DigiCert

Certification Practices Statement for

Private PKI Services

TABLE OF CONTENTS

1. INTRODUCTION

1.1. OVERVIEW

This document is the DigiCert, Inc. ("DigiCert") Certification Practices Statement (CPS) for Private PKI Services that outlines the principles and practices related to DigiCert's certification of non-cross-certified and non-publicly trusted X.509 digital certificates.

This CPS is only one of several documents that control DigiCert's certification services. Other important documents include both private and public documents, such as DigiCert's agreements with its customers, relying party agreements, and DigiCert's privacy policy. DigiCert may provide additional certificate policies or certification practice statements. These supplemental policies and statements are available to applicable users or relying parties.

1.2. DOCUMENT NAME AND IDENTIFICATION

This document is the DigiCert Certification Practices Statement for Private PKI Services and has been approved for publication by the DigiCert Policy Authority (DCPA) as of the date indicated on the cover page.

1.3. PKI PARTICIPANTS

1.3.1. Certification Authorities

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 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.

1.3.2. Registration Authorities and Other Delegated Third Parties

DigiCert may delegate the performance of certain functions to Registration Authorities (RA) and other third parties to request certificates and/or perform identification and authentication for end-user certificates. The specific role of an RA or delegated third party varies greatly between entities, ranging from simple translation services to actual assistance in gathering and verifying Applicant information. Some RAs operate identity management systems (IdMs) and may manage the certificate lifecycle for end-users. Specific roles of each RA under a private PKI depend highly on the contract with the private PKI party.

1.3.3. Subscribers

Subscribers use DigiCert's services and PKI to support transactions and communications. Subscribers are not always the party identified in a certificate, such as when certificates are issued to an organization's employees. The *Subject* of a certificate is the party named in the certificate. A *Subscriber*, as used herein, refers to both the Subject of the certificate and the entity that contracted with DigiCert for the certificate's issuance.

1.3.4. Relying Parties

Relying parties are entities that act in reliance on a certificate and/or digital signature issued by DigiCert. Relying parties are defined by the community supported by the private PKI infrastructure and by contract with DigiCert.

1.3.5. Other Participants

No stipulation.

1.4. CERTIFICATE USAGE

A *digital certificate* (or *certificate*) is formatted data that cryptographically binds an identified subscriber with a Public Key. A digital certificate allows an entity taking part in an electronic transaction to prove its identity to other participants in such transaction.

1.4.1. Appropriate Certificate Uses

Certificates issued pursuant to this CPS may be used for all legal authentication, encryption, access control, and digital signature purposes, as designated by the key usage and extended key usage fields found within the certificate. However, the sensitivity of the information processed or protected by a certificate varies greatly, and each relying party must evaluate the application environment and associated risks before deciding on whether to use a certificate issued under this CPS. The exact use of each Certificate is left to the discretion of the community for which the PKI is operated.

1.4.2. Prohibited Certificate Uses

Certificates do not guarantee that the Subject is trustworthy, honest, reputable in its business dealings, compliant with any laws, or safe to do business with. A certificate only establishes that the information in the certificate was verified as reasonably correct when the certificate issued.

1.5. POLICY ADMINISTRATION

1.5.1. Organization Administering the Document

This CPS and the documents referenced herein are maintained by the DCPA, which can be contacted at:

DigiCert Policy Authority
Suite 500
2801 N. Thanksgiving Way
Lehi, UT 84043 USA
Tel: 1-801-701-9600 Fax: 1-801-705-0481

1.5.2. Contact Person

Attn: Legal Counsel DigiCert Policy Authority
Suite 500
2801 N. Thanksgiving Way
Lehi, UT 84043 USA

1.5.3. Person Determining CPS Suitability for the Policy

The DCPA determines the suitability and applicability of this CPS based on the contract with the customer for which the PKI is operated and any relevant audits. The DCPA is responsible for the PKI's compliance with this CPS.

1.5.4. CPS Approval Procedures

The DCPA approves the CPS and any amendments. Amendments are made after the DCPA has reviewed the amendments' consistency with relevant contracts. The DCPA determines whether an amendment to this CPS is consistent with a contract, requires notice, or requires an OID change.

1.6. DEFINITIONS AND ACRONYMS

1.6.1. Definitions

"Applicant" means an entity applying for a certificate.

"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.

"Subscriber" means either the entity identified as the subject in the certificate or the entity that is receiving DigiCert's time-stamping services.

1.6.2. Acronyms

CA	Certificate Authority or Certification Authority
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DCPA	DigiCert Policy Authority
FIPS	(US Government) Federal Information Processing Standard
HSM	Hardware Security Module
IdM	Identity Management System
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
PKCS	Public Key Cryptography Standard
RA	Registration Authority
SHA	Secure Hashing Algorithm
SSL	Secure Sockets Layer
TLS	Transport Layer Security
URL	Uniform Resource Locator
X.509	The ITU-T standard for Certificates and their corresponding authentication framework

1.6.3. References

No stipulation.

2. 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.

2.2.   PUBLICATION OF CERTIFICATION INFORMATION
The DigiCert certificate services and the repository are accessible through several means of communication:

1. On the web via URIs included in the certificates themselves

2. By email to support@digicert.com

3. By mail addressed to: DigiCert, Inc., Suite 500, 2801 N. Thanksgiving Way, Lehi, Utah 84043

4. By telephone Tel: 1-801-877-2100

5. By fax: 1-801-705-0481

2.3.   TIME OR FREQUENCY OF PUBLICATION
CRLs for end-user certificates are issued at least once per day. CRLs for CA certificates are issued in accordance with the applicable customer agreement. Typically, this is every 6 months and also within 18 hours if a CA certificate is revoked. Under special circumstances, DigiCert may publish new CRLs prior to the scheduled issuance of the next CRL. New or modified versions of this CPS, Subscriber Agreements, or Relying Party Warranties are typically published within seven days after their approval.

2.4.   ACCESS CONTROLS ON REPOSITORIES
Read-only access to the repository is unrestricted. Logical and physical controls prevent unauthorized write access to repositories.

3. IDENTIFICATION AND AUTHENTICATION

3.1.   NAMING

3.1.1. Types of Names
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.

3.1.2. Need for Names to be Meaningful
DigiCert uses distinguished names to identify the subject (i.e. person, organization, device, or object) or issuer of the certificate.

