# Certificate Policy/ Certification Practices Statement for Private PKI Services

DigiCert, Inc.
Version 3.11
August 18th, 2023
801 N. Thanksgiving Way
Suite 500
Lehi, UT 84043
USA
Tel: 1-801-877-2100
Fax: 1-801-705-0481
www.digicert.com

4.7.7 Notification of Certificate Issuance by the CA to Other Entities ..... 24
4.8 CERTIFICA

7.1 CERTIFICATE PROFILE ..... 43
7.1.1 Version Number(s) ..... 43
7.1.2 Certificate Extensions ..... 43
7.1.3 Algorithm Object Identifiers ..... 43
7.1.4 Name Forms

9.4.1 Privacy Plan ..... 47
9.4.2 Information Treated as Private ..... 47
9.4.3 Information Not Deemed Private ..... 47
9.4.4 Responsibility to Protect

# INTRODUCTION

## *1.1 OVERVIEW*

This document is the DigiCert, Inc. (“DigiCert”) Certificate Policy/Certification Practices Statement (CP/CPS) for Private

| | | |
|---|---|---|
| 29-September-2021 | Clarification of Verified Mark Certificate practices, including disclosure of Problem Reporting Mechanism and updated version of Verified Mark Certificate Requirements. | 3.5 |

Subscribers for Private PKI External Programs are defined within their respective CP documents, guidelines, and within the legal agreements between the associated parties. Parties identified in those documents as functioning in these roles are required to abide by those definitions as enforced in the additional supportive

# PUBLICATION AND REPOSITORY RESPONSIBILITIES

## *2.1 REPOSITORIES*

CRLs and OCSP responses are available through online resources 24 hours a day, 7 days a week with systems described in Section 5 to minimize downtime.

CRL will be used to communicate revocations of VMCs to maintain privacy when requested by Subscribers.

## *2.2 PUBLICATION OF CERTIFICATION INFORMATION*

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

- On the web via URIs included in the certificates themselves
- By email to support@digicert.com
- By mail addressed to: DigiCert, Inc., Suite 500, 2801 N. Thanksgiving Way, Lehi, Utah 84043
- By telephone Tel: 1-801-877-2100
- By fax: 1-801-705-0481

DigiCert protects information not intended for public dissemination through the request process listed above.

## *2.3 TIME*

- the associated Public Key has not reached the end of its

### 4.7.2 *Who May Request Certification of a New Public Key*

DigiCert will only accept re-key requests from the subject of the certificate or the PKI sponsor. DigiCert may initiate a certificate re-key at the request of the certificate subject or in DigiCert's own discretion.

### 4.7.3 *Processing Certificate Re-keying Requests*

DigiCert may re-use existing verification information unless re-verification and authentication is required by contract or if DigiCert believes that the information has become inaccurate. DigiCert or the RA will confirm the identity of the Subscriber in accordance with the requirements specified in the CP and contracts for the authentication of an original Certificate Application. The RAs will describe this practice in their respective RPS.

CA Certificate re-key requests will be approved according to the requirements in the associated contract, guidelines, requirements, and CP.

### 4.7.4 *Notification of Certificate Issuance to Subscriber*

DigiCert notifies the Subscriber within a reasonable time after the certificate issues or per the requirements within the legal agreements and External Program CP.

### 4.7.5 *Conduct Constituting Acceptance of a Re-keyed Certificate*

Issued certificates are considered accepted 30 days after the certificate is re-keyed, or earlier upon use of the certificate when evidence exists that the Subscriber used the certificate.

### 4.7.6 *Publication of the Issued Certificate by the CA*

DigiCert publishes re-keyed certificates by delivering them to Subscribers or per the requirements within the legal agreements and program CP.

### 4.7.7 *Notification of Certificate Issuance by the CA to Other Entities*

RAs may receive notification of a certificate's re-key if the RA was involved in the issuance process. The applicable community is notified when a CA Certificate is issued for that community.

## 4.8 *CERTIFICATE MODIFICATION*

### 4.8.1 *Circumstances for Certificate Modification*

Modifying a certificate means creating a new certificate for the same subject with information that BT/F3 9.96 Tf1 0 0 1 320.45



publishes

RAs that modify certificates will specify the compliant practice in their RPS according to this CP/CPS and the CP for the certificate type and subject.

