DigiCert

Certificate Policy/ Certification Practices Statement for Private PKI Services

DigiCert, Inc.
Version 3.8
8/10/2022
801 N. Thanksgiving Way
Suite 500
Lehi, UT 84043
USA
Tel: 1-801-877-2100
Fax: 1-801-705-0481
www.digicert.com

Contents

1. INTRODUCTION

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

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
19-January-2022	Inclusion of VMC Requirements version 1.2.	3.6
05-April-2022	Inclusion of VMC Requirements version 1.4.	3.7
10-August-2022	Inclusion of additional recommended algorithms and conformance requirements of the MATTER program.	3.8

DigiCert is a certification authority (CA) that issues digital certificates. As a CA, DigiCert performs functions associated with both Private PKI Services and public key operations, including receiving applicable certificate requests, issuing, revoking and renewing a digital certificate, and maintaining, issuing, and publishing CRLs and OCSP responses. General information about DigiCert's products and services are available at https://www.digicert.com.

DigiCert Root Certificate Authorities and Intermediate CAs under the control of DigiCert are managed by the DigiCert Policy Authority (DCPA) which is composed of members of DigiCert management appointed by DigiCert's executive management. The DCPA is responsible for this CP/CPS0.008 Tw 0.14 0 T7a 0 Td( )Tj-0.008 Tc 0.008 Tw 0.16

outage, you have questions, or you believe our findings are incorrect please contact revoke@digicert.com.

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

“Subscriber” inf1rmer(as02 Tc -0.002 Tw 0 10.008 Tc 0.008 Tw 0.16 0 Td[(m)-16 (ean) 5.38 0 Td( )Tj-

2

3 IDENTIFICATION AND AUTHENTICATION

Certificates are issued with a subject Distinguished Name (DN) that complies with ITU X.500 standards. Some certificates may have a null subject DN if it includes at least one alternative name form that is marked critical. Policies on certificate field and extension information are specified in a separate Certificate Profile document or technical specification of the program.

DigiCert uses distinguished names to identify the subject (i.e. person, organization, device, or object) or issuer of the certificate.

Where required by the applicable CP or guidelines, Subscriber certificates will contain meaningful names with commonly understood semantics permitting the determination of the identity of the organization that is the Subject of the certificate by DigiCert and by designated RAs. RAs will describe this process in their associated RPS.

The subject name in CA Certificates match the issuer name in certificates issued by such DigiCert CAs, as required by [RFC 5280].

Except where requiTw 0.3 84828 -0 0 10 ba5 451 Tm[(A)7.4 (n)-0.5y2dTw 1 0 10 1 -0 0 10 Tw 1)0]8-T.c0.008 Tw 0.3 0 Td[(r) Tw 0 3

DigiCert may use any legal means of communication or investigation to ascertain the identity of an organizational or individual Applicant. DigiCert may refuse to issue a certificate in its sole discretion. Participating RAs must specify the validation methods used to verify identity information in their applicable RPS.

DigiCert establishes that the Applicant holds or controls the Private Key corresponding to the Public Key by performing signature verification or decryption on data purported to have been digitally signed or encrypted with the Private Key by using the Public Key associated with the certificate request.

Certificates generated by DigiCert require proof that the Subscriber possesses the private key. Typically, the RA verifies this by verifying the subscriber's digital signature on the PKCS #10 Certificate Signing Request (CSR) with the public key in the CSR. If DigiCert generates the key pair on behalf of the subscriber, proof of possession by the subscriber is not required.

The process of proving possession of the private key for end-entity certificates by RAs will be described in their respective RPS.

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 or an RA.

In no particular order, the enrollment process may include:

- Submitting a certificate application including the required documentation from the associated program,
- Generating a key pair,
- Delivering the public key of the key pair to DigiCert,
- Agreeing to the applicable Subscriber Agreement, and
- Paying any applicable fees.

After receiving a certificate application, DigiCert or an RA verifies the application information and other information in accordance with Section 3.2. If an RA assists in the verification, the RA must create and maintain records sufficient to establish that it has performed its required verification tasks and communicate the completion of such performance to DigiCert in accordance with sections 5.4 and 5.5. After verification is complete, DigiCert or the RA evaluates the corpus of information and decides whether or not to issue the certificate. DigiCert considers a source [illegible]

DigiCert may renew a certificate if:

- the associated Public Key has not reached the end of its validity period,
- the Subscriber and attributes are consistent, and
- the associated Private Key remains uncompromised.

DigiCert may also renew a certificate if a CA Certificate is re-keyed or as otherwise necessary to provide services to a customer. DigiCert may notify Subscribers prior to a certificate's expiration date. Certificate renewal requires payment of additional fees. In all cases, any renewal requirements are specified by the applicable CP or guidelines.