3.1.3. Anonymity or Pseudonymity of Subscribers
DigiCert may issue anonymous and pseudonymous end-entity certificates provided that they are not prohibited by policy and any applicable name space uniqueness requirements are met.

3.1.4. Rules for Interpreting Various Name Forms
Distinguished Names in certificates are interpreted using X.500 standards and ASN.1 syntax. *See* RFC 2253 and RFC 2616 for further information on how X.500 distinguished names in certificates are interpreted as Uniform Resource Identifiers and HTTP references.

3.1.5. Uniqueness of Names
The uniqueness of each subject name in a certificate depends on the contract with the customer. Typically, uniqueness is maintained through the domain name in the certificate, email address in the certificate, or a

combination of the certificate's subject information.

3.1.6. Recognition, Authentication, and Role of Trademarks

Subscribers may not request certificates with content that infringes on the intellectual property rights of another entity. Unless otherwise specifically stated in an agreement with a customer, 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 an organizational or individual Applicant. DigiCert may refuse to issue a Certificate in its sole discretion.

3.2.1. Method to Prove Possession of Private Key

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.

3.2.2. Authentication of Organization Identity

As set forth in the applicable customer agreement. Verification depends on the community ordering the certificate.

3.2.3. Authentication of Individual Identity

Verification of individual identities depends on the requirements of the community ordering the certificates. Verification may include confirmation of an email address, through record checks of the individual's identity, or other similar means.

3.2.3.1. Authentication for Role-based Client Certificates

DigiCert may issue certificates that identify a specific role that the Subscriber holds instead of a specific individual (e.g., Chief Information Officer is a unique individual whereas Program Analyst is not). These role-based certificates are used when non-repudiation is desired. A sponsor of the role-based Certificates is verified in accordance with Section 3.2.3 above.

3.2.3.2. Authentication for Group Client Certificates

DigiCert issues group certificates (a certificate that corresponds to a Private Key that is shared by multiple Subscribers) if several entities are acting in one capacity and if non-repudiation is not required. A sponsor for the group Certificate is verified under Section 3.2.3 before the Certificate is issued. The sponsor must maintain and continuously update a list of Subscribers with access to the private key and account for the time period during which each Subscriber had control of the key.

3.2.3.3. Authentication of Devices

No stipulation.

3.2.4. Non-verified Subscriber Information

Private client certificates may contain non-verified subscriber information.

3.3.   IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1. Identification and Authentication for Routine Re-key

Subscribers may request re-key of a certificate prior to a certificate's expiration. After receiving a request for re-key, DigiCert creates a new certificate with the same certificate contents except for a new Public Key and, optionally, an extended validity period. If the certificate has an extended validity period, DigiCert may perform some revalidation of the Applicant but may also rely on information previously provided or obtained.

3.4.   IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

DigiCert or an RA authenticates all revocation requests. DigiCert may authenticate revocation requests by referencing the use of the Private Key corresponding to the Certificate's Public Key, regardless of whether the associated Private Key is compromised.

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

4.1.2. Enrollment Process and Responsibilities

In no particular order, the enrollment process may include:

- Submitting a certificate application,

- Generating a key pair,

- Delivering the public key of the key pair to DigiCert,

- Agreeing to the applicable Subscriber Agreement, and

- Paying any applicable fees.

4.2.   CERTIFICATE APPLICATION PROCESSING
4.2.1. Performing Identification and Authentication Functions

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. After verification is complete, DigiCert evaluates the corpus of information and decides whether or not to issue the certificate. DigiCert considers a source's availability, purpose, and reputation when determining whether a third party source is reasonably reliable.

4.2.2. Approval or Rejection of Certificate Applications

DigiCert may reject a certificate application if DigiCert believes that issuing the certificate could damage or diminish DigiCert's reputation or business.

4.2.3. Time to Process Certificate Applications

As specified in the relevant customer agreement. If the timeframe is not specified, DigiCert will usually complete the validation process and issue or reject a certificate application within two working days after receiving all of the necessary details and documentation from the Applicant, although events outside of the control of DigiCert can delay the issuance process.

4.3.   CERTIFICATE ISSUANCE

4.3.1. CA Actions during Certificate Issuance

Issuance is completed using the appropriate CA certificate. After issuance is complete, the certificate is stored in a database and sent to the Subscriber.

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

DigiCert may deliver certificates in any secure manner within a reasonable time after issuance. Generally, DigiCert delivers certificates by providing the Subscriber a hypertext link to a user id/password-protected location where the subscriber may log in and download the certificate or via email to the email address designated by the Subscriber during the application process.

4.4. CERTIFICATE ACCEPTANCE

4.4.1. Conduct Constituting Certificate Acceptance

Subscribers are solely responsible for installing the issued certificate on the Subscriber's computer or hardware security module. Certificates are considered accepted 30 days after the certificate's issuance, or earlier upon use of the certificate when evidence exists that the Subscriber used the certificate.

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 may receive notification of a certificate's issuance if the RA was involved in the issuance process.

4.5. KEY PAIR AND CERTIFICATE USAGE

4.5.1. Subscriber Private Key and Certificate Usage

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 in accordance with their intended purpose.

4.5.2. Relying Party Public Key and Certificate Usage

DigiCert does not warrant that any third party software will support or enforce the controls and requirements found herein. A Relying Party should use discretion when relying on a certificate and should consider the totality of the circumstances and risk of loss prior to relying on a certificate. If the circumstances indicate that additional assurances are required, the Relying Party must obtain such assurances before using the certificate.

4.6. CERTIFICATE RENEWAL

4.6.1. Circumstance for Certificate Renewal

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.

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's certificates. DigiCert may renew a certificate without a corresponding request if the signing certificate is re-keyed.

4.6.3. Processing Certificate Renewal Requests

Renewal application requirements and procedures are generally the same as those used during the certificate's original issuance. DigiCert may refuse to renew a certificate if it cannot verify any rechecked information. If an individual is renewing a client certificate and the relevant information has not changed, then DigiCert does not require any additional identity vetting. If the Private Key and domain information has not changed, the Subscriber may renew an SSL/TLS server certificate using a previously issued certificate or provided CSR.