#### 4.8.3 *Processing Certificate Modification Requests*

After receiving a request for modification, DigiCert or an RA

certificate;

9. DigiCert ceased operations and did not arrange for another certificate authority to provide revocation support for the certificates;

10. DigiCert's right to manage certificates under applicable industry standards was terminated (unless arrangements have been made to continue revocation services and maintain the CRL/OCSP Repository);

11. Any information appearing in the certificate was or became inaccurate or misleading;
12. The technical content or format of the certificate presents an unacceptable

information, as applicable. Typically, revocation information for CA Certificates is published within 24 hours of notification based on the requirements of the contracts and relevant CP.

#### 4.9.13 *Circumstances for Suspension*

Not applicable.

#### 4.9.14 *Who Can Request Suspension*

Not applicable.

#### 4.9.15 *Procedure for Suspension Request*

Not applicable.

#### 4.9.16 *Limits on Suspension Period*

Not applicable.

### 4.10 *CERTIFICATE STATUS SERVICES*

#### 4.10.1 *Operational Characteristics*

Certificate status information may be available via CRL and OCSP responder. The Repository is available via HTTP or another accessible transfer protocol as specified in section 2.1. The serial number of a revoked certificate remains on the CRL until one additional CRL is published after the end of

# FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

## *5.1 PHYSICAL CONTROLS*

### *5.1.1 Site Location and Construction*

DigiCert performs its CA operations from secure and geographically diverse commercial data centers. The data centers are equipped with logical and physical controls that make DigiCert's CA operations inaccessible to non-trusted personnel as described in section 5.1.2. DigiCert operates under a security policy designed to detect, deter, and prevent unauthorized access to DigiCert's operations.

### *5.1.2 Physical Access*

DigiCert protects its equipment from unauthorized access and implements physical controls to reduce the risk of equipment tampering. The secure parts of DigiCert CA hosting facilities are protected using physical access controls making them accessible only to appropriately authorized individuals in layers of security as described here. Access to secure areas of the buildings requires the use of an "access" or "pass" card. The buildings are equipped with motion detecting sensors, and the exterior and internal passageways of the buildings are under constant video surveillance in each subsequent area. DigiCert securely stores all removable media and paper containing sensitive plain-text information related to its CA operations in secure

### 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 and unauthorized physical access. Backup files are created on a regular basis. DigiCert's backup files are maintained at locations separate from DigiCert's primary data operations facility.

### 5.1.7 *Waste Disposal*

CA media and documentation that are no longer needed for operations are destroyed in a secure manner. All unnecessary copies of printed sensitive information are shredded on-site before disposal.

### 5.1.8 *Off-site Backup*

DigiCert maintains at least one full backup and 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 in safe deposit boxes that are accessible only by trusted 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 PKI operations. All personnel in trusted roles must be free from conflicts of interest that might prejudice

### 5.2.2 *Number of Persons Required per Task*

CA keys will be under personnel control according to the requirements in the relevant legal agreements, CPs, technical specification documents, requirement(s), and this CP/CPS.

DigiCert requires that at least one person in a trusted role perform actions such as activating DigiCert's Private Keys, generating a CA key pair, or backing up a DigiCert private key, unless otherwise specified by the documents referenced above. When multi person control is required, one person must be the CA Administrator, the other cannot be an Internal Auditor. The Internal Auditor may serve to fulfill the requirement of multiparty control for physical

For Trusted Roles maintained by RAs external to DigiCert, these requirements will be addressed in their

### 5.4.8 *Vulnerability Assessments*

DigiCert performs annual risk assessments that identify and assess reasonably foreseeable internal and external 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

19. Export of Private Keys,
20. Approval or rejection of a certificate status change request,
21. Appointment of an individual to a trusted role,
22. Destruction of a cryptographic module,
23. Certificate compromise notifications,
24. Remedial action taken as a result of violations of physical security, and
25. Violations of the CP/CPS.

### 5.5.2 *Retention Period for Archive*

Archive records are kept in accordance with the community requirements.

## 5.6 KEY CHANGEOVER

Key changeover procedures enable the smooth transition from expiring CA Certificates to new CA Certificates. 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, OCSP responses, 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 helps minimize any adverse effects from CA Certificate expiration.

A CA Certificate may be renewed if permitted by the applicable communit

## 5.8 CA OR RA TERMINATION

Before terminating its CA activities, DigiCert will:

1. Provide notice and information about the termination by sending notice by email to its customers; and
2. Transfer all responsibilities to a qualified successor entity.

