DigiCert

Certification Practices Statement

DigiCert, Inc.
Version 4.01
August 26, 2010

Suite 200
Canopy Building II
355 South 520 West
Lindon, UT 84042
USA
Tel: 1-801-877-2100
Fax: 1-801-705-0481
www.digicert.com

TABLE OF CONTENTS

1. INTRODUCTION

1.1. OVERVIEW

This document is the DigiCert, Inc. ("DigiCert") Certification Practices Statement (CPS) that outlines the legal, commercial, and technical principles and practices related to DigiCert's certification and time-stamping services. This CPS applies to all entities participating in or using DigiCert's certificate and time-stamping services, including subsidiary Certificate Authorities (CAs), Registration Authorities (RAs), Subscribers, and Relying Parties.

This CPS describes the practices that DigiCert follows in issuing digital certificates and time-stamp tokens in accordance with the DigiCert Certificate Policy (the "CP") as well as requirements found in other applicable policies, including the CDS Certificate Policy of Adobe Systems Incorporated ("Adobe"), the X.509 Certificate Policy for the Federal Bridge Certification Authority ("FBCA"), and the current version of "Guidelines for the Issuance and Management of Extended Validation Certificates," as published by the Certification Authority / Browser Forum ("CAB Forum"). DigiCert always conforms to the current version of the CAB Forum Guidelines published at http://www.cabforum.org (the "EV Guidelines"). If any inconsistency exists between this CPS and the EV Guidelines, the EV Guidelines take precedence. Time-stamping services are provided according to the IETF RFC 3161, ETSI 102 023, and ETSI 101 861 technical standards.

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 the CP, DigiCert's agreements with its customers, Relying Party agreements, its privacy policy, and its Certificate Profiles document. DigiCert may publish additional certificate policies or certification practice statements as necessary to describe other product or service offerings. These supplemental policies and statements are available to applicable users or relying parties.

Pursuant to the IETF PKIX RFC 3647 CP/CPS framework, this CPS is divided into nine (9) parts that cover the security controls and practices and procedures for certificate or time-stamping services within the DigiCert PKI. To preserve the outline specified by RFC 3647, section headings that do not apply have the statement "Not applicable" or "No stipulation."

1.2. DOCUMENT NAME AND IDENTIFICATION

This document is the DigiCert Certification Practices Statement and was approved for publication on 9 August 2010 by the DigiCert Policy Authority (DCPA). Revisions of this document have been made as follows:

Date	Changes	Version
26-August-2010	Updated the process used to authenticate the certificate requester's authority under section 3.2.5 for code signing certificates issued to organizations	4.01
9-August-2010	This version 4.0 replaces the DigiCert Certificate Policy and Certification Practices Statement, Version 3.08, dated May 29, 2009, and the DigiCert Certification Practice Statement for Extended Validation Certificates, Version 1.0.4, May 29, 2009.	4.0

The OID for DigiCert is joint-iso-ccitt (2) country (16) USA (840) US-company (1) DigiCert (114412). The OID for this version of the CPS is 2.16.840.1.114412.0.2.4. Subsequent revisions to this CPS might have new OID assignments. DigiCert issues certificates and time-stamp tokens containing the following OIDs / OID arcs:

Digitally Signed Object	Object Identifier (OID)
Organization-Vetted SSL Certificates	2.16.840.1.114412.1
Extended Validation SSL Certificates	2.16.840.1.114412.2
Code Signing Certificates	2.16.840.1.114412.3
Level 1 Certificates - Personal	2.16.840.1.114412.4.1.1
Level 1 Certificates - Enterprise	2.16.840.1.114412.4.1.2
Level 2 Certificates	2.16.840.1.114412.4.2
Level 3 Certificates	2.16.840.1.114412.4.3
Level 4 Certificates	2.16.840.1.114412.4.4
PIV-I Hardware - keys require activation by the PIV-I Cardholder (PIV Auth, Dig Sig and Key Management)	2.16.840.1.114412.5.1
PIV-I Card Authentication - keys do not require PIV-I Cardholder activation	2.16.840.1.114412.5.2
PIV-I Content Signing – use by PIV-I-compliant CMS	2.16.840.1.114412.5.3
EU Qualified Certificates ETSI TS 101 456	2.16.840.1.114412.6.1 0.4.0.1456.1.2
EU QC on Secure Signature Creation Device ETSI TS 101 456	2.16.840.1.114412.6.2 0.4.0.1456.1.1
ETSI TS 101 862 - Qualified Certificate Statements	0.4.0.1862.1.x
Adobe CDS Certificates and Timestamping	1.2.840.113583.1.x
Trusted Timestamping	2.16.840.1.114412.7.1
EU Qualified Timestamping ETSI TS 102 023	2.16.840.1.114412.7.2 0.4.0.2023.1.x

Specific OIDs used when objects are signed pursuant to this CPS are indicated in the accompanying Certificate Profiles document.

1.3. PKI PARTICIPANTS

1.3.1. Certification Authorities

DigiCert is a certification authority (CA) that issues high quality and highly trusted digital certificates in accordance with this CPS. As a CA, DigiCert performs functions associated with Public Key operations, including receiving certificate requests, issuing, revoking and renewing a digital certificate, and maintaining, issuing, and publishing CRLs and OCSP responses.

DigiCert's self-signed, offline Root CAs create online subordinate CAs in accordance with this CPS and applicable cross-certification / federation policies and memoranda of agreement with other CAs. For ease of reference herein, all DigiCert Root CAs and cross-signed or subordinate CAs that issue certificates are referred to as "Issuer CAs." In accordance with EU Directive 99/93, EU Qualified Certificates will only be issued by Issuer CAs operated under the control of DigiCert. In accordance with requirements of the U.S. Federal PKI Policy Authority (FPKIPA), DigiCert shall notify the FPKIPA prior to issuing a CA certificate to an external Issuer CA that DigiCert desires to chain to the Federal Bridge CA. In all cases, an external Issuer CA is contractually required to adopt and implement procedures that are at least as restrictive as those found herein.

DigiCert is also a time stamping authority (TSA) and provides proof-of-existence for data at an instant in time as described herein.

DigiCert CA and TSA operations are managed by the DigiCert Policy Authority (DCPA) which is composed of members of DigiCert management appointed by DigiCert's Board of Directors. The DCPA is responsible for the approval of this CPS and overseeing the conformance of CA and TSA practices with applicable requirements.

DigiCert's CAs include three 2048-bit RSA Root CAs (DigiCert Global Root CA, DigiCert High Assurance EV Root CA, and DigiCert Assured ID Root CA); a 384-bit Elliptical Curve Root CA (DigiCert High Assurance Root CA (ECC)); and the 2048-bit DigiCert CA for Adobe Certified Document Services.

1.3.2. Registration Authorities

Registration Authorities (RA) request certificates and/or perform identification and authentication for end-user certificates. The specific role of an RA varies greatly between entities, ranging from simple translation services to actual assistance in gathering and verifying Applicant information. Some RAs may manage the lifecycle of certificates for end-users.

At a minimum, DigiCert contractually obligates all RAs to abide by the CP, CPS, and any industry standards that are applicable to the RA's role in certificate issuance, management, and revocation.

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. Prior to verification of identity and issuance of a certificate, a Subscriber is an *Applicant*.

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 must check the appropriate CRL or OCSP response prior to relying on information featured in a certificate. The location of the CRL distribution point is detailed within the certificate.

Adobe makes the Certified Document Services (CDS) platform available in Acrobat® 6.0 and above in order to provide document recipients with improved assurances that certified PDF documents are authentic. Document recipients are Relying Parties who use the free Adobe Reader on supported platforms to verify the Subscriber's signature on a certified document.

1.3.5. Other Participants

Other participants include: Bridge CAs and CAs that cross-certify DigiCert CAs as trust anchors in other PKI communities; Card Management Systems and integrators (CMSs) that ensure proper operation and provisioning of PIV-I cards; and Time Source Entities, Time Stamp Token Requesters, and Time Stamp Verifiers involved in trusted timestamping. When issuing PIV-I cards, DigiCert makes a Card Management Systems (CMS) that meets the requirements herein responsible for managing smart card token content. DigiCert does not issue certificates to a CMS that include a PIV-I Hardware or PIV-I Card Authentication policy OID.

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. Digital certificates are used in commercial environments as a digital equivalent of an identification card.
A *time-stamp token* (*TST*) cryptographically binds a representation of data to a particular time stamp, thus establishing evidence that the data existed at a certain point in time.

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.

This CPS covers several different types of end entity certificates/tokens with varying levels of assurance. The following table provides a brief description of the appropriate uses of each. The descriptions are for guidance only and are not binding.

Certificate	Appropriate Use
OV SSL Certificates	Used to secure online communication where the risks and consequences of data compromise are moderate, including transactions having substantial monetary value or risk of fraud or involving access to private information where the likelihood of malicious access is substantial.
EV SSL Certificates	Used to secure online communication where risks and consequences of data compromise are high, including transactions having high monetary value, risk of fraud, or where involving access to private information where the likelihood of malicious access is high.
Code Signing Certificates	Establishes the identity of the Subscriber named in the certificate and that the signed code has not been modified since signing.
Level 1 Client Certificates - Personal (email certificates)	Provides the lowest degree of assurance concerning identity of the individual and is generally used only to provide data integrity to the information being signed. These certificates should only be used where the risk of malicious activity is low and if an authenticated transaction is not required.
Level 1 Client Certificates - Enterprise (C4 certificates)	Used in environments where there are risks and consequences of data compromise, but such risks are not of major significance. Users are assumed not likely to be malicious.
Level 2 Client Certificates (Corporate certificates)	Used in environments where there are risks and consequences of data compromise, but such risks are not of major significance. Users are assumed not likely to be malicious.
Level 3 Client Certificates (High assurance and FBCA Medium)	Used in environments where risks and consequences of data compromise are moderate, including transactions having substantial monetary value or risk of fraud or involving access to private information where the likelihood of malicious access is substantial.
Level 4 Client Certificates (Highest assurance and FBCA Medium Hardware)	Used in environments where risks and consequences of data compromise are high, including transactions having high monetary value or risk of fraud or involving access to private information where the likelihood of malicious access is high.
PIV-I Hardware PIV-I Card Authentication PIV-I Content Signing PIV-I Digital Signature PIV-I Key Management	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include contactless smart card readers where use of an activation PIN is not practical. Personal Identity Verification – Interoperable (PIV-I) cards are intended to technically interoperate with Federal PIV Card readers and applications. The requirements associated with PIV-I Hardware and PIV-I Content Signing are identical to Level 4 Certificates except where specifically noted herein. PIV-I Content Signing policy is reserved for certificates used by the Card Management System (CMS) to sign the PIV-I card security objects
EU Qualified Certificate and EU QC on Secure Signature Creation Device	EU Qualified Certificates may only be used for signing (ETSI TS 101 456)
CDS Certificates	Used to show that the signed document originated from the stated author and that the portion of the document signed by the author has

	not been modified since signing. Subscribers may only use CDS signing certificates to digitally sign and verify Adobe Acrobat documents.
Time Stamp Token	Used to identify the existence of data at a set period of time.