4.6.4. Notification of New Certificate Issuance to Subscriber

DigiCert may deliver the certificate in any secure fashion, typically by email or by providing the Subscriber a hypertext link to a user id/password-protected location where the subscriber may log in and download the certificate.

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

Renewed certificates are considered accepted 30 days after the certificate'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.

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

RAs may receive notification of a certificate's renewal if the RA was involved in the issuance process.

4.7.   CERTIFICATE RE-KEY

4.7.1. Circumstance for Certificate Rekey

Re-keying a certificate consists of creating a new certificate with a new public key and serial number while keeping the subject information the same. The new certificate may have a different validity date, key identifiers, CRL and OCSP distribution points, and signing key.

4.7.2. Who May Request Certificate Rekey

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 Rekey 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.

4.7.4. Notification of Certificate Rekey to Subscriber

DigiCert notifies the Subscriber within a reasonable time after the certificate issues.

4.7.5. Conduct Constituting Acceptance of a Rekeyed Certificate

Issued certificates are considered accepted 30 days after the certificate is rekeyed, 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 rekeyed certificates by delivering them to Subscribers.

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

RAs may receive notification of a certificate's rekey if the RA was involved in the issuance process.

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 differs slightly from the old certificate (e.g., changes to email address or non-essential parts of names or attributes) provided that the modification otherwise complies with this CPS. The new certificate may have the same or a different subject public key.

4.8.2. Who May Request Certificate Modification
DigiCert modifies certificates at the request of certain certificate subjects or in its own discretion. DigiCert does not make certificate modification services available to all Subscribers.

4.8.3. Processing Certificate Modification Requests
After receiving a request for modification, DigiCert verifies any changed information in accordance with section 3.2.

4.8.4. Notification of Certificate Modification to Subscriber
DigiCert notifies the Subscriber within a reasonable time after the certificate issues.

4.8.5. Conduct Constituting Acceptance of a Modified Certificate
Modified certificates are considered accepted 30 days after the certificate is modified, or earlier upon use of the certificate when evidence exists that the Subscriber used the certificate.

4.8.6. Publication of the Modified Certificate by the CA
DigiCert publishes modified certificates by delivering them to Subscribers.

4.8.7. Notification of Certificate Modification by the CA to Other Entities
RAs may receive notification of a certificate's modification if the RA was involved in the issuance process.

4.9. CERTIFICATE REVOCATION AND SUSPENSION

4.9.1. Circumstances for Revocation
Revocation of a 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 the identity and authority of the entity requesting revocation. DigiCert may revoke any certificate in its sole discretion, including if DigiCert believes that:

1. The Subscriber requested revocation of its certificate;

2. The Subscriber did not authorize the original certificate request and did not retroactively grant authorization;

3. Either the Private Key associated with the certificate or the Private Key used to sign the certificate was compromised or misused;

4. The Subscriber breached a material obligation under the CPS or the relevant agreement;

5. Either the Subscriber's or DigiCert's obligations under the CPS are delayed or prevented by circumstances beyond the party's reasonable control, including computer or communication failure, and, as a result, another entity's information is materially threatened or compromised;

6. The Subscriber, sponsor, or other entity that was issued the certificate has lost its rights to a name, trademark, device, IP address, domain name, or other attribute that was associated with the certificate;

7. The certificate was not issued in accordance with the 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 prohibited person to a blacklist or is operating from a destination prohibited under the laws of the United States.

4.9.2. Who Can Request Revocation

Any appropriately authorized party, such as a recognized representative of a subscriber or cross-signed partner, may request revocation of a certificate. DigiCert may revoke a certificate 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.

4.9.3. Procedure for Revocation Request

DigiCert processes a revocation request as follows:

1. DigiCert logs the identity of entity making the request or problem report and the reason for requesting revocation. DigiCert may also include its own reasons for revocation in the log.

2. DigiCert may request confirmation of the revocation from the Subscriber or a known administrator, where applicable, via out-of-band communication (e.g., telephone, fax, etc.).

3. If the request is authenticated as originating from the Subscriber, DigiCert revokes the certificate.

4. For requests from third parties, DigiCert personnel begin investigating the request and decide whether revocation is appropriate based on the following criteria:

    a. the nature of the alleged problem,

    b. the number of reports received about a particular certificate,

    c. 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

    d. relevant legislation.

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

DigiCert maintains a continuous 24/7 ability to internally respond to any high priority revocation requests. If appropriate, DigiCert forwards complaints to law enforcement.

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.

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. Other certificates are revoked as quickly as practical after validating the revocation request.

4.9.6. Revocation Checking Requirement for Relying Parties

No stipulation.

4.9.7. CRL Issuance Frequency

CRLs are generally published at least every 24 hours.

4.9.8. Maximum Latency for CRLs

CRLs for certificates issued to end entity subscribers are posted automatically to the online repository within a commercially reasonable time after generation, usually within minutes of generation. Regularly scheduled CRLs are posted prior to the nextUpdate field in the previously issued CRL of the same scope.

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 Related to Key Compromise

No stipulation.

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 serial number of a revoked certificate remains on the CRL until one additional CRL is published after the end of the certificate's validity period.

4.10.2. Service Availability

Certificate status services are available 24x7 without interruption.

4.10.3. Optional Features

OCSP Responders may not be available for all certificate types.

4.11. END OF SUBSCRIPTION

A Subscriber's subscription service ends if its certificate expires or is revoked or if the applicable Subscriber Agreement expires without renewal.

4.12. KEY ESCROW AND RECOVERY

4.12.1. Key Escrow and Recovery Policy Practices

No stipulation.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5. 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. 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. 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. DigiCert securely stores all removable media and paper containing sensitive plain-text information related to its CA operations in secure containers in accordance with its Data Classification Policy.

The data centers where DigiCert's CA systems operate have security personnel on duty full time (24 hours per day, 365 days per year). Access to the data centers housing the CA platforms requires two-factor authentication—the individual must have an authorized access card and pass biometric access control authenticators. These biometric authentication access systems log each use of the access card.

DigiCert deactivates and securely stores its CA equipment when not in use. Activation data must either be memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module. Activation data is never stored with the cryptographic module or removable hardware associated with equipment used to administer DigiCert's private keys. Cryptographic hardware includes a mechanism to lock the hardware after a certain number of failed login attempts.

