, and customers shall grant permission to use revocation information to perform Relying Party functions subject to the applicable CRL usage agreement, Relying Party Agreement, or any other applicable agreements.

9.5.2. Property Rights in the CP

Issuer CAs acknowledge that DigiCert retains all intellectual property rights in and to this CPS.

9.5.3. Property Rights in Names

Subscribers and Applicants retain all rights it has (if any) in any trademark, service mark, or trade name

For EV Certificates, DigiCert represents to Subscribers, Subjects, Application Software Vendors that distribute
~  root Certificates, and Relying Parties that use a DigiCert Certificate while the Certificate is valid

9.6.4. Relying Party Representations and Warranties

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

1. Obtained sufficient knowledge on the use of digital Certificates and PKI,
2. Studied the applicable limitations on the usage of Certificates and agrees to assume liability related to the use of Certificates,
3. Has read, understands, and agrees to the DigiCert Relying Party Agreement and this CPS,
4. Verified both the DigiCert Certificate

4. Liability related to the security, usability, or integrity of products not supplied by DigiCert, including hardware;

9.10.1. Term

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

9.10.2. Termination

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

9.10.3. Effect of Termination and Survival

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

APPENDIX A: SAMPLE OPINION LETTER

[]

To: DigiCert, Inc.

2801 N. Thanksgiving Way
Suite 500
Lehi, UT 84043
Email: support@digicert.com
Fax: 801-705-0481

Re: Digital Certificate for *[Exact company name of client – see footnote 1]* Client

This firm