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. Code signing certificates do not indicate that the signed code is safe to install or free from malware, bugs, or vulnerabilities.

Certificates issued under this CPS may not be used (i) for any application requiring fail-safe performance such as (a) the operation of nuclear power facilities, (b) air traffic control systems, (c) aircraft navigation systems, (d) weapons control systems, or (e) any other system whose failure could lead to injury, death or environmental damage; or (ii) where prohibited by law.

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 200 - Canopy Building II
355 South 520 West
Lindon, UT 84042 USA
Tel: 1-801-877-2100
Fax: 1-801-705-0481

1.5.2. Contact Person

Attn: Legal Counsel
DigiCert Policy Authority
Suite 200 - Canopy Building II
355 South 520 West
Lindon, UT 84042 USA

1.5.3. Person Determining CPS Suitability for the Policy

The DCPA determines the suitability and applicability of this CPS based on the results and recommendations received from an independent auditor (see Section 8). The DCPA is also responsible for evaluating and acting upon the results of compliance audits.

1.5.4. CPS Approval Procedures

The DCPA approves the CPS and any amendments. Amendments are made by either updating the entire CPS or by publishing an addendum. The DCPA determines whether an amendment to this CPS requires notice or an OID change. *See also* Section 9.10 and Section 9.12 below.

1.6. DEFINITIONS AND ACRONYMS

"Affiliated Organization" means an organization that has an organizational affiliation with a Subscriber and that approves or otherwise allows such affiliation to be represented in a certificate.

"Applicant" means an entity applying for a certificate.

"Application Software Vendor" means a software developer whose software displays or uses certificates and distributes root certificates.

"CAB Forum" is defined in section 1.1.

"Certificate Approver" is defined in the EV Guidelines.

"Certificate Requester" is defined in the EV Guidelines.

"Contract Signer" is defined in the EV Guidelines.

"EU Directive 99/93" means the EU Council Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for Electronic Signatures, OJ L 13, 19.01.2000, pp. 12-20.

"EV Guidelines" is defined in section 1.1.

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

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

"**PIV-I Profile**" means the X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards, Ver. 1.0, Date: April 23 2010.

"**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.

"Qualified Certificate" means a certificate that meets the requirements in Annex I of EU Directive 99/93 and is provided by an Issuer CA meeting the requirements of Annex II of the Directive.

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

"Relying Party Agreement" means an agreement which must be read and accepted by the Relying Party of an SSL Certificate prior to validating, relying on or using a Certificate or accessing or using DigiCert's Repository. The Relying Party Agreement is available for reference through a DigiCert online repository.

"Secure Signature Creation Device" means a signature-creation device that meets the requirements laid down in Annex III of EU Directive 99/93.

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

"Subscriber Agreement" means an agreement, specific to a certificate type, that the Applicant must read and accept before receiving a certificate.

"WebTrust EV Program" means the additional audit procedures specified for CAs that issue EV Certificates by the AICPA/CICA to be used in conjunction with its WebTrust Program for Certification Authorities.

"WebTrust" means the current version of the AICPA/CICA WebTrust Program for Certification Authorities.

Acronyms:

CA	Certificate Authority or Certification Authority
CDS	Certified Document Services
CMS	Card Management System
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DBA	Doing Business As (also known as "Trading As")
DCPA	DigiCert Policy Authority
ETSI	European Telecommunications Standards Institute
EU	European Union
EV	Extended Validation
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number (e.g. a secret access code)
PIV-I	Personal Identity Verification-Interoperable
PKI	Public Key Infrastructure
PKIX	IETF Working Group on Public Key Infrastructure
PKCS	Public Key Cryptography Standard
QGIS	Qualified Government Information Source
QTIS	Qualified Government Tax Information Source
QIIS	Qualified Independent Information Source
RA	Registration Authority
SHA	Secure Hashing Algorithm
SSCD	Secure Signature Creation Device
SSL	Secure Sockets Layer
TLD	Top-Level Domain
TLS	Transport Layer Security
TSA	Time Stamping Authority
TST	Time-Stamp Token
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
X.509	The ITU-T standard for Certificates and their corresponding authentication framework

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. REPOSITORIES

DigiCert publishes its root certificates, revocation data for issued digital certificates, CPs, CPSs, Relying Party Agreements, and Subscriber Agreements in DigiCert's publicly-available online repositories.

DigiCert operates its PKI infrastructure to ensure that its root certificates and CRLs are available through an online repository 24 hours a day, 7 days a week, with a minimum of 99% availability overall per year with a scheduled down-time that does not exceed 0.5% annually.

2.2. PUBLICATION OF CERTIFICATION INFORMATION

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

1. On the web: www.digicert.com
2. By email to admin@digicert.com
3. By mail addressed to: DigiCert, Inc., 355 South 520 West, Lindon, Utah 84042
4. By telephone Tel: 1-801-877-2100
5. By fax: 1-801-705-0481

DigiCert publishes its CP, CPS, CA certificates, cross-certificates, Subscriber Agreements, Relying Party Agreements, and CRLs in online repositories. The CRLs contain entries for all revoked un-expired certificates and are valid, depending on certificate type, from 18 hours up to 31 days.

2.3. TIME OR FREQUENCY OF PUBLICATION

CA certificates are published in a repository as soon as possible after issuance. CRLs for end-user certificates are issued at least once per day. CRLs for CA certificates are issued at least every 6 months (every 31 days for offline CAs chaining to the Federal Bridge CA), and also within 18 hours if a CA certificate is revoked. Each CRL includes a monotonically increasing sequence number for each CRL issued. Under special circumstances, DigiCert may publish new CRLs prior to the expiration of the current CRL.

New or modified versions of the CP, this CPS, Subscriber Agreements, or Relying Party Warranties are published within seven days after their approval.

2.4. ACCESS CONTROLS ON REPOSITORIES

Information published on repositories is public information. Read only access is unrestricted. DigiCert has implemented logical and physical controls to prevent unauthorized write access to its repositories.

3. IDENTIFICATION AND AUTHENTICATION

3.1. NAMING

3.1.1. Types of Names

Certificates are issued with a non-null subject Distinguished Name (DN) that complies with ITU X.500 standards. Some certificates, including certificates for intranet use and Unified Communications Certificates, may contain entries in the subject alternative name extension that are not intended to be relied upon by the general public (e.g., they contain non-standard top level domains like .local or they are addressed to an IP number space that has been allocated as private by RFC1918).

Non-wildcard SSL Certificates and Unified Communications Certificates are issued using the Fully Qualified Domain Name (FQDN) name or IP address of the servers, services, or applications. Wildcard SSL Certificates have a wildcard asterisk character for the server name in the subject field.

The FQDN or authenticated domain name is placed in the Common Name (CN) attribute of the Subject field and, when applicable, the Subject Alternative Name extension contains the FQDNs or authenticated domain names of the servers that are owned or under the control of the Subscriber. Subject Alternative Names are marked non-critical. When DNs are used, common names must respect name space uniqueness and must not be misleading.

Certificates for PIV-I cards include both a non-null subject name and subject alternative name.

Each PIV-I Hardware certificate indicates whether or not the Subscriber is associated with an Affiliated Organization by taking one of the following forms:

For certificates with an Affiliated Organization:

cn=*Subscriber's full name*, ou=*Affiliated Organization Name*,{*Base DN*}

For certificates with no Affiliated Organization:

cn=*Subscriber's full name*, ou=Unaffiliated, ou=*Entity CA's Name*,{*Base DN*}

Each PIV-I Content Signing certificate also clearly indicates the organization administering the CMS. PIV-I Card Authentication subscriber certificate do not include a Subscriber common name.

Each PIV-I Card Authentication certificate indicates whether or not the Subscriber is associated with an Affiliated Organization by taking one of the following forms:

For certificates with an Affiliated Organization:

serialNumber=*UUID*, ou=*Affiliated Organization Name*,{*Base DN*}

For certificates with no Affiliated Organization:

serialNumber=*UUID*, ou=Unaffiliated, ou=*Entity CA's Name*,{*Base DN*}

The UUID is encoded within the serialNumber attribute using the UUID string representation defined in Section 3 of RFC 4122 (e.g., "f81d4fae-7dec-11d0-a765-00a0c91e6bf6").

The subject name in each EU Qualified Certificates complies with section 3.1.2 of RFC 3739

3.1.2. Need for Names to be Meaningful

DigiCert uses distinguished names that identify both the subject and issuer of the certificate. DigiCert only allows directory information trees that accurately reflect organization structures.

3.1.3. Anonymity or Pseudonymity of Subscribers

Generally, DigiCert does not issue anonymous or pseudonymous certificates; however, for IDNs, DigiCert may include the Punycode version of the IDN as the subject name. DigiCert may issue other pseudonymous end-entity certificates provided that they are approved for the same assurance level within cross-certified PKI domains and in conjunction with privacy enhancing technologies that allow identity and attributes to be communicated to authorized relying parties who have a legitimate need for identity or other attribute information.

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 is enforced as follows:

SSL Server Certificates	Entering the domain name in the Common Name attribute of the subject field. Domain name uniqueness is controlled by the Internet Corporation for Assigned Names and Numbers (ICANN).
Client Certificates	Requiring a unique email address or using a unique serial integer assigned to the certificate.

Code Signing Certificates	Requiring a unique organization name and address or using a unique serial integer assigned to the certificate.
Time Stamping	Requiring a unique hash and time or unique serial integer assigned to the time stamp

3.1.6. Recognition, Authentication, and Role of Trademarks

Subscribers may not request certificates with any content that infringes on the intellectual property rights of another entity. Unless otherwise specifically stated in this CPS, 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

The Applicant must submit a CSR, generally in a PKCS#10 format, to establish that it holds the Private Key corresponding to the Public Key in the certificate request.