The DigiCert data centers are continuously attended. However, if DigiCert ever becomes aware that a data center is to be left unattended or has been left unattended for an extended period of time, DigiCert personnel will perform a security check of the data center to verify that:

1. DigiCert's equipment is in a state appropriate to the current mode of operation,

2. Any security containers are properly secured,

3. Physical security systems (e.g., door locks) are functioning properly, and

4. The area is secured against unauthorized access.

DigiCert's administrators are responsible for making these checks and must sign off that all necessary physical protection mechanisms are in place and activated. The identity of the individual making the check is logged.

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 diesel generators provide redundant backup power. DigiCert monitors capacity demands and makes projections about future capacity requirements to ensure that adequate processing power and storage are available. DigiCert's data center facilities use multiple load-balanced HVAC systems for heating, cooling, and air ventilation through perforated-tile raised flooring to prevent overheating and to maintain a suitable humidity level for sensitive computer systems.

5.1.4. Water Exposures

The cabinets housing DigiCert's CA systems are located on raised flooring, and the data centers are equipped with monitoring systems to detect excess moisture.

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

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 the impartiality of the DigiCert PKI's operations. Trusted roles are appointed by senior management. 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. 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, including enrollment, identity verification, and compliance with required issuance and revocation steps such as managing the certificate request queue and completing certificate approval checklists as identity vetting tasks are successfully completed.

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 CA and RA 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 CPS.

5.2.2. Number of Persons Required per Task

DigiCert requires that at least two people acting in a trusted role (one the CA Administrator and the other not 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.

5.2.3. Identification and Authentication for each Role

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.

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 key management or CA administration.

5.3. PERSONNEL CONTROLS

5.3.1. Qualifications, Experience, and Clearance Requirements

The DCPA is responsible and accountable for DigiCert's PKI operations and ensures compliance with this CPS. DigiCert's personnel and management practices provide reasonable assurance of the trustworthiness and competence of its employees and of the satisfactory performance of their duties.

5.3.2. Background Check Procedures

DigiCert verifies the identity of each employee appointed to a trusted role and performs a background check prior to allowing such person to act in a trusted role. DigiCert requires each individual to appear in-person before a human resources employee whose responsibility it is to verify identity. The human resources employee 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 include employment history, education, character references, social security number, previous residences, driving records and criminal background. Checks of previous residences are over the past three years. All other checks are for the previous five years. The highest education degree obtained is verified regardless of the date awarded. Based upon the information obtained during the background check, the human resources department makes an adjudication decision, with the assistance of legal counsel when necessary, as to whether the individual is suitable for the position to which they will be assigned. Background checks are refreshed and re-adjudication occurs at least every ten years.

5.3.3. Training Requirements

DigiCert provides skills training to all employees involved in DigiCert's PKI operations. The training relates to 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.

5.3.4. Retraining Frequency and Requirements

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 plan, to all employees acting in trusted roles.

5.3.5. Job Rotation Frequency and Sequence

No stipulation.

5.3.6. Sanctions for Unauthorized Actions

DigiCert employees and agents failing to comply with this CPS, whether through negligence or malicious intent, are subject to administrative or disciplinary actions, including termination of employment or agency and criminal sanctions. If a person in a trusted role is cited by management for unauthorized or inappropriate actions, the person will be immediately removed from the trusted role pending management review. After management has reviewed and discussed the incident with the employee involved, management may reassign that employee to a non-trusted role or dismiss the individual from employment as appropriate.

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 in trusted roles are provided with the documentation necessary to perform their duties. Personnel are also given access to information on internal systems and security documentation, identity vetting policies and procedures, discipline-specific books, treatises and periodicals, and other information.

5.4. AUDIT LOGGING PROCEDURES

5.4.1. Types of Events Recorded

DigiCert's systems require identification and authentication at system logon with a unique user name and password. Important system actions are logged to establish the accountability of the operators who initiate such actions.

DigiCert enables all essential event auditing capabilities of its CA applications in order to record the events listed below. If DigiCert's applications cannot automatically record an event, DigiCert implements 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. Event records are available to auditors as proof of DigiCert's practices.

Auditable Event
SECURITY AUDIT
Any changes to the audit parameters, e.g., audit frequency, type of event audited
Any attempt to delete or modify the audit logs
AUTHENTICATION TO SYSTEMS
Successful and unsuccessful attempts to assume a role
The value of maximum number of authentication attempts is changed
Maximum number of authentication attempts occur during user login
An administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts
An administrator changes the type of authenticator, e.g., from a password to a biometric
LOCAL DATA ENTRY
All security-relevant data that is entered in the system
REMOTE DATA ENTRY
All security-relevant messages that are received by the system
DATA EXPORT AND OUTPUT
All successful and unsuccessful requests for confidential and security-relevant information
KEY GENERATION
Whenever a CA generates a key (not mandatory for single session or one-time use symmetric keys)
PRIVATE KEY LOAD AND STORAGE
The loading of Component Private Keys
All access to certificate subject Private Keys retained within the CA for key recovery purposes
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE
SECRET KEY STORAGE
The manual entry of secret keys used for authentication
PRIVATE AND SECRET KEY EXPORT
The export of private and secret keys (keys used for a single session or message are excluded)
CERTIFICATE REGISTRATION
All certificate requests, including issuance, re-key, renewal, and revocation
Certificate issuance
Verification activities
CERTIFICATE REVOCATION
All certificate revocation requests
CERTIFICATE STATUS CHANGE APPROVAL AND REJECTION
CA CONFIGURATION
Any security-relevant changes to the configuration of a CA system component
ACCOUNT ADMINISTRATION
Roles and users are added or deleted
The access control privileges of a user account or a role are modified