[illegible] (05 (r)-17 -0.008480 T[0 85 563 Tm-17W 3.52
(i)-10 (Td( )Tj0.00286c 0.008 Tw [(ar)-14 (e)]TJ0 Tc0 160 (ew)-1 (n)-10oes)-18 Tw 1.82 (.)]TJ0 Td( )Tj0.003.26 -0.002 Tw 0.2 0 Td[(C)5 (e)-10

[illegible]

recovery from key compromise. A CA Certificat

7. The certificate was not issued in accordance with the CP/CPS or applicable industry standards;
8. DigiCert received a lawful and binding order from a government or regulatory body to revoke the 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 risk; or
13. The Subscriber was added as a denied party or

    d. relevant legislation.

5. If DigiCert determines that revocation is appropriate, DigiCert personnel revoke the certificate and update the CRL.

.

No stipulation.

Revocation information for CA Certificates are published after creation of the appropriate CRL and OCSP 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.

Not applicable. .0 5845

DigiCert performs its CA operations from secure and geographically diverse commercial data centers. The data centers are equipped with logical

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.

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.

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.

Personnel acting in trusted roles include CA and RA system administ min4.3 (l)15 (o)1 Tw 0.91.42 0 Td( )DC / 0 Tb].91.42 0 T an Internal Auditor) take action requiring a trusted role, such as activating DigiCert's 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.

All personnel are required to authenticate themselves to CA and RA systems before they are allowed access to systems necessary to perform their trusted roles. External RA system access and control by trusted roles are specified in the respective RPS.

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 key management or CA administration.

For RAs, the separation of duties for trusted roles are addressed in their respective RPS.

The DCPA is responsible and accountable for DigiCert's PKI operations and ensures compliance with this CP/CPS. DigiCert's personnel and management practices provide reasonable assurance of the trustworthiness and compTetence of its employees and of the satisfactory
T

the person’s job functions and covers:

1. basic Public Key Infrastructure (PKI) knowledge,

2. software versions used by DigiCert,

3. authentication and verification policies and procedures,

4. DigiCert security principals and mechanisms,

5. disaster recovery and business continuity procedures,

6. common threats to the validation process, including phishing and other social engineering tactics, and

7. applicable industry and government guidelines.

Training is provided via a mentoring process involving senior members of the team to which the employee belongs.

DigiCert maintains records of who received training and what level of training was completed. Registration Officers must have the minimum skills necessary to satisfactorily perform validation duties before being granted validation privileges. Where competence is demonstrated in lieu of training, DigiCert maintains supporting documentation.

Employees must maintain skill levels that are consistent with industry-relevant training and performance programs in order to continue acting in trusted roles. DigiCert makes all employees acting in trusted roles aware of any changes to DigiCert’s operations. If DigiCert’s operations change, DigiCert will provide documented training, in accordance with an executed training BDC /TT0 18Tf0-18.3 -1.18 Td(E)Tj-0.00umTd(1 (e)1 0 Td2.0n)Tj0 T

20.

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.

6

RAs with cryptographic modules will protect the Private Keys at the level specified in the relevant CP, legal agreements, this CP/CPS, and technical specification documents. These practices will be stated in their respective RPS.

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 off-site 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.

No stipulation.

No stipulation.

No stipulation.

CA private keys are transferred from one cryptographic module to another to perform CA key backup procedures in section 6.3.4.

All other keys are generated by and in a cryptographic modul(-0.003 Tc.1 (y)-0.003 Tc.1 (y)-0.003 Tc.1)n20m (n)4[(C)1 (A)]TJ0 [illegible]

[illegible]

processes if a certain number of failed password attempts occur. DigiCert protects the activation data for its private keys using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys. These details are maintained in the disaster recovery procedures. DigiCert maintains an audit trail of Secret Shares, and Shareholders participate in the maintenance of an audit trail.

DigiCert will follow the requirements of the associated legal agreements, CPs, and technical specification documents. If RAs handle activation data, they will follow the requirements of their associated legal agreements, the CP, this CP/CPS, and the related technical specification documents and state those practices in their respective RPS.

Computer security controls are required to ensure CA operations are performed as specified in the relevant contract agreements, CPs, and technical specification documents.

DigiCert secures its CA systems and authenticates and protects communications between its systems and trusted roles. DigiCert's CA servers and support-and-vetting workstations run on trustworthy systems that are configured and hardened using industry best practices.

No stipulation.

DigiCert has mechanisms in place to control and monitor the acquisition and development of its CA systems. Change requests require the approval of at least one administrator who is different from the person submitting the request. DigiCert only installs software on CA systems if the software is part of the CA's operation. CA hardware and software are dedicated to performing operations of the CA.