3.2.2. Authentication of Organization Identity

DigiCert requires organizational applicants to include the organization name and address in the certificate application. DigiCert verifies the organizational existence and identity of Applicants using reliable third party and government databases or through other direct means of communication with the entity or jurisdiction governing the organization's legal creation, existence, or recognition. If such efforts are insufficient to confirm the legal existence and identity of the subject, DigiCert requires the Applicant to submit official company documentation, such as a business license, filed or certified articles of incorporation/organization, tax certificate, corporate charter, official letter, sales license, or other relevant documents. DigiCert verifies the authority of the person requesting the certificate on behalf of an organization in accordance with Section 3.2.5.

DigiCert also requires the following additional verification depending on the certificate type:

SSL Server Certificates (other than EV)	DigiCert also validates the Applicant's right to use the domain name that will be listed in the certificate. Domain name ownership is validated by: 1. Relying on publicly available records from the Domain Name Registrar; 2. Communicating with one of the following email addresses: webmaster@domain.com, administrator@domain.com, admin@domain.com, hostmaster@domain, postmaster@domain, and any address listed in the technical, registrant, or administrative contact field of the domain's Domain Name Registrar record; and/or 3. Requiring a practical demonstration of domain control (e.g., requiring the Applicant to make a specified change to a live page on the given domain). If a third-party makes the certificate application on behalf of the company listed in the Domain Name Registrar record, the third party must submit a document that shows the Applicant's right to use the domain name (such as the Domain Authorization Letter in Appendix A) that is signed by the Registrant (e.g. a domain owner's authorized representative) or the Administrative Contact on the Domain Name Registrar record.
EV Certificates	EV Certificates are validated in accordance with the EV guidelines.

PIV-I	For certificates that assert an organizational affiliation between a human subscriber and an organization, the organization is required to enter into an agreement authorizing that affiliation and is required to request revocation of the certificate when that affiliation ends.

3.2.3. Authentication of Individual Identity

For the following certificate types, DigiCert shall verify an individual's entity using at least the following:

Certificate	Validation
SSL Server Certificates, CDS Certificates, and Code Signing Certificates (issued to an individual)	1. A legible copy of at least one currently valid government-issued photo ID (passport, drivers license, military ID, national ID, or equivalent document type). 2. Applicant's name and address are cross-checked for consistency with reliable data sources. 3. If further assurance is required, then DigiCert requires an additional form of identification, such as recent utility bills, financial account statements, credit card, college/university ID, or equivalent document type. 4. Confirming that the Applicant is able to receive communication by telephone, postal mail/courier, or fax. If DigiCert cannot verify the Applicant's identity using the procedures described above, then the Applicant must submit a Declaration of Identity that is witnessed and signed by a Registration Authority, Trusted Agent, notary, lawyer, accountant, postal carrier, or any entity certified by a State or National Government as authorized to confirm identities.
Code Signing Certificates (issued to organization)	See section 3.2.5
EV Certificates (issued to a sole proprietor)	As specified in the EV Guidelines
Level 1 Client Certificates - Personal (email certificates) (Equivalent to NIST 800-63/Kantara Level 1 and FBCA CP Rudimentary)	Applicant's control of the email address or website listed in the certificate. For corporate email certificates, DigiCert verifies the organization and domain name listed in the certificate similar to an SSL Server Certificate.
Level 1 Client Certificates - Enterprise (email certificates) (Equivalent to NIST 800-63/Kantara Level 1 and FBCA CP Rudimentary)	Any one of the following: 1. In-person appearance before a Registration Authority or Trusted Agent with presentment of an original or certified government-issued credential (e.g., driver's license or birth certificate). 2. Using procedures similar to those used when applying for consumer credit and authenticated through information in consumer credit databases or government records, such as: a. the ability to place or receive calls from a given number; or b. the ability to obtain mail sent to a known physical address. 3. Through information derived from an ongoing business relationship with the credential provider or a partner company (e.g., a financial institution, airline, employer, or

	retail company). Acceptable information includes: a. the ability to obtain mail at the billing address used in the business relationship; b. verification of information established in previous transactions (e.g., previous order number); or c. the ability to place calls from or receive phone calls at a phone number used in previous business transactions. 4. Any method used to validate a Level 2, 3, or 4 Client Certificate.
Level 2 Client Certificates (Corporate certificates) (Equivalent to NIST 800-63/Kantara Levels 2 and 3 and FBCA CP Basic)	1. In-person proofing before a Registration Authority or Trusted Agent with presentment of a government-issued photo ID, examined for authenticity and validity. An entity certified by a State or Federal Entity as authorized to confirm identities may also perform in-person authentication on behalf of the RA, provided that the certified entity forwards the information collected from the applicant directly to the RA in a secure manner. Packages secured in a tamper-evident manner by the certified entity satisfy this requirement; other secure methods are also acceptable. Such authentication does not relieve the RA of its responsibility to verify the presented data. 2. Remotely verifying information provided by applicant (including name, date of birth, and current address or telephone number) through confirming his/her attestation to current possession of a government-issued photo ID and one additional form of ID such as another government-issued ID, an employee or student ID card number, a financial account number (e.g., checking account, savings account, loan or credit card), or a utility service account number (e.g., electricity, gas, or water) for an address matching the applicant's residence. The CA or RA shall verify that the asserted name matches: (a) the referenced photo-ID; (b) date of birth; and (c) current address or personal telephone number; and are consistent with the application and sufficient to identify a unique individual. Confirmation of (c) may be obtained by issuing credentials in a manner that confirms: the address of record supplied by the applicant, or the ability of the applicant to receive telephone communications at a number associated with the applicant in records, while recording the applicant's voice. Additional information may be requested so as to ensure a unique identity, and alternative information may be sought if it leads to at least the same degree of certitude when verified. 3. Where the CA or RA has a current, ongoing relationship with the Applicant, identity may be verified through the exchange of a previously exchanged shared secret (e.g., a PIN or password)

	that meets or exceeds NIST SP 800-63 Level 2 entropy requirements, provided that: (a) identity was originally established with the degree of rigor equivalent to that required in 1 or 2 above, and (b) an ongoing relationship exists sufficient to ensure the Applicant's continued personal possession of the shared secret. 4. Any of the methods used to validate a Level 3 or 4 Client Certificate.
Level 3 Client Certificates (including ClickID certificates) (Equivalent to NIST 800-63/Kantara Level 3 and FBCA CP Medium and Medium Hardware)	In-person proofing before an RA, Trusted Agent, or an entity certified by a State or Federal Entity that is authorized to confirm identities (provided that the certified entity forwards the information collected from the applicant directly to the RA in a secure manner and that the RA is not relieved of its responsibility to verify the presented data). Credentials required are either one Federal Government-issued Picture I.D., or two Non-Federal Government I.D.s, one of which shall be a photo I.D. (e.g., driver's license). The entity performing the validation must examine the credentials for authenticity and validity. For each Level 3 Client Certificate issued, DigiCert or the RA shall review and record a Declaration of Identity that is signed by both the Applicant and the person performing the in-person identification. The information provided (name, date of birth, and current address) is verified to ensure legitimacy. DigiCert or an RA may verify this information electronically by a record check with the specified issuing authority or through similar databases to establish the existence of such records with matching name and reference numbers and to corroborate date of birth, current address of record, and other personal information sufficient to ensure a unique identity. A trust relationship between an RA or Trusted Agent and the applicant that is based on an in-person antecedent (as defined in FBCA Supplementary Antecedent, In-Person Definition) may suffice as meeting the in-person identity proofing requirement provided that (1) it meets the thoroughness and rigor of in-person proofing described above, (2) supporting ID proofing artifacts exist to substantiate the antecedent relationship, and (3) mechanisms are in place that bind the individual to the asserted identity. If the photo ID is valid and confirms the address of record for the Applicant, then the certificate may be approved for issuance with notice of issuance sent to the address of record. If the photo ID does not confirm the Applicant's address of record, then the certificate shall be issued in a manner that confirms the address of record. For Level 3 Client Certificates, the identity of the Applicant must be established no earlier than 30 days prior to initial certificate issuance.
Level 4 Client Certificates (Biometric ID certificates)	In-person proofing before an RA, Trusted Agent, or an entity certified by a State or Federal Entity that is authorized to confirm

(Equivalent to NIST 800-63/Kantara Level 4 and FBCA CP Medium Hardware)	identities (provided that the certified entity forwards the information collected from the applicant directly to the RA in a secure manner and that the RA is not relieved of its responsibility to verify the presented data). Credentials required are either one Federal Government-issued Picture I.D., or two Non-Federal Government I.D.s, one of which shall be a photo I.D. (e.g., driver's license) and the contemporaneous collection of at least one biometric (e.g. photograph or fingerprints) to ensure that the Applicant cannot repudiate application. DigiCert examines the credentials for authenticity and validity. For each Level 4 Client Certificate issued, DigiCert or the RA reviews and records a Declaration of Identity which shall be signed by the applicant and the person performing the in-person identification. For Level 4 Client Certificates, the use of an in-person antecedent is not applicable, and DigiCert establishes the identity no more than 30 days prior to initial certificate issuance. Level 4 Client Certificates are issued in a manner that confirms the Applicant's address of record.
PIV-I Certificates	PIV-I Hardware certificates are only be issued to human subscribers. The following biometric data is collected by DigiCert, an RA, or a Trusted Agent during the identity proofing and registration process: 1. An electronic facial image used for printing facial image on the card, as well as for performing visual authentication during card usage. A new facial image is collected each time a card is issued; and 2. Two electronic fingerprints are stored on the card for automated authentication during card usage. The Subscriber must also present two identity source documents in original form that come from the list of acceptable documents included in Form I-9, OMB No. 1115-0136, Employment Eligibility Verification. At least one document must be a valid State or Federal Government-issued picture identification (ID). For PIV-I, the use of an in-person antecedent is not applicable. Identity is established no more than 30 days prior to initial certificate issuance.
EU Qualified Certificates	Verify (in person) at time of registration by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to whom the qualified certificate will be issued. Evidence of identity is checked against a physical person either directly or is checked indirectly using means which provides equivalent assurance to physical presence. Acceptable evidence consists of a government-issued ID. Collected information includes the Subscriber's full name; date and place of birth; and a nationally recognized identity number (or another attribute that distinguishes the person from others with the same name).

Acceptable forms of government ID include a:

1. driver's license,
2. passport, or
3. military ID.

Acceptable forms of non-government ID include a:

1. voided check from a current checking account,
2. recent utility bill showing Applicant's name, address, and utility account number, or
3. social security card.

DigiCert may allow other forms of comparable identification.