CERTIFICATE PROFILE MANAGEMENT
All changes to the certificate profile
REVOCATION PROFILE MANAGEMENT
All changes to the revocation profile
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT
All changes to the certificate revocation list profile
Generation of CRLs and OCSP entries
TIME STAMPING
Clock synchronization
MISCELLANEOUS
Appointment of an individual to a Trusted Role
Designation of personnel for multiparty control
Installation of an Operating System, PKI Application, or Hardware Security Module
Removal or Destruction of HSMs
System Startup
Logon attempts to PKI Application
Receipt of hardware / software
Attempts to set or modify passwords
Backup or restoration of the internal CA database
File manipulation (e.g., creation, renaming, moving)
Posting of any material to a repository
Access to the internal CA database
All certificate compromise notification requests
Loading HSMs with Certificates
Shipment of HSMs
Zeroizing HSMs
Re-key of the Component
CONFIGURATION CHANGES
Hardware
Software
Operating System
Patches
Security Profiles
PHYSICAL ACCESS / SITE SECURITY
Personnel access to secure area housing CA component
Access to a CA component
Known or suspected violations of physical security
Firewall and router activities
ANOMALIES
System crashes and hardware failures
Software error conditions
Software check integrity failures
Receipt of improper messages and misrouted messages
Network attacks (suspected or confirmed)
Equipment failure
Electrical power outages
Uninterruptible Power Supply (UPS) failure
Obvious and significant network service or access failures
Violations of a CPS
Resetting Operating System clock

5.4.2. Frequency of Processing Log

At least once every two months, a DigiCert administrator reviews 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) prepares a written summary of the review. Any anomalies or irregularities found in the logs are investigated. The summaries include recommendations to DigiCert's operations management committee and are made available to DigiCert's auditors upon request. DigiCert documents any actions taken as a result of a review.

5.4.3. Retention Period for Audit Log

DigiCert retains audit logs on-site until after they are reviewed. The individuals who remove audit logs from DigiCert's CA systems are different than the individuals who control DigiCert's signature keys.

5.4.4. Protection of Audit Log

CA audit log information is retained on equipment until after it is copied by a system administrator. DigiCert's CA systems are configured to ensure that (i) only authorized people have read access to logs, (ii) only authorized people may archive audit logs, and (iii) audit logs are not modified. Audit logs are protected from destruction prior to the end of the audit log retention period and are retained securely on-site until transferred to a backup site. DigiCert's off-site storage location is a safe and secure location that is separate from the location where the data was generated.

5.4.5. Audit Log Backup Procedures

DigiCert makes regular backup copies of audit logs and audit log summaries and saves a copy of the audit log off-site on at least a monthly basis.

5.4.6. Audit Collection System (internal vs. external)

Automatic audit processes begin on system startup and end at system shutdown. If an automated audit system fails and the integrity of the system or confidentiality of the information protected by the system is at risk, DigiCert's Administrators and the DCPA shall be notified and the DCPA will consider suspending the CA's or RA's operations until the problem is remedied.

5.4.7. Notification to Event-causing Subject

No stipulation.

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 policies, procedures, information systems, technology, and other arrangements that DigiCert has in place to control such risks. DigiCert's Internal Auditors review the security audit data checks for continuity. 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.

5.5. RECORDS ARCHIVAL

DigiCert complies with all record retention policies that apply by law. DigiCert includes sufficient detail in all archived records to show that a certificate was issued in accordance with this CPS.

5.5.1. Types of Records Archived

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

1. Accreditations of DigiCert,

2. CP and 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. CRL and OCSP entries,

13. Data or applications necessary to verify an archive's contents,

14. Compliance auditor reports,

15. Changes to DigiCert's audit parameters,

16. Any attempt to delete or modify audit logs,

17. Key generation, destruction, storage, backup, and recovery,

18. Access to Private Keys for key recovery purposes,

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 CPS.

5.5.2. Retention Period for Archive
No stipulation.

5.5.3. Protection of Archive
Archive records are stored at a secure off-site location and are maintained in a manner that prevents unauthorized modification, substitution, or destruction. Archives are not released except as allowed by the DCPA or as required by law. DigiCert maintains any software application required to process the archive data until the data is either destroyed or transferred to a newer medium.

If DigiCert needs to transfer any media to a different archive site or equipment, DigiCert will maintain both archived locations and/or pieces of equipment until the transfer are complete. All transfers to new archives will occur in a secure manner.

5.5.4. Archive Backup Procedures

On at least an annual basis, DigiCert creates an archive disk of the data listed in section 5.5.1 by grouping the data types together by source into separate, compressed archive files. DigiCert stores the archive disk in a secure off-site location for the duration of the set retention period.

5.5.5. Requirements for Time-stamping of Records

DigiCert automatically time-stamps archived records with system time (non-cryptographic method) as they are created. DigiCert synchronizes its system time at least every eight hours using a real time value distributed by a recognized UTC(k) laboratory or National Measurement Institute.

5.5.6. Archive Collection System (internal or external)

Archive information is collected internally by DigiCert.

5.5.7. Procedures to Obtain and Verify Archive Information

Details concerning the creation and storage of archive information are found in section 5.5.4. After receiving a request made for a proper purpose by a Customer, its agent, or a party involved in a dispute over a transaction involving the PKI, DigiCert may elect to retrieve the information from archival. DigiCert may elect to transmit the relevant information via a secure electronic method or courier, or it may also refuse to provide the information in its discretion and may require prior payment of all costs associated with the data.

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.

5.7. COMPROMISE AND DISASTER RECOVERY

5.7.1. Incident and Compromise Handling Procedures

DigiCert maintains incident response procedures to guide personnel in response to security incidents, natural disasters, and similar events that may give rise to system compromise. DigiCert reviews, tests, and updates its incident response plans and procedures on at least an annual basis.

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

DigiCert makes regular system backups on at least a weekly basis and maintains backup copies of its Private Keys, which are stored in a secure, off-site location. If DigiCert discovers that any of its 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 DigiCert determines that a continued 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 Private Keys has been comprised or lost, then an emergency response team will convene and assess the situation to determine the degree and scope of the incident and take appropriate action. DigiCert may generate a new key pair and sign a new certificate. If a disaster physically damages DigiCert's equipment and destroys all copies of DigiCert's signature keys, then DigiCert will provide notice to affected parties at the earliest feasible time.

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 reviews, tests, and updates the BCMP and supporting procedures at least annually.

DigiCert's systems are redundantly configured at its primary facility and are mirrored at a separate, geographically diverse location for failover in the event of a disaster. If a disaster causes DigiCert's primary CA operations to become inoperative, DigiCert will re-initiate its operations at its secondary location giving priority to the provision of certificate status information and time stamping capabilities, if affected.