Vendors are selected based on their reputation in the market, ability to deliver quality product, and likelihood of remaining viable in the future. Management is involved in the vendor selection and purchase decision process. Non-PKI hardware and software is purchased without identifying the purpose for which the component will be used. All hardware and software 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 process through testing and documentation or by purchasing from trusted vendors as discussed above.

Updates of equipment and software are purchased or developed in the same manner as the original equipment or software and are installed and tested by trusted and trained personnel. All hardware and software essential to DigiCert's operations is scanned for malicious code on first use and periodically thereafter.

DigiCert has mechanisms in place to control and monitor the security-related configurations of its CA systems. 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. DigiCert verifies the integrity of software used with its CA processes at least once a week.

7 CERTIFICATE, CRL, AND OCSP PROFILES

DigiCert uses the ITU X.509, version 3 standard to construct digital certificates for use within the DigiCert PKI. Specific certificate profiles are specified in DigiCert's profile documentation, technical specification documents, and in the relevant community's CP or requirements document.

All certificates are X.509 version 3 certificates. 0 TdcNucecificati0 Tw 3.86

DigiCert issues version 2 CRLs that contain the following fields:

Field	Value
Issuer Signature Algorithm	sha-1WithRSAEncryption [1 2 840 113549 1 1 5] OR sha-256WithRSAEncryption [1 2 840 113549 1 1 11] OR ecdsa-with-sha256 [1 2 840 10045 4 3 2] OR ecdsa-with-sha384 [1 2 840 10045 4 3 3]
Issuer Distinguished Name	[As appropriate]
thisUpdate	CRL issue date in UTC format
nextUpdate	Date when the next CRL will issue in UTC format.
Revoked Certificates List	List of revoked certificates, including the serial number and revocation date
Issuer's Signature	[Signature]

CRLs have the following extensions:

Extension	Value
CRL Number	Never repeated monotonically increasing integer
Authority Key Identifier	Same as the Authority Key Identifier listed in the certificate
Invalidity Date	Optional date

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

Audits referencing this CP/CPS shall cover DigiCert’s CA systems, Sub CAs, and OCSP Responders.

RAs must comply with the audit requirements as specified in the legal agreements, the CP, relevant technical specification requirements, and this CP/CPS. How those audit requirements are met will be stipulated in their RPS.

As agreed to with the customer in the relevant legal agreements, CP, and technical specification documents. RAs must comply with the audit requirements as specified in the legal agreements, the CP, relevant technical specification requirements, and this CP/CPS. How those audit requirements are met will be stipulated in their RPS.

As agreed to with the customer in the relevant legal agreements, CP, requirement(s), and technical specification documents.

RAs must comply with the audit requirements as specified in the legal agreements, the CP, relevant technical specification requirements, and this CP/CPS. How those audit requirements are met will be stipulated in their RPS.

Any audit covers DigiCert's business practices disclosure, the integrity of DigiCert's PKI operations, and DigiCert’s compliance with relevant standards.

RAs must comply with the audit requirements as specified in the legal agreements, the CP, relevant technical specification will - (

9 OTHER BUSINESS AND LEGAL MATTERS

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

If not specified in the relevant legal agreements or CP of an associated third party, DigiCert may charge a reasonable fee for access to its certificate databases.

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 certificate status information via OCSP.

No stipulation.

As set forth in the relevant customer agreement with DigiCert.

DigiCert maintains Commercial G0 Tci-0 0 (ins)-8 (C)5 (o)13 (m)-6 (m)-6 (e)10 (r)-4 (c)3 (i8)]TJ/T41Lr Comm[illegible]

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

DigiCert's employees, agents,

All secret shares (distributed elements) of the DigiCert Private Keys are the property of DigiCert.

All intellectual property of entities participating in the DigiCert Private PKI remains the property of its

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

NOTHING HEREIN LIMITS LIABILITY RELATED TO (I) DEATH OR PERSONAL INJURY RESULTING FROM DIGICERT’S NEGLIGENCE OR (II) FRAUD COMMITTED BY DIGICERT. EXCEPT AS STATED ABOVE, ANY ENTITY USING A DIGICERT CERTIFICATE OR SERVICE WAIVES ALL LIABILITY OF DIGICERT RELATED TO SUCH USE, PROVIDED THAT DIGICERT HAS MATERIALLY COMPLIED WITH THIS CP/CPS IN PROVIDING THE CERTIFICATE OR SERVICE. Subscriber

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

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

TERM AND TERMINATION

This CP/CPS and any amendments to the CP/CPS are effective when adopted by the DCPA and remain in effect until replaced with a newer version.

This CP/CPS and any amendments remain in effect until replaced by a newer version.

DigiCert will communicate the conditions and effect of this CP/CPS's termination via email or 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 agreements remain effective until the certificate is revoked or expired, even if this CP/CPS terminates.

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

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.

Clauses for force majeure will be added to the extent of applicable law for relevant parties and affiliates within the associated legal agreements.