A Declaration of Identity consists of the following:

1. the identity of the person performing the verification,
2. a signed declaration by the verifying person stating that they verified the identity of the Subscriber as required using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law,
3. a unique identifying number from the verifier's identification,
4. a unique identifying number from the Applicant's identification,
5. the date and time of the verification, and
6. a declaration of identity by the Applicant that is signed in handwriting in the presence of the person performing the verification using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law.

If an Applicant cannot participate in face-to-face registration, a trusted person who already has a certificate of the same type applied for by the Applicant may represent the Applicant during the validation process. The trusted person must present their certificate and the Applicant's information to the person performing the face-to-face registration.

3.2.3.1. Authentication for Role-based Client Certificates

DigiCert may issue certificates that identify a specific role that the Subscriber holds, provided that the role identifies a specific individual within an organization (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. DigiCert only issues role-based certificates to Subscribers who first obtain an individual Subscriber certificate that is at the same or higher assurance level as the requested role-based certificate. DigiCert may issue certificates with the same role to multiple Subscribers. However, DigiCert requires that each certificate have a unique key pair. Individuals may not share their issued role-based certificates and are required to protect the role-based certificate in the same manner as individual certificates.

DigiCert verifies the identity of the individual requesting a role-based certificate (i.e. the sponsor) in accordance with Section 3.2.3 and records the information identified in Section 3.2.3 for a sponsor associated with the role before issuing a role-based certificate. The sponsor must hold an individual certificate in his/her own name issued by the same CA at the same or higher assurance level as the role-based certificate.. If the certificate is a pseudonymous certificate that identifies subjects by their organizational roles, then DigiCert validates that the individual either holds that role or has the authority to sign on behalf of the role.

3.2.3.2. Authentication for Group Client Certificates

For cases where there are several entities acting in one capacity, and where non-repudiation for transactions is not desired, DigiCert may issue a certificate that corresponds to a Private Key that is shared by multiple Subscribers. DigiCert or the RA records the information identified in Section 3.2.3 for a sponsor from the Information Systems Security Office or equivalent before issuing a group certificate.

In addition, DigiCert:

1. Requires that the Information Systems Security Office, or equivalent, be responsible for ensuring control of the private key, including maintaining a list of Subscribers who have

access to the private key, and account for the time period during which each Subscriber had control of the key,
2. Does not include a subjectName DN in the certificate that could imply that the subject is a single individual,
3. Requires that the sponsor provide and continuously update a list of individuals who hold the shared private key, and
4. Ensures that the procedures for issuing group certificates comply with all other stipulations of this CP (e.g., key generation, private key protection, and Subscriber obligations).

3.2.3.3. Authentication of Devices for Client Certificates

DigiCert issues client certificates for use on computing or network devices, provided that the entity owning the device is listed as the subject. In all cases, the device has a human sponsor who provides:

1. Equipment identification (e.g., serial number) or service name (e.g., DNS name),
2. Equipment public keys,
3. Equipment authorizations and attributes (if any are to be included in the certificate), and
4. Contact information.

If the client certificate's sponsor is changed, the new sponsor is required to review the status of each device to ensure it is still authorized to receive certificates. Each sponsor is contacted annually using previously verified information to ensure that the device is still under the sponsor's control or responsibility. All sponsors are contractually obligated to notify DigiCert if the equipment is no longer in use or no longer requires a certificate. All registration is verified in accordance with the requested client certificate type.

3.2.4. Non-verified Subscriber Information

For Level 1 - Personal client certificates verified only by email address, DigiCert is not required to confirm that the common name requested by the Applicant is the legal name of the Subscriber, and such certificates shall contain a notice advising potential relying parties that the person's identity has not been verified. OV SSL Certificates may contain a pseudo-domain for use within the Subscriber's internal, non-public-DNS networks. Provided that the right to use a domain name is verified in accordance with Section 3.2.2, DigiCert may rely on the Subscriber's indication of the host or server name that forms the fully qualified domain name to be included in the SSL Certificate. Any other non-verified information included in a certificate is designated as such in the certificate. Unverified information is never included in a Level 2, Level, 3, Level 4, PIV-I, or EU Qualified Certificate.

3.2.5. Validation of Authority

The authority of the individual requesting a certificate on behalf of an organization verified under section 3.2.2 is validated as follows:

Certificate	Verification
SSL Server Certificates (other than EV)	Verifying the authority of the requester with an authorized contact listed with the Domain Name Registrar, through a person with control over the domain, or though an out-of-band confirmation with the organization. Communication to persons with control over the domain consists of emailing one or more of the following email addresses: webmaster@domain.com, administrator@domain.com, admin@domain.com, hostmaster@domain, postmaster@domain, or any address listed as a contact field of the domain's Domain Name Registrar record.
EV Certificates	Verifying authority of the Contract Signer and Certificate Approver
Code Signing Certificates and CDS Certificates	Confirming the contact information and authority of the certificate requester with an authoritative source within the organization (e.g. corporate, legal, IT, HR, or other appropriate organizational sources)

	using a reliable means of communication; and Obtaining approval of the certificate request using a means of communication confirmed by the organization.
Level 1 Client Certificates - Personal (email certificates)	Verifying that the individual has control over the email address listed in the certificate.
Level 1 Client Certificates - Enterprise (email certificates)	Having an individual with control over the domain visit a specified DigiCert URL where the person enters their name and acknowledges that the person requesting the certificate has the right and authority to apply for the certificate. In addition, an email is also sent to the Applicant at the email address that will be listed in the certificate. The Applicant for the Enterprise Email Certificate must respond and acknowledge the certificate request.
Client Certificates Levels 2, 3 and 4 and PIV-I Certificates	Confirming with the organization that the individual is affiliated with the organization and that the individual has the authority to possess a certificate indicating the affiliation. The organization must request revocation of the certificate when the affiliate ends.
EU Qualified Certificates	Verifying that the individual is associated with the organization and is authorized and that the organization consents to the publication of the certificate.

3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1. Identification and Authentication for Routine Re-key

Subscribers may request automatic 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.

Subscribers re-establish their identity as follows:

Certificate	Routine Re-Key Authentication	Re-Verification Required
SSL Server Certificates	Username and password	At least every six years
EV SSL Certificates	Username and password	According to the EV Guidelines
Code Signing Certificates	Username and password	At least every six years
CDS Certificates	Username and password	At least every six years
Level 1 Client Certificates	Username and password	At least every nine years
Level 2 Client Certificates	Shared secret (PIN/password) meeting NIST 800-63 Level 2 entropy requirements (Table A.2)	At least every nine years
Level 3 and 4 Client Certificates and PIV-I Certificates	Current signature key	At least every nine years

DigiCert does not re-key a certificate without additional authentication if doing so would allow the Subscriber to use the certificate beyond the limits described above.

3.3.2. Identification and Authentication for Re-key After Revocation

A subscriber requesting re-key after a certificate is revoked for a reason other than during a renewal or update action undergoes the initial registration process.

3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

Revocation requests are authenticated. DigiCert may authenticate revocation requests by referencing 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. For certificates that include a domain name, the Domain Name Registrar record maintained by the domain registrar presumptively indicates who has authority over the domain. If a certificate request is submitted by an agent of the domain owner, the agent must send DigiCert a document that authorizes Subscriber's use of the domain (such as the letter in Appendix A). Applicants are responsible for any data that the Applicant or an agent of the Applicant supplies to DigiCert.

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

DigiCert does not issue certificates to any entity that is on a government denied list maintained by the United States or that is located in a country with which the laws of the United States prohibit doing business. For EV Certificates, DigiCert verifies that the Applicant, the Contract Signer, the Certificate Approver, the Applicant's Jurisdiction of Incorporation, Registration, and Place of Business are not included on such lists or subject to such prohibition.

4.1.2. Enrollment Process and Responsibilities

DigiCert requires each Applicant to submit a certificate request and application information prior to issuing a Certificate. DigiCert authenticates all communication from an Applicant and protects communication from modification.

Generally, Applicants request a certificate by completing the request forms online. DigiCert may, in its sole discretion, also allow certificate requests to be submitted by fax, email, or postal mail. Applicants are solely responsible for submitting a complete and accurate certificate request and signed Subscriber Agreement for each certificate.

The enrollment process includes:

1. Submitting a complete certificate application,
2. Generating a key pair,
3. Delivering the public key of the key pair to DigiCert,
4. Agreeing to the applicable Subscriber Agreement, and
5. Paying any applicable fees.

4.2. CERTIFICATE APPLICATION PROCESSING

4.2.1. Performing Identification and Authentication Functions

After receiving an application, DigiCert verifies the application information and other information in accordance with Section 3.2. All EV Certificates are validated in accordance with the EV Guidelines. After verification is complete, DigiCert evaluates the corpus of information and decides whether or not to issue the certificate.

4.2.2. Approval or Rejection of Certificate Applications

DigiCert rejects any certificate application that DigiCert cannot verify. DigiCert may also reject a certificate application if DigiCert believes that issuing the certificate could damage or diminish DigiCert's reputation or business.

Except for Enterprise EV Certificates, EV Certificate issuance approval requires two separate DigiCert validation specialists. The second validation specialist cannot be the same individual who collected the documentation and originally approved the EV Certificate. The second validation specialist reviews the collected information and documents for discrepancies or details that require further explanation. If the validation specialist has any concerns about the application, the second validation specialist may require additional explanations and documents. Enterprise RAs may perform the final cross-correlation and due diligence described herein using a single person representing the Enterprise RA. If satisfactory explanations and/or additional documents are not received within a reasonable time, DigiCert will reject the EV Certificate request and notify the Applicant accordingly.

If some or all of the documentation used to support the application is in a language other than English, a DigiCert employee skilled in such language and having the appropriate training, experience, and judgment in confirming organizational identification and authorization performs the final cross-correlation and due diligence. DigiCert may also rely on a translation of the relevant portions of the documentation by either a qualified translator or the RA who assisted with the validation.

If the certificate application is not rejected and is successfully validated in accordance with this CPS, DigiCert will approve the certificate application and issue the certificate. DigiCert is not liable for any rejected certificate and is not obligated to disclose the reasons for a rejection. Rejected Applicants may re-apply. Subscribers are required to check the data listed in the certificate for accuracy prior to using the certificate.

4.2.3. Time to Process Certificate Applications

Under normal circumstances, DigiCert confirms certificate application information and issues a digital certificate within a reasonable time frame. Issuance time frames are greatly dependent on when the Applicant provides the details and documentation necessary to complete validation. For non-EV SSL certificates, DigiCert will usually confirm submitted application data, complete the validation process, and issue or reject a certificate application within two working days after DigiCert receives all of the necessary details and documentation from the Applicant. DigiCert requires that identity be established no more than 30 days before initial issuance of a Level 3, Level 4, or PIV-I Certificate.