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 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. 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. Typically, the cryptographic hardware is evaluated to FIPS 140-1 Level 3 and EAL 4+. DigiCert creates auditable evidence during the key generation process to prove that the CPS was followed and role separation was enforced during the key generation process.

6.1.2. Private Key Delivery to Subscriber
No stipulation.

6.1.3. Public Key Delivery to Certificate Issuer
Subscribers generate key pairs and submit the Public Key to DigiCert in a CSR as part of the certificate request process. The Subscriber's signature on the request is authenticated prior to issuing the certificate.

6.1.4. CA Public Key Delivery to Relying Parties
No stipulation.

6.1.5. Key Sizes
No stipulation.

6.1.6. Public Key Parameters Generation and Quality Checking
DigiCert uses a cryptomodule that conforms to FIPS 186-2 and provides random number generation and on-board generation of up to 4096-bit RSA Public Keys and a wide range of ECC curves.

6.1.7. Key Usage Purposes (as per X.509 v3 key usage field)
DigiCert's certificates may include key usage extension fields that specify the intended use of the certificate and technically limit the certificate's functionality in X.509v3 compliant software. The use of a specific key is determined by the key usage extension in the X.509 certificate. Subscriber certificates assert key usages based on the intended application of the key pair. In particular, certificates to be used for digital signatures (including authentication) set the digitalSignature and/or nonRepudiation bits. Certificates to be used for key or data encryption shall set the keyEncipherment and/or dataEncipherment bits. Certificates to be used for key agreement shall set the keyAgreement bit.

Key usage bits and extended key usages are specified in the certificate profile for each type of certificate as set forth in relevant profiled document.

6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1. Cryptographic Module Standards and Controls
No stipulation.

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 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.

6.2.3. Private Key Escrow
No stipulation.

6.2.4. Private Key Backup
No stipulation.

6.2.5. Private Key Archival
No stipulation.

6.2.6. Private Key Transfer into or from a Cryptographic Module
No stipulation.

6.2.7. Private Key Storage on Cryptographic Module
No stipulation.

6.2.8. Method of Activating Private Keys
DigiCert's Private Keys are activated according to the specifications of the cryptographic module manufacturer. Activation data entry is protected from disclosure. Subscribers are solely responsible for protecting their Private Keys. Subscribers should use a strong password or equivalent authentication method to prevent unauthorized access or use of the Subscriber's Private Key. At a minimum, Subscribers are required to authenticate themselves to the cryptographic module before activating their private keys.

6.2.9. Method of Deactivating Private Keys

DigiCert's Private Keys are deactivated via logout procedures on the applicable HSM device when not in use. DigiCert never leaves its HSM devices in an active unlocked or unattended state. Subscribers should deactivate their Private Keys via logout and removal procedures when not in use.

6.2.10. Method of Destroying Private Keys

DigiCert/RA personnel, acting in trusted roles, destroy CA, RA, and status server Private Keys when no longer needed. Subscribers shall destroy their Private Keys when the corresponding certificate is revoked or expired or if the Private Key is no longer needed. DigiCert may destroy a Private Key by deleting it from all known storage partitions. DigiCert also zeroizes the HSM device and associated backup tokens according to the specifications of the hardware manufacturer. This reinitializes the device and overwrites the data with binary zeros.

6.2.11. Cryptographic Module Rating

See Section 6.2.1.

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1. Public Key Archival

DigiCert archives copies of Public Keys in accordance with Section 5.5.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

No stipulation.

6.4. ACTIVATION DATA

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. All DigiCert personnel and Subscribers are instructed to use strong passwords and to protect PINs and passwords. DigiCert employees are required to create non-dictionary, alphanumeric passwords with a minimum length and to change their passwords on a regular basis. If DigiCert uses passwords as activation data for a signing key, DigiCert will change the activation data change upon rekey of the CA certificate.

6.4.2. Activation Data Protection

DigiCert protects data used to unlock private keys from disclosure using a combination of cryptographic and physical access control mechanisms. Protection mechanisms include keeping activation mechanisms secure using role-based physical control. All DigiCert personnel are instructed to memorize and not to write down their password or share it with another individual. DigiCert locks accounts used to access secure CA processes if a certain number of failed password attempts occur.

6.4.3. Other Aspects of Activation Data

No stipulation.

6.5. COMPUTER SECURITY CONTROLS

6.5.1. Specific Computer Security Technical Requirements

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.

6.5.2. Computer Security Rating

No stipulation.

6.6. LIFE CYCLE TECHNICAL CONTROLS

6.6.1. System Development Controls

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.

6.6.2. Security Management Controls

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.

6.6.3. Life Cycle Security Controls

No stipulation.

6.7. NETWORK SECURITY CONTROLS

DigiCert documents and controls the configuration of its systems, including any upgrades or modifications made. DigiCert's CA system is connected to one internal network and is protected by firewalls and Network Address Translation for all internal IP addresses (e.g., 192.168.x.x). DigiCert's customer support and vetting workstations are also protected by firewall(s) and only use internal IP addresses. Root Keys are kept offline and brought online only when necessary to sign certificate-issuing subordinate CAs, OCSP responses, OCSP Responder Certificates, or periodic CRLs. Firewalls and boundary control devices are configured to allow access only by the addresses, ports, protocols and commands required for the trustworthy provision of PKI services by such systems. DigiCert's security policy is to block all ports and protocols and open only ports necessary to enable CA functions. All CA equipment is configured with a minimum number of services and all unused network ports and services are disabled. DigiCert's network configuration is available for review on-site by its auditors and consultants under an appropriate non-disclosure agreement.

6.8. TIME-STAMPING

No stipulation.

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.

7.1. CERTIFICATE PROFILE

7.1.1. Version Number(s)
All certificates are X.509 version 3 certificates.

7.1.2. Certificate Extensions
As agreed to with the customer.

7.1.3. Algorithm Object Identifiers
As agreed to with the customer. DigiCert strongly recommends the following:

sha256WithRSAEncryption	[iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11]
ecdsa-with-sha384	[iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures (4) ecdsa-with-SHA2 (3) 3]

7.1.4. Name Forms
No stipulation.

7.1.5. Name Constraints
No stipulation.

7.1.6. Certificate Policy Object Identifier
No stipulation.

7.1.7. Usage of Policy Constraints Extension
Not applicable.

7.1.8. Policy Qualifiers Syntax and Semantics
DigiCert may include 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.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension
No stipulation.