If a qualified successor entity does not exist, DigiCert will:

1. transfer those functions capable of being transferred to a reliable third party and arrange to preserve all relevant records with a reliable third party or a government, regulatory, or legal body with appropriate authority;
2. revoke all certificates that are still un-revoked or un-expired on a date as specified in the notice and publish final CRLs;
3. destroy all Private Keys; and
4. make other necessary arrangements that are in accordance with this CP/CPS.

DigiCert has made arrangements to cover the costs associated with fulfilling these requirements in case DigiCert becomes bankrupt or is unable to cover the costs. Any requirements of this section that are varied by contract apply only the contracting parties.

# TECHNICAL SECURITY CONTROLS

## *6.1 KEY PAIR GENERATION AND INSTALLATION*

### *6.1.1 Key Pair Generation*

CA key pairs are generated by trusted roles and using a cryptographic hardware device or per section 5.2.2. Typically, if hardware is required,

## 6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

### 6.2.1 Cryptographic Module Standards and Controls

CA Private keys and generally protected using FIPS 140-2 Level 3 systems. External Program communities may elect a different standard for key protection, in which case that standard prevails. Private key holders must take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of such Private Keys in

## 6.4 ACTIVATION DATA

### 6.4.1 Activation Data Generation and Installation

DigiCert activates the cryptographic module containing its CA Private Keys

component will be used. All hardware and software (if applicable) are shipped under standard conditions to ensure delivery of the component directly to a trusted employee who ensures that the equipment is installed without opportunity for tampering.

Some of the PKI software components used by DigiCert are developed in-house or by consultants using standard software development methodologies. All such software is designed and developed in a controlled environment and subjected to quality assurance review. Other software is purchased commercial off-the-shelf (COTS). Quality assurance is maintained throughout the

# CERTIFICATE, CRL, AND OCSP PROFILES

DigiCert uses the

## 7.2 CRL PROFILE

### 7.2.1 Version number(s)

DigiCert issues

# OTHER BUSINESS AND LEGAL MATTERS

## *9.1 FEES*

### *9.1.1 Certificate Issuance or Renewal Fees*

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

### *9.1.2 Certificate Access Fees*

If not specified in the relevant legal agreements or CP of an associated third party, DigiCert may charge a

### *9.3.2 Information Not Within the Scope of Confidential Information*

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

### *9.3.3*

All intellectual property of entities participating in the DigiCert Private PKI remains the property of its respective owners as per the relevant legal agreements.

## 9.6 REPRESENTATIONS AND WARRANTIES

### 9.6.1 CA Representations and Warranties

Except as expressly stated in this CP/CPS or in a separate agreement with a Subscriber, DigiCert does not make any representations regarding its products or services. DigiCert represents, to the extent specified in this CP/CPS, that:

DigiCert:

- DigiCert complies, in all material aspects, with this CP/CPS and all applicable laws and regulations,
- DigiCert publishes and updates CRLs and OCSP responses on a regular basis,
- Does not warrant the accuracy, authenticity, completeness, or fitness of any unverified information,
- Is not responsible for information contained in a certificate except as stated in this CP/CPS,
- Does not warrant the quality, function, or performance of any software or hardware device, and
- Is not responsible for failing to comply with this CP/CPS because of circumstances outside of DigiCert's control.

### 9.6.2 RA Representations and Warranties

this CP/CPS, any applicable CP or guidelines, and the relevant Subscriber Agreement, including only installing SSL certificates on servers accessible at the domain listed in the certificate and not using code signing certificates to sign malicious code or any code that is downloaded without a user's consent, and

7. Promptly cease using the certificate and related Private Key after the certificate's expiration.

For VMC participants, Applicants can find the VMC Terms of Use ("VMC Terms") in

### *9.7 DISCLAIMERS OF WARRANTIES*

EXCEPT AS EXPRESSLY STATED IN SECTION 9.6.1, ALL CERTIFICATES AND ANY RELATED SOFTWARE AND SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE". TO THE MAXIMUM EXTENT PERMITTED BY LAW, DIGICERT DISCLAIMS ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING ALL WARRANTIES OF

- Subscriber's misuse of the certificate or Private Key.

### *9.9.3 Indemnification by Relying Parties*