Occasionally, events outside of the control of DigiCert delay the issuance process. However, DigiCert makes reasonable effort to meet its issuance times and make Applicants aware of any factors that affect issuance times.

4.3. CERTIFICATE ISSUANCE

4.3.1. CA Actions during Certificate Issuance

DigiCert verifies the source of the certificate request and the identity of the Applicant in a secure manner prior to issuing a certificate. Any database used to confirm Subscriber information is protected from unauthorized modification. After validation is complete, the certificate is issued 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 via email to the email address designated by the Subscriber during the application process. The Subscriber is also provided a hypertext link to a user

id/password-protected location on DigiCert's web server where the Subscriber may log in and download each certificate or the zip file containing all certificates in the trust chain.

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 on the earlier of (i) the Subscriber's use of the certificate or (ii) 30 days after the certificate's issuance.

4.4.2. Publication of the Certificate by the CA

DigiCert publishes all CA certificate in its repository. 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 the issuance of certificate in which they are involved.

4.5. KEY PAIR AND CERTIFICATE USAGE

4.5.1. Subscriber Private Key and Certificate Usage

Subscribers are contractually 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 Private Keys only as specified in the key usage extension.

4.5.2. Relying Party Public Key and Certificate Usage

Relying Parties may only use software that is compliant with X.509 and other applicable standards. DigiCert does not warrant that any third party's 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. Any warranties provided by DigiCert are only valid if a Relying Party's reliance was reasonable and if the Relying Party adhered to the Relying Party Agreement set forth in the DigiCert repository.

A Relying Party should rely on a digital signature or SSL/TLS handshake only if:

1. the digital signature or SSL/TLS session was created during the operational period of a valid certificate and can be verified by referencing a valid certificate,
2. the certificate is not revoked and the Relying Party checked the revocation status of the certificate prior to the certificate's use by referring to the relevant CRLs or OCSP responses, and
3. the certificate is being used for its intended purpose and in accordance with this CPS.

Before relying on a time-stamp token, a Relying Party must:

1. verify that the time-stamp token has been correctly signed and that the Private Key used to sign the time-stamp token has not been compromised prior to the time of the verification,
2. take into account any limitations on the usage of the time-stamp token indicated by the time-stamp policy, and
3. take into account any other precautions prescribed in this CPS or elsewhere.

4.6. CERTIFICATE RENEWAL

4.6.1. Circumstance for Certificate Renewal

DigiCert may renew a certificate if:

1. the associated public key has not reached the end of its validity period,
2. the Subscriber name and attributes are unchanged,
3. the associated private key remains un compromised, and
4. re-verification of the Subscriber's identity is not required under Section 3.3.1.

DigiCert may also renew a certificate if a CA certificate is re-keyed.

DigiCert makes reasonable efforts to notify Subscribers via email of the imminent expiration of a digital certificate and may begin providing notice of pending expiration 60 days prior to the expiration date. Certificate renewal requires payment of additional fees which are disclosed on DigiCert's website and to Subscribers approaching their certificate expiration date.

4.6.2. Who May Request Renewal

Only an authorized representative of a Subscriber 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 validation personnel may reconfirm domain name ownership using current Domain Name Registrar information and may check state or other jurisdictional records to confirm geographic location, company control and good standing the jurisdiction of organization. If DigiCert cannot verify any information it rechecks, the certificate is not renewed. If an individual is renewing a client certificate and the individual's location and Domain Name Registrar information have not changed, then DigiCert does not require any additional identity vetting.

DigiCert will not reuse EV Certificate validation information if the age of the data exceeds the time specified in the EV Guidelines.

Some device platforms, e.g. Apache, allow renewed use of the Private Key. If the Subscriber's other contact information and Private Key have not changed, the Subscriber may use the same CSR as was used for the previous certificate.

4.6.4. Notification of New Certificate Issuance to Subscriber

DigiCert delivers renewed certificates to Subscribers in a secure fashion, typically via email to the address provided by the Subscriber during the renewal process. DigiCert may deliver the certificate by providing the Subscriber a hypertext link to a user id/password-protected location on DigiCert's web server 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 on the earlier of (i) the Subscriber's use of the certificate or (ii) 30 days after the certificate's renewal.

4.6.6. Publication of the Renewal Certificate by the CA

DigiCert publishes a renewed certificate by delivering it to the Subscriber. Renewed CA certificates are published in DigiCert's repository.

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

DigiCert may send any RA involved in the certificate issuance process notice of the certificate's issuance.

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 period, key identifiers, CLR and OCSP distributions, and a different signing key. After re-keying a certificate, DigiCert may revoke the old certificate but may not further re-key, renew, or modify the old certificate.

4.7.1. Who May Request Certificate Rekey

DigiCert may initiate certificate re-key certificates at the request of the certificate subject or in DigiCert's own discretion.

4.7.1. Processing Certificate Rekey Requests

If the Subscriber's other contact information and Private Key have not changed, DigiCert can issue a replacement certificate using the previously provided CSR. Otherwise, the Subscriber must submit a new CSR. DigiCert re-uses existing verification information unless re-verification is required under section 3.3.1 or DigiCert believes that the information has become inaccurate.

4.7.2. Notification of Certificate Rekey to Subscriber

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

4.7.3. Conduct Constituting Acceptance of a Rekeyed Certificate

Issued certificates are considered accepted on the earlier of (i) the Subscriber's use of the certificate or (ii) 30 days after the certificate is rekeyed.

4.7.4. Publication of the Issued Certificate by the CA

DigiCert publishes rekeyed certificates by delivering them to Subscribers.

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

DigiCert may send any RA involved in the certificate issuance process notice of the certificate's rekey.

4.8. CERTIFICATE MODIFICATION

Modifying a certificate means creating a new certificate for the same subject with authenticated 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.

After modifying a certificate, DigiCert can revoke the old certificate but will not further re-key, renew, or modify the old certificate.

4.8.1. 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.

4.8.2. Processing Certificate Modification Requests

After receiving a request for modification, DigiCert verifies any information that will change in the modified certificate. DigiCert will only issue the modified certificate after completing the verification process on all modified information. DigiCert will not issue a modified certificate that has a validity period that exceeds the applicable time limits found in section 3.3.1 or 6.3.2.

4.8.3. Notification of Certificate Modification to Subscriber

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

4.8.4. Conduct Constituting Acceptance of a Modified Certificate

Issued certificates are considered accepted on the earlier of (i) the Subscriber's use of the certificate or (ii) 30 days after the certificate is rekeyed.

4.8.5. Publication of the Modified Certificate by the CA

DigiCert publishes modified certificates by delivering them to Subscribers.

4.8.6. Notification of Certificate Modification by the CA to Other Entities

DigiCert may send any RA involved in the certificate issuance process notice of the certificate's modification.

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;
4. The Subscriber or DigiCert breached a material obligation under the CP, the CPS, or the relevant Subscriber Agreement;
5. Either the Subscriber's or DigiCert's obligations under the CP or 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 certificate was not issued in accordance with the CP, CPS, or applicable industry standards;
7. DigiCert received a lawful and binding order from a government or regulatory body to revoke the certificate;
8. DigiCert ceased operations and did not arrange for another certificate authority to provide revocation support for the certificates;
9. 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);
10. A court or arbitrator revoked the Subscriber's right to use a name or mark listed in the certificate, or the Subscriber failed to maintain a valid registration for such name or mark;
11. Any information appearing in the Certificate was or became inaccurate or misleading;
12. 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;
13. For CDS Certificates, upon Adobe's request; or
14. For code-signing certificates, the certificate was used to sign, publish, or distribute malware, code that is downloaded without user consent, or other harmful content.

DigiCert always revoke a certificate if the binding between the subject and the subject's public key in the certificate is no longer valid or if an associated Private Key is compromised.

4.9.2. Who Can Request Revocation

The Subscriber or another appropriately authorized party (such as an administrative contact, a Contract Signer, Certificate Approver, or Certificate Requester) may request revocation of a certificate. DigiCert may require that the revocation request be made by either the organizational contact, billing contact or domain registrant.

DigiCert will revoke a certificate if it receives sufficient evidence of compromise of loss of the private key and may revoke a certificate of its own volition without reason, even if no other entity has requested revocation. Other entities may request revocation of a certificate for problems related to fraud, misuse, or compromise by filing a "Certificate Problem Report". All certificate revocation requests must include the identity of the entity requesting revocation and the reason for revocation.

4.9.3. Procedure for Revocation Request

Entities submitting certificate revocation requests must list their identity and explain the reason for requesting revocation. DigiCert employs the following procedure after receiving a revocation request:

1. DigiCert personnel log 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 requests confirmation of the revocation from a known administrator via out-of-band communication (e.g., telephone, fax, etc.).
3. If the request is authenticated as originating from the Subscriber, DigiCert will always revoke a certificate.
4. For requests from third parties, DigiCert personnel begin investigating all Certificate Problem Reports within 24 hours after receipt and decide whether revocation is appropriate based on the following criteria:
    a. the nature of the alleged problem,
    b. the number of Certificate Problem Reports received about a particular certificate or website,
    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 revocation is appropriate, DigiCert personnel revoke the certificate and have the CRL updated.

DigiCert maintains a continuous 24/7 ability to internally respond to any high priority Certificate Problem Reports. If appropriate, DigiCert forwards complaints to law enforcement. The serial number of the revoked certificate remains on the CRL until one additional CRL is published after the end of the certificate's validity period.

Whenever a PIV-I Card is no longer valid, the RA responsible for its issuance or maintenance is required collect it from the Subscriber as soon as possible, destroy it, and log its collection and physical destruction.

4.9.4. Revocation Request Grace Period

DigiCert provides revocation grace periods to Subscribers 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 instructions from the DCPA. Other certificates are revoked as quickly as practical after validating the revocation request in accordance with the following process:.

1. Revocation requests received two or more hours before a CRL issuance are processed before the next CRL is published,
2. Revocation requests received within two hours of CRL issuance are processed before the following CRL is published, and
3. Regardless, all Certificate revocation requests are processed within 18 hours after their receipt.

4.9.6. Revocation Checking Requirement for Relying Parties

Prior to relying on information listed in a certificate, a Relying Party must confirm the validity of each certificate in the certificate path in accordance with IETF PKIX standards, including checks for certificate validity, issuer-to-subject name chaining, policy and key use constraints, and revocation status through CRLs or OCSP responders identified in each certificate in the chain.