7.2. CRL PROFILE

7.2.1. Version number(s)
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-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]

7.2.2. CRL and CRL Entry Extensions
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 in UTC format
Reason Code	Optional reason for revocation

7.3. *OCSP PROFILE*

7.3.1. Version Number(s)
DigiCert's OCSP responders conform to version 1 of RFC 2560.

7.3.2. OCSP Extensions
No stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1. *FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT*
Audits referencing this CPS shall cover DigiCert's CA systems, Sub CAs, and OCSP Responders.

8.2. *IDENTITY/QUALIFICATIONS OF ASSESSOR*
No stipulation.

8.3. *ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY*
No stipulation.

8.4. *TOPICS COVERED BY ASSESSMENT*
Any audit covers DigiCert's business practices disclosure, the integrity of DigiCert's PKI operations, and DigiCert's compliance with relevant standards.

8.5. *ACTIONS TAKEN AS A RESULT OF DEFICIENCY*
If an audit reports a material noncompliance with applicable law, this CPS, or any other contractual obligations related to DigiCert's services, then (1) the auditor will document the discrepancy, (2) the auditor will promptly notify DigiCert, and (3) DigiCert will develop a plan to cure the noncompliance. DigiCert will submit the plan to the DCPA for approval and to any third party that DigiCert is legally obligated to satisfy. The DCPA may require additional action if necessary to rectify any significant issues created by the non-compliance, including requiring revocation of affected certificates.

8.6. *COMMUNICATION OF RESULTS*
The results of each audit are reported to the DCPA and to any third party entities which are entitled by law, regulation, or agreement to receive a copy of the audit results.

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 for certificate issuance and renewal. DigiCert may change its fees 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 certificate status information via OCSP.

9.1.4. Fees for Other Services

No stipulation.

9.1.5. Refund Policy

As set forth in the relevant customer agreement.

9.2.   FINANCIAL RESPONSIBILITY

9.2.1. Insurance Coverage

DigiCert maintains Commercial General Liability insurance with a policy limit of at least $2 million in coverage and Professional Liability/Errors & Omissions insurance with a policy limit of at least $5 million in coverage. Insurance is carried through companies rated no less than A- as to Policy Holder's Rating in the current edition of Best's Insurance Guide (or with an association of companies, each of the members of which are so rated).

9.2.2. Other Assets

No stipulation.

9.2.3. Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3.   CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1. Scope of Confidential Information

The following information is considered confidential and protected against disclosure using a reasonable degree of care:

- 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 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 CPS).

9.3.2. Information Not Within the Scope of Confidential Information

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

9.3.3. Responsibility to Protect Confidential Information

DigiCert's employees, agents, and contractors are responsible for protecting confidential information and are contractually obligated to do so. Employees receive training on how to handle confidential information.

9.4. PRIVACY OF PERSONAL INFORMATION

9.4.1. Privacy Plan

DigiCert follows the privacy policy posted on its website when handling personal information. Personal information is only disclosed when the disclosure is required by law or when requested by the subject of the personal information.

9.4.2. Information Treated as Private

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

9.4.3. Information Not Deemed Private

Private information does not include certificates, CRLs, or their contents.

9.4.4. Responsibility to Protect Private Information

DigiCert employees and contractors are expected to handle personal information in strict confidence and meet the requirements of US and European law concerning the protection of personal data. All sensitive information is securely stored and protected against accidental disclosure.

9.4.5. Notice and Consent to Use Private Information

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

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

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

9.4.7. Other Information Disclosure Circumstances

No stipulation.

9.5. INTELLECTUAL PROPERTY RIGHTS

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

Certificate and revocation information are the property of DigiCert. DigiCert grants permission to reproduce and distribute certificates on a non-exclusive and royalty-free basis, provided that they are reproduced and distributed in full. DigiCert does not allow derivative works of its certificates or products without prior written permission. Private and Public Keys remain the property of the Subscribers who rightfully hold them. All secret shares (distributed elements) of the DigiCert Private Keys are the property of DigiCert.

9.6. REPRESENTATIONS AND WARRANTIES

9.6.1. CA Representations and Warranties

Except as expressly stated in this 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 CPS, that:

- DigiCert complies, in all material aspects, with this CPS and all applicable laws and regulations, and

- DigiCert publishes and updates CRLs and OCSP responses on a regular basis,

DigiCert:

- 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 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 CPS because of circumstances outside of DigiCert's control.

9.6.2. RA Representations and Warranties

RAs represent that:

1. The RA's certificate issuance and management services conform to this CPS,

2. Information provided by the RA does not contain any false or misleading information,

3. Translations performed by the RA are an accurate translation of the original information, and

4. All certificates requested by the RA meet the requirements of this CPS.

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

9.6.3. Subscriber Representations and Warranties

Subscribers are solely responsible for any misrepresentations they make to third parties and for all transactions that use the 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. Subscribers represent to DigiCert, Application Software Vendors, and Relying Parties that, for each certificate, the Subscriber will:

1. Securely generate its Private Keys and protect its Private Keys from compromise,

2. Provide accurate and complete information when communicating with DigiCert,

3. Confirm the accuracy of the certificate data prior to using the certificate,

4. Promptly cease using a certificate and notify DigiCert if (i) any information that was submitted to DigiCert or is included in a certificate changes or becomes misleading or (ii) there is any actual or suspected misuse or compromise of the Private Key associated with the certificate,

5. Ensure that individuals using certificates on behalf of an organization have received security training appropriate to the certificate,

6. Use the certificate only for authorized and legal purposes, consistent with the certificate purpose, this CPS, any applicable CP, 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.