4.9.7. CRL Issuance Frequency

DigiCert uses its offline root CAs to publish CRLs for its intermediate CAs at least every 6 months. For an offline CA that has been cross-signed by the Federal Bridge CA and only issue CA certificates, certificate-status-checking certificates, or internal administrative certificates, DigiCert issues a CRL at least every 31 days. All other CRLs are published at least every 24 hours. If a Certificate is revoked for reason of key compromise, an interim CRL is published as soon as feasible, but no later than 18 hours after receipt of the notice of key compromise.

4.9.8. Maximum Latency for CRLs

CRLs are posted automatically to the online repository within a commercially reasonable time after generation, usually within minutes of generation. Irregular, interim, or emergency CRLs are posted no later than four hours after generation (and no later than 18 hours after notification of compromise). Otherwise, DigiCert always posts regularly scheduled CRLs prior to the nextUpdate field in the previously issued CRL of the same scope.

4.9.9. On-line Revocation/Status Checking Availability

DigiCert makes certificate status information available via OCSP for SSL and PIV-I Certificates. OCSP may not be available for other kinds of certificates. Where OCSP support is required by the applicable CP, OCSP responses are provided within a commercially reasonable time and no later than six seconds after the request is received, subject to transmission latencies over the Internet.

4.9.10. On-line Revocation Checking Requirements

A relying party must confirm the validity of a certificate in accordance with section 4.9.6 prior to relying on the certificate.

4.9.11. Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12. Special Requirements Related to Key Compromise

DigiCert uses commercially reasonable efforts to notify potential Relying Parties if it discovers or suspects the compromise of a Private Key. DigiCert will transition any revocation reason code in a CRL to "key compromise" upon discovery of such reason or as required by an applicable CP. If a certificate is revoked because of compromise, DigiCert will issue a new CRL within 18 hours after receiving notice of the compromise.

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 is available via CRL and OCSP responder.

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
DigiCert never escrows CA Private Keys. However, DigiCert may escrow Subscriber key management keys to provide key recovery services. When providing escrow services, DigiCert encrypts and protects escrowed Private Keys using at least the level of security that was used to generate and deliver the Private Key. DigiCert never allows the escrow of a Subscriber's private signature key.

DigiCert allows Subscribers and other authorized entities to recover escrowed (decryption) Private Keys. DigiCert implements multi-person controls when its personnel are involved in key recovery in order to prevent unauthorized access to a Subscriber's escrowed Private Keys. DigiCert accepts key recovery requests:

1. From the Subscriber or Subscriber's organization, if the Subscriber has lost or damaged the private key token;
2. From the Subscriber's organization, if the Subscriber is not available or is no longer part of the organization that contracted with DigiCert for Private Key escrow;
3. From an authorized investigator or auditor, if the Private Key is part of a required investigation or audit;
4. From a requester authorized by a competent legal authority to access the communication that is encrypted using the key;
5. From a requester authorized by law or governmental regulation; or
6. From an entity contracting with DigiCert for escrow of the Private Key when key recovery is mission critical or mission essential.

Entities that receive key escrow services shall:

1. Notify Subscribers that their Private Keys are escrowed;
2. Protect escrowed keys from unauthorized disclosure;
3. Protect any authentication mechanisms that could be used to recover escrowed Private Keys;
4. Release escrowed keys only for properly authenticated and authorized requests for recovery;

5. Not enter into any obligation to communicate key recovery process or requests to the Subscriber or any third party;
6. Not disclose key recovery processes or requests to the Subscriber or third parties when prohibited by law or internal policy; and
7. Not disclose escrowed keys or escrowed key-related information to any third party unless required to do so by law or the entity's internal policies.

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 and TSA operations from secure, geographically diverse, commercial data centers that are equipped with logical and physical controls that make DigiCert's CA and TSA 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.

The buildings where DigiCert's CA and TSA systems are housed are accessed through areas with security personnel on duty full time (24 hours per day, 365 days per year). 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 stores all removable media and paper containing sensitive plain-text information related to its CA operations in secure, locked containers.

5.1.2.1. Data Center

Access to the data centers housing the CA and TSA platforms requires two-factor authentication—the individual must have an authorized access card, and doors to access rooms where the equipment is housed are equipped with biometric access control authenticators. These card-based biometric authentication access systems are also programmed to log each use of the access card.

DigiCert deactivates, removes, 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 and is never stored with the cryptographic module or removable hardware associated with equipment used to administer DigiCert's private keys.

The DigiCert facility is continuously attended. However, if DigiCert ever becomes aware that a data center has been left unattended, DigiCert personnel will perform a security check of the data 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, vent covers) 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.

5.1.2.2. Support and Vetting Room

A controlled access door secures the support and vetting room where DigiCert personnel perform identity vetting and other RA functions. Access card use is logged by the building security system. The room is equipped with motion-activated video surveillance cameras.

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 and TSA 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 daily basis and are stored in a backup location that is separate from DigiCert's primary facility.

5.1.7. Waste Disposal

All out-dated or unnecessary copies of printed sensitive information are shredded on-site before disposal. All electronic media are zeroized (all data is overwritten with binary zeros so as to prevent the recovery of the data) using programs meeting U.S. Department of Defense requirements.

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. On at least a weekly basis, DigiCert moves media designated for storage off-site to a safe deposit box located inside a federally insured financial institution. Backup copies of CA Private Keys and activation data are stored off-site in locations that are accessible only by trusted personnel.

5.1.9. CMS and External RA Systems

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

5.2. PROCEDURAL CONTROLS

5.2.1. Trusted Roles

Personnel acting in trusted roles include CA, TSA, and RA system administration personnel, and personnel involved with identity vetting and customer support. The functions and duties performed by persons in trusted roles are distributed so that one person alone cannot circumvent security measures or subvert the security and trustworthiness of the PKI or TSA operations. 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.

Persons acting in trusted roles are only allowed to access a CMS after they are authenticated using a method commensurate with issuance and control of PIV-I Hardware.

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.

5.2.1.1. CA Officers – CMS, RA, Validation and Vetting Personnel

The CA 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.

5.2.1.2. 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, CMS and RA systems updated with software patches and other maintenance needed for system stability and recoverability.

5.2.1.3. Internal Auditors

Internal Auditors are responsible for reviewing, maintaining, and archiving audit logs and performing or overseeing internal compliance audits to determine if DigiCert, an Issuer CA, or RA is operating in accordance with this CPS or an RA's Registration Practices Statement.

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 to activate DigiCert's Private Keys, generate a CA key pair, or backup 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.

No single individual has the capability to issue a PIV-I credential.

5.2.3. Identification and Authentication for each Role

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

5.2.4. Roles Requiring Separation of Duties

Roles requiring a separation of duties include:

1. The verification of information in certificate applications,
2. The approval of certificate applications,
3. The approval of revocation requests, and
4. Most duties related to CA/TSA key management or CA/TSA administration.

DigiCert specifically designates individuals to the trusted roles defined above. Individuals may assume only one of the Officer, Administrator, and Auditor roles, but any individual may assume the Operator role. DigiCert's systems identify and authenticate individuals acting in trusted roles, restrict an individual from assuming multiple roles, and prevent any individual from having more than one identity.

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 and the CP. 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. All trusted roles for CAs issuing Client Certificates at Levels 3 and 4 and for PIV-I Certificates

are held by citizens of the United States. An individual performing a trusted role for an RA may be a citizen of the country where the RA is located. There is no citizenship requirement for personnel performing trusted roles associated with the issuance of other kinds of certificates.

Management and operational support personnel involved in time-stamp operations possess experience with information security and risk assessment and knowledge of time-stamping technology, digital signature technology, mechanisms for calibration of time stamping clocks with UTC, and security procedures. The DCPA ensures that all individuals assigned to trusted roles have the experience, qualifications, and trustworthiness required to perform their duties under this CPS.

5.3.2. Background Check Procedures

DigiCert verifies the identity of each person to be 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 the required forms of 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. Background investigations are performed by a competent independent authority that has the authority to perform background investigations. 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.

5.3.3. Training Requirements

DigiCert provides skills training to all personnel involved in DigiCert's PKI and TSA 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. disaster recovery and business continuity procedures,
5. common threats to the validation process, including phishing and other social engineering tactics, and
6. applicable industry and government guidelines.

Training lasts for at least two months and 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. Validation Specialists must have the minimum skills necessary to satisfactorily perform validation duties before being granted validation privileges. All Validation Specialists validating EV Certificates are required to pass an internal examination on the EV Certificate validation criteria outlined in the EV Guidelines.

5.3.4. Retraining Frequency and Requirements

Personnel 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 individuals 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 personnel 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, including a copy of the CP, this CPS, EV Guidelines, and other technical and operational documentation needed to maintain the integrity of DigiCert's CA operations. 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 and TSA 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. DigiCert records the precise time of any significant TSA events. All 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

Auditable Event
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
Installation of a PKI Application
Installation of a Hardware Security Modules
Removal of HSMs
Destruction of HSMs
System Startup
Logon attempts to PKI Application
Receipt of hardware / software
Attempts to set passwords
Attempts to modify passwords
Backup of the internal CA database
Restoration from backup 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

Auditable Event
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 or TSA component
Access to a CA or TSA 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 CA 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

DigiCert personnel are required to keep all generated audit log information on their equipment until after it is copied by the System Administrator. DigiCert's CA and TSA 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.

DigiCert makes time-stamping records available when required to prove in a legal proceeding that DigiCert's time-stamping services are operating correctly. Audit logs are made available to auditors upon request.

5.4.5. Audit Log Backup Procedures

On at least a monthly basis, DigiCert makes backup copies of audit logs and audit log summaries and sends a copy of the audit log off-site.

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 will consider suspending its operation until the problem is remedied.

5.4.7. Notification to Event-causing Subject

No stipulation.