9.6.4. Relying Party Representations and Warranties

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

1. Obtained sufficient knowledge on the use of digital certificates and PKI,

2. Studied the applicable limitations on the usage of certificates and agrees to DigiCert's limitations on liability related to the use of certificates,

3. Has read, understands, and agrees to the DigiCert Relying Party Agreement and this CPS,

4. Verified both the DigiCert certificate and the certificates in the certificate chain using the relevant CRL or OCSP,

5. Will not use a DigiCert certificate if the certificate has expired or been revoked, and

6. Will take all reasonable steps to minimize the risk associated with relying on a digital signature, including only relying on a DigiCert certificate after considering:

   a) applicable law and the legal requirements for identification of a party, protection of the confidentiality or privacy of information, and enforceability of the transaction;

   b) the intended use of the certificate as listed in the certificate or this CPS,

   c) the data listed in the certificate,

   d) the economic value of the transaction or communication,

   e) the potential loss or damage that would be caused by an erroneous identification or a loss of confidentiality or privacy of information in the application, transaction, or communication,

   f) the Relying Party's previous course of dealing with the Subscriber,

   g) the Relying Party's understanding of trade, including experience with computer-based methods of trade, and

   h) any other indicia of reliability or unreliability pertaining to the Subscriber and/or the application, communication, or transaction.

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

9.6.5. Representations and Warranties of Other Participants

No stipulation.

9.7. DISCLAIMERS OF WARRANTIES

EXCEPT AS EXPRESSLY STATED IN SECTION 9.6.1, ALL CERTIFICATES AND ANY RELATED SOFTWARE AND SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE". TO THE MAXIMUM EXTENT PERMITTED BY LAW, DIGICERT DISCLAIMS ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING ALL WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. DIGICERT DOES NOT WARRANT THAT ANY SERVICE OR PRODUCT WILL MEET ANY EXPECTATIONS OR THAT ACCESS TO CERTIFICIATES 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.

9.8.   LIMITATIONS OF LIABILITY

NOTHING HEREIN LIMITS LIABILTY 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 CPS IN PROVIDING THE CERTIFICATE OR SERVICE. DIGICERT'S LIABILITY FOR CERTIFICATES AND SERVICES THAT DO NOT MATERIALLY COMPLY WITH THIS CPS IS LIMITED AS FOLLOWS:

1. NO LIABILITY IF THE DAMAGE OR LOSS RELATES TO A CERTIFICATE OTHER THAN A SSL CERTIFICATE OR CODE SIGNING CERTIFICATE,

2. A MAXIMUM LIABILITY OF $1,000 PER TRANSACTION FOR SSL CERTIFICATES,

3. AN AGGREGATE MAXIMUM LIABILITY OF $10,000 FOR ALL CLAIMS RELATED TO A SINGLE CERTIFICATE OR SERVICE,

4. AND AN AGGREGATE MAXIMUM LIABILITY OF $1 MILLION FOR ALL CLAIMS, REGARDLESS OF THE NUMBER OR SOURCE OF THE CLAIMS.

DIGICERT APPORTIONS PAYMENTS RELATED TO AN AGGREGATE MAXIMUM LIMITATION ON LIABILITY UNDER THIS SECTION TO THE FIRST CLAIMS THAT ACHIEVE FINAL RESOLUTION.

All liability is limited to actual and legally provable damages. DigiCert is not liable for:

1. Any indirect, consequential, special, or punitive damages or any loss of profit, revenue, data, or opportunity, even if DigiCert is aware of the possibility of such damages;

2. Liability related to fraud or willful misconduct of the Applicant;

3. Liability related to use of a certificate that exceeds the limitations on use, value, or transactions as stated either in the certificate or this CPS;

4. Liability related to the security, usability, or integrity of products not supplied by DigiCert, including the Subscriber's and Relying Party's hardware; or

5. Liability related to the compromise of a Subscriber's Private Key.

The limitations in this section apply to the maximum extent permitted by law and apply regardless of (i) the reason for or nature of the liability, including tort claims, (ii) the number of claims of liability, (iii) the extent or nature of the damages, (iv) whether DigiCert failed to follow any provision of this CPS, or (v) whether any provision of this CPS was proven ineffective.

The disclaimers and limitations on liabilities in this CPS are fundamental terms to the use of DigiCert's certificates and services.

9.9.   INDEMNITIES
9.9.1. Indemnification by DigiCert
As set forth in the relevant customer agreement.

9.9.2. Indemnification by Subscribers
To the extent permitted by law, each Subscriber shall indemnify DigiCert, its partners, and any cross-signed entities, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to (i) any misrepresentation or omission of material fact by Subscriber, regardless of whether the misrepresentation or omission was intentional or unintentional;

(ii) Subscriber's breach of the Subscriber Agreement, this 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.

9.9.3. Indemnification by Relying Parties

To the extent permitted by law, each Relying Party shall indemnify DigiCert, its partners, and any cross-signed entities, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to the Relying Party's (i) breach of the Relying Party Agreement, an End-User License Agreement, this 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 CPS and any amendments to the CPS are effective when adopted by the DCPA and remain in effect until replaced with a newer version.

9.10.2. Termination

This CPS and any amendments 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'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 CPS terminates.

9.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

DigiCert accepts notices related to this 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.

9.12. AMENDMENTS

9.12.1. Procedure for Amendment

This CPS is periodically reviewed and updated by the DCPA. Controls are in place to reasonably ensure that this CPS is not amended and published without the prior authorization of the DCPA.

9.12.2. Notification Mechanism and Period

DigiCert does not guarantee or set a notice-and-comment period and may make changes to this 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 CPS.

9.12.3. Circumstances under which OID Must Be Changed

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

9.13. DISPUTE RESOLUTION PROVISIONS

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

9.14. GOVERNING LAW

The laws of the state of Utah govern the interpretation, construction, and enforcement of this CPS and all

proceedings related to DigiCert's products and services, including tort claims, without regard to any conflicts of law principles. The state of Utah has non-exclusive venue and jurisdiction over any proceedings related to the CPS or any DigiCert product or service.

9.15. COMPLIANCE WITH APPLICABLE LAW

This CPS is subject to all applicable laws and regulations, including United States restrictions on the export of software and cryptography products.

9.16. MISCELLANEOUS PROVISIONS

9.16.1. Entire Agreement

DigiCert contractually obligates any entity operating under this CPS to comply with this 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 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 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 CPS is held invalid or unenforceable by a competent court or tribunal, the remainder of the CPS will remain valid and enforceable. Each provision of this 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 CPS does not waive DigiCert's right to enforce the same provision later or right to enforce any other provision of this 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 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.

9.17. OTHER PROVISIONS

No stipulation.