5.4.8. Vulnerability Assessments

DigiCert performs routine 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 assess the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the DigiCert has in place to control such risks. DigiCert's auditors review the security audit data checks for continuity and will 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 or time-stamp token 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 / TSA operations):

1. Accreditations of DigiCert,
2. CP and CPS versions,
3. Contractual obligations and other agreements concerning the operation of the CA / TSA,
4. System and equipment configurations, modifications, and updates,
5. Certificate and revocation requests,
6. Identity authentication data,
7. Any documentation related to the receipt or acceptance of a certificate or token,
8. Subscriber Agreements,
9. Issued certificates,
10. A record of certificate re-keys,
11. CRLs,
12. Any data or applications necessary to verify an archive's contents,
13. Compliance auditor reports,
14. Any changes to DigiCert's audit parameters,
15. Any attempt to delete or modify audit logs,
16. Key generation,
17. Access to Private Keys for key recovery purposes,
18. Changes to trusted Public Keys,
19. Export of Private Keys,
20. Approval or rejection of a certificate status change request,

21. Appointment of an individual to a trusted role,
22. Destruction of a cryptographic module,
23. Certificate compromise notifications,
24. Remedial action taken as a result of violations of physical security, and
25. Violations of the CP or CPS.

5.5.2. Retention Period for Archive

DigiCert retains archived data for at least 10.5 years.

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 shall main 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

Backups are written on a daily basis to a server at a secure location. In general, the process for creating, packaging, and transmitting archived records and backup copies is automated.

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.

DigiCert stamps and records information collected during the identity verification process, including IP addresses associated with applicant submissions and screen shots provided by verification information sources where applicable.

Certificate issuance is time-stamped as a function of the "Valid From" field in accordance with the X.509 Certificate Profile.

Certificate revocation is time-stamped as a function of the "Revocation Date" field in accordance with the X.509 Certificate Revocation List Profile.

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

Upon a proper request made for a proper purpose by a Customer, its agent, or a party involved in a dispute over a transaction involving the DigiCert PKI, and payment of all associated research, retrieval, verification, and redaction costs, DigiCert will create, verify, package, and send that discrete portion of the archived information that is relevant to the dispute or question involving the DigiCert PKI. The integrity of archived information is verified when it is restored by, among other things, reference to the time stamps associated with such records as described in Section 5.5.5. Access and use of archive data is restricted in accordance with DigiCert's internal security policies and procedures which govern the creation, verification, packaging, transmission, and storage of archive information.

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 (well in advance of expiration) and uses the old Private Key only to sign CRLs and OCSP responder certificates. A new CA signing key pair is commissioned and all subsequently issued certificates and CRLs are signed with the new private signing key. Both the old and the new key pairs may be concurrently active. This key changeover process helps minimize any adverse effects from CA certificate expiration. The corresponding new CA Public Key certificate is provided to subscribers and relying parties through the delivery methods detailed in Section 6.1.4.

5.7. COMPROMISE AND DISASTER RECOVERY

5.7.1. Incident and Compromise Handling Procedures

If a disaster causes DigiCert's CA or TSA operations to become inoperative, DigiCert will re-initiate its operations on replacement hardware using backup copies of its software, data, and Private Keys at a comparable, secured facility after ensuring the integrity and security of the CA or TSA systems. DigiCert will give priority to reestablishing the generation of certificate status information and time stamping capabilities. If the Private Keys are destroyed, DigiCert will reestablish operations as quickly as possible, giving priority to generating new key pairs.

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

DigiCert makes daily system backups and regular Private Key backups. Private Key backups are stored in a secure off-site location. If a disaster causes DigiCert's CA or TSA operations to become inoperative, DigiCert shall, after ensuring the integrity and security of the CA or TSA systems, re-initiate its operations on replacement hardware using backup copies of its software, data, and Private Keys at a secure facility. DigiCert shall give priority to reestablishing the generation of certificate status information and time stamping capabilities. If the Private Keys are destroyed, DigiCert shall reestablish operations as quickly as possible, giving priority to generating new key pairs.

5.7.3. Entity Private Key Compromise Procedures

If DigiCert suspects that one of its Private Keys has been comprised or lost then DigiCert's Operations Manager will immediately convene an emergency incident response team to assess the situation, to determine the degree and scope of the incident, and take appropriate action, including implementing DigiCert's incident response plan. Specifically, DigiCert will:

1. Collect all information related to the incident (and if the event is ongoing, ensure that all data is captured and recorded);
2. Begin investigating the incident and determine the degree and scope of the compromise;
3. Have its incident response team determine and report on the course of action or strategy that should be taken to correct the problem and prevent reoccurrence;
4. If appropriate, contact government agencies, law enforcement, and other interested parties and activate any other appropriate additional security measures;
5. If the compromises involves a Private Key used to sign time-stamp tokens, provide a description of the compromise to Subscribers and Relying Parties;
6. Notify any cross-certified entities of the compromise so that they can revoke their cross-certificates;
7. Make information available that can be used to identify which certificates and time-stamp tokens are affected, unless doing so would breach the privacy of a DigiCert user or the security of DigiCert's services;
8. Monitor its system, continue its investigation, ensure that data is still being recorded as evidence, and make a forensic copy of data collected;
9. Isolate, contain, and stabilize its systems, applying any short-term fixes needed to return the system to a normal operating state;
10. Prepare and circulate an incident report that analyzes the cause of the incident and documents the lessons learned; and

11. Incorporate lessons learned into the implementation of long term solutions and the Incident Response Plan.

Following revocation of the corresponding certificate and implementation of the Incident Response Plan, DigiCert may generate a new key pair and sign a new certificate. DigiCert will distribute the new certificate in accordance with Section 6.1.4. DigiCert will cease related operations until appropriate steps have been taken to recover from the compromise and restore security. If a disaster physically damages DigiCert's equipment and destroys all copies of DigiCert's signature keys then DigiCert will provide notice to all interested 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. DigiCert has developed a Business Continuity Management Program (BCMP). 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 with a tertiary system located at a separate, geographically diverse location for failover in the event of a disaster.

5.8. CA OR RA TERMINATION

Before terminating its CA or TSA activities, DigiCert will:

1. Provide notice and information about the termination by sending notice by email to its customers, Application Software Vendors, and cross-certifying entities and by posting such information on DigiCert's web site; and
2. Transfer all responsibilities to a qualified successor entity.

If no qualified successor entity exists, 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

All keys must be generated using a FIPS-approved method or equivalent international standard.

DigiCert's CA key pairs are generated by multiple trusted individuals using a cryptographic hardware device as part of scripted key generation ceremony. The cryptographic hardware is evaluated to FIPS 140-1 Level 3 and EAL 4+. Activation of the hardware requires the use two-factor authentication tokens.

The key generation ceremony is performed by DigiCert personnel acting in trusted roles. 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.

An independent auditor validates that each key is generated in accordance with this CPS by having the auditor either witness the key generation or examine a signed and documented record of the key generation. DigiCert requires that an auditor witness the generation of any CA keys used to sign CDS Certificates or EV Certificates.

After the root key is generated, the auditor issues a report that DigiCert:

1. Documented its root key generation and protection procedures,
2. Included appropriate detailed procedures and controls in its root key generation script, and
3. Performed all of the procedures required by the root key generation script.

Subscribers must generate their keys in a secure manner that is appropriate for the certificate type. Keys for Level 3 Hardware or Level 4 Biometric certificates must be generated on validated hardware cryptographic modules using a FIPS-approved method. Subscribers who generate their own keys for a Qualified Certificate on an SSCD shall ensure that the SSCD meets the requirements of CWA 14169 and that the Public Key to be certified is from the key pair generated by the SSCD.

6.1.2. Private Key Delivery to Subscriber

If DigiCert, a CMS, or an RA generates a key for a Subscriber, then it must deliver the Private Key securely to the Subscriber. Keys may be delivered electronically or on a hardware cryptographic module / SSCD. In all cases:

1. The key generator will not retain a copy of the Subscriber's Private Key after delivery,
2. The key generator will protect the private key from activation, compromise, or modification during the delivery process,
3. The Subscriber must acknowledge receipt of the private key(s), and
4. The key generator will deliver the Private Key in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers, including:
    a. For hardware modules, the key generator maintaining accountability for the location and state of the module until the Subscriber accepts possession of it and
    b. For electronic delivery of private keys, the key generator encrypting key material using a cryptographic algorithm and key size at least as strong as the private key. The key generator shall deliver activation data using a separate secure channel.

The entity assisting the Subscriber with key generation shall maintain a record of the Subscriber's acknowledgement of receipt of the device containing the Subscriber's Key Pair. A CMS or RA providing key delivery services is required to provide a copy of this record to DigiCert.

6.1.3. Public Key Delivery to Certificate Issuer

The Subscriber generates its key pair and submits the Public Key to DigiCert in a CSR as part of the certificate request process. The Subscriber's signature is authenticated prior to issuing the certificate.

6.1.4. CA Public Key Delivery to Relying Parties

DigiCert's Public Keys are provided to Relying Parties as specified in a certificate validation or path discovery policy file, as trust anchors in commercial browsers and operating system root store, and/or as roots signed by other CAs. DigiCert may also distribute Public Keys that are part of an updated signature key pair as a self-signed certificate, as a new CA certificate, or in a key roll-over certificate. Relying Parties may obtain DigiCert's self-signed CA certificates from DigiCert's web site or by email.

6.1.5. Key Sizes

DigiCert follows the NIST timelines in using and retiring signature algorithms and key sizes. Currently, DigiCert generates and uses the following keys, signature algorithms, and hash algorithms for signing certificates, CRLs, and certificate status server responses:

2048-bit RSA Key with Secure Hash Algorithm version 1 (SHA-1)
2048-bit RSA Key with Secure Hash Algorithm version 2 (SHA-256)

384-bit ECDSA Key with Secure Hash Algorithm version 2 (SHA-256)

DigiCert issues end-entity certificates that contain the following:

1. For certificates that expire on or before Dec 31, 2010, at least 1024-bit Public Keys for RSA or 224-bit Public Keys for ECDSA,
2. For certificates that expire on or after Dec 31, 2013 and that include a keyUsage extension that only asserts the digitalSignature bit, at least 2048 bits for RSA or DSA, or 224 bits for elliptic curve algorithms,
3. For certificates expiring after 12/31/2010, at least 2048 bits for RSA, DSA, or Diffie-Hellman, or 224 bits for elliptic curve algorithms,

DigiCert may require higher bit keys in its sole discretion. PIV-I Certificates contain public keys and algorithms that conform to [NIST SP 800-78].

Any certificates (whether CA or end-entity) expiring after 12/31/2030 must be at least 3072 bit for RSA and 256 bit for ECDSA. Signatures on certificates, OCSP responses, and CRLs that are issued after 12/31/2010 are generated using, at a minimum, SHA-224. Signatures on certificates, OCSP responses, and CRLs that are issued after 12/31/2030 are generated using, at a minimum, SHA-256.

DigiCert and Subscribers may fulfill their requirements under the CP and this CPS using TLS or another protocol that provides similar security, provided the protocol requires at least:

1. triple-DES or equivalent for the symmetric key and at least 1024 bit RSA or equivalent for the asymmetric keys through 12/31/2010,
2. AES (128 bits) or equivalent for the symmetric key and at least 2048 bit RSA or equivalent for the asymmetric keys after 12/31/2010, and
3. AES (128 bits) or equivalent for the symmetric key, and at least 3072 bit RSA or equivalent for the asymmetric keys after 12/31/2030.

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 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. Key usage bits and extended key usages are specified in the certificate profile for each type of certificate as set forth in DigiCert's Certificate Profiles document.

DigiCert does not issue Level 3 and Level 4 certificates that are certified for both signing and encryption. DigiCert may issue Level 1 and Level 2 certificates that can be used for both encryption and signature. Such dual-use certificates must:

1. be generated and managed in accordance with their respective signature certificate requirements, except where otherwise noted in this CPS.
2. never assert the non-repudiation key usage bit, and
3. not be used for authenticating data that will be verified on the basis of the dual-use certificate at a future time.

6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1. Cryptographic Module Standards and Controls

DigiCert's cryptographic modules are validated to the FIPS 140 Level 3 and International Common Criteria (CC) Information Technology Security Evaluation Assurance Level (EAL) 14169 EAL 4+ Type 3 (EAL 4 Augmented by AVA_VLA.4 and AVA_MSU.3) in the European Union (EU).

Cryptographic module requirements for subscribers and registration authorities are shown in the table below.

Assurance Level	Subscriber	Registration Authority
CDS	FIPS 140 Level 2 (Hardware)	FIPS 140 Level 3 (Hardware)
Level 1	N/A	FIPS 140 Level 1 (Hardware or Software)
Level 2	FIPS 140 Level 1 (Hardware or Software)	FIPS 140 Level 1 (Hardware or Software)
Level 3	FIPS 140 Level 1 (Software) FIPS 140 Level 2 (Hardware)	FIPS 140 Level 2 (Hardware)
Level 4	FIPS 140 Level 2 (Hardware)	FIPS 140 Level 2 (Hardware)
Level 4 & PIV-I Card Authentication	FIPS 140 Level 2 (Hardware)	FIPS 140 Level 2 (Hardware)
EU QC on SSCD	EAL 4 Augmented (Hardware)	EAL 4 Augmented (Hardware)

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

DigiCert does not escrow its signature keys. Subscribers may not escrow their private signature keys or dual use keys. DigiCert may provide escrow services for Subscriber Private Keys used for encryption.

6.2.4. Private Key Backup

DigiCert's Private Keys are generated and stored inside DigiCert's cryptographic module, which has been evaluated to at least FIPS 140 Level 3 and EAL 4+. When keys are transferred to other media for backup and disaster recovery purposes, the keys are transferred and stored in an encrypted form. DigiCert's CA key pairs are backed up by multiple trusted individuals using a cryptographic hardware device as part of scripted and videotaped key backup process.

DigiCert may provide backup services for (1) Level 1, Level 2, and Level 3 subscriber private signature keys, provided that the backup copies are held in Subscriber's control and (2) subscriber key management keys. DigiCert may require backup of PIV-I Content Signing private signature keys to facilitate disaster recovery, provided that all backup is performed under multi-person control.

DigiCert does not backup Level 4 subscriber private signature keys. Backup keys are stored with security controls that are consistent with the protection provided by the Subscriber's cryptographic module. Backed up keys are never stored in a plain text form outside of the cryptographic module.

6.2.5. Private Key Archival

DigiCert does not archive Private Keys.

6.2.6. Private Key Transfer into or from a Cryptographic Module

All keys must be generated by and in a cryptographic module. Private Keys are exported from the cryptographic module only for backup purposes. The Private Keys are encrypted when transferred out of the module and never exist in plaintext form. When transported between cryptographic modules, DigiCert encrypts the private key and protects the keys used for encryption from disclosure. Private Keys used to encrypt backups are securely stored and require two-person access.

6.2.7. Private Key Storage on Cryptographic Module

DigiCert's Private Keys are generated and stored inside DigiCert's cryptographic module, which has been evaluated to at least FIPS 140 Level 3 and EAL 4+.

6.2.8. Method of Activating Private Keys

DigiCert's Private Keys are activated according to the specifications of the cryptographic module manufacturer during a scripted, videotaped, and witnessed key generation or certificate signing ceremony. Activation data entry is protected from disclosure.

Subscribers are solely responsible for protection of 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. *See also* Section 6.4.

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. Root Private Keys are further deactivated by removing them entirely from the storage partition on the HSM device. 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 personnel acting in trusted roles destroy CA, RA, and status server Private Keys when they are 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. If the zeroization or re-initialization procedure fails, DigiCert will crush, shred, and/or incinerate the device in a manner that destroys the ability to extract any Private Key.

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

DigiCert certificates have maximum validity periods of:

Type	Private Key Use	Certificate Term
Root CA	20 years	25 years
Sub CA	12 years	15 years
CRL and OCSP responder signing	3 years	31 days*
OV SSL	No stipulation	42 months
EV SSL	No stipulation	27 months
Time Stamping Authority	10 years	10 years
Code Signing Certificate	39 months	10 years†
CDS Certificate	39 months	5 years
End Entity Client used for signatures, including EU Qualified Certificates, code and content signatures	36 months	36 months
End Entity Client used for key management	36 months	36 months
End Entity Client for all other purposes	42 months	42 months
PIV-I Cards	60 months	60 months

* OCSP responder and CRL signing certificates associated with a PIV-I certificate only have a maximum certificate validity period of 31 days.
† Extended from 39 months to 10 years under either the Time Stamp or Signing Authority method.

Relying parties may still validate signatures generated with these keys after expiration of the certificate. Private keys associated with self-signed root certificates that are distributed as trust anchors are used for a maximum of 20 years. DigiCert does not issue PIV-I subscriber certificates that expire later than the expiration date of the PIV-I hardware token on which the certificates reside.

DigiCert may voluntarily retire its CA Private Keys before the periods listed above to accommodate key changeover processes. DigiCert does not issue Subscriber certificates with an expiration date that is past the signing root's expiration date or that exceeds the routine re-key identification requirements specified in Section 3.1.1.

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. This method has been evaluated as meeting the requirements of FIPS 140-2 Level 3. The cryptographic hardware is held under two-person control as explained in Section 5.2.2 and elsewhere in this CPS. DigiCert will only transmit activation data via an appropriately protected channel and at a time and place that is distinct the associated cryptographic module.

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

If DigiCert must reset activation data associated with a PIV-I certificate then DigiCert or an RA performs a successful biometric 1:1 match of the applicant against the biometrics collected in Section 3.2.3.

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. All systems are scanned for malicious code and protected against spyware and viruses.

DigiCert's systems, including any remote workstations, are configured to:

7. authenticate the identity of users before permitting access to the system or applications,
8. manage privileges of users to limit users to their assigned roles,
9. generate and archive audit records for all transactions,
10. enforce domain integrity boundaries for security critical processes, and
11. support recovery from key or system failure.

All Certificate Status Servers:

1. authenticate the identity of users before permitting access to the system or applications,
2. manage privileges to limit users to their assigned roles,
3. enforce domain integrity boundaries for security critical processes, and
4. support recovery from key or system failure.

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 senior administrator (e.g. the Operations Manager, CA Administrator or System Administrator/ System Engineer) who must be different from the person submitting the request. This allows DigiCert to verify that each change to the system was properly evaluated for risk mitigation and authorized by management. DigiCert only installs software on CA systems that is necessary to the CA's operation and all CA hardware and software is dedicated only 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 under a formal, documented, development methodology in a controlled environment. 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, including change control data entries that are processed, logged and tracked for any security-related changes. 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, a Demilitarized Zone (DMZ) 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 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 necessary ports 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

The system time on DigiCert's computers is updated using the Network Time Protocol (NTP) to synchronize system clocks at least once every eight hours (Windows default). All times are traceable to the real time value distributed by a UTC(k) laboratory or National Measurement Institute and are updated when a leap second occurs as notified by the appropriate body. DigiCert maintains an accuracy of its clocks within one second or less. However, Relying Parties should be aware that all times included in a time-stamp token are synchronized with UTC within the accuracy defined in the time-stamp token itself, if present.

If a clock is detected as inaccurate, DigiCert will not issue a time-stamp token using that clock. All clocks used for time-stamping are housed in the DigiCert's secure facilities and are protected against threats that could result in an unexpected change to the clock's time. DigiCert's facilities automatically detect and report any clock that drifts or jumps out of synchronization with UTC. All clock adjustments are auditable events.

DigiCert includes a unique integer for each newly generated time-stamp token. DigiCert only time-stamps hash representations of data, not the data itself. Information can be hashed for time-stamping using SHA-1 or SHA-256 with RSA encryption and either 1024 or 2048 bit key size for signature creation. DigiCert does not examine the imprint being time-stamped other than to check the imprint's length. DigiCert also does not include any identification of the Time Stamp Token

Requester (TST Requester) in the time-stamp token. All time-stamp tokens are signed using a key generated exclusively for that purposes and have the property of the key indicated in the certificate.

TST Requesters request time-stamp tokens by sending a request to DigiCert. After the TST Requester receives a response from DigiCert, it must verify the status error returned in the response. If an error was not returned, the TST Requester must then verify the fields contained in the time-stamp token and the validity of the time-stamp token's digital signature. In particular, the TST Requester must verify that the time-stamped data corresponds to what was requested and that the time-stamp token contains the correct certificate identifier, the correct data imprint, and the correct hash algorithm OID. The TST Requester must also verify the timeliness of the response by verifying the response against a local trusted time reference. The TST Requester is required to notify DigiCert immediately if any information cannot be verified.

Time Stamp Verifiers shall verify the digital signature on the time-stamp token and confirm that the data to be verified corresponds to the hash value in the time-stamp token by generating a hash value of the data using the same hash algorithm as indicated in the time-stamp token, and comparing the generated hash value with the hash value contained in the time-stamp token.

6.9. PIV-I CARDS

The following requirements apply to PIV-I Cards:

1. To ensure interoperability with Federal systems, PIV-I Cards use a smart card platform that is on GSA's FIPS 201 Evaluation Program Approved Product List (APL) and use the PIV application identifier (AID).
2. All PIV-I Cards conform to [NIST SP 800-731].
3. The mandatory X.509 Certificate for Authentication is only issued under a policy that is cross certified with the FBCA PIV-I Hardware policy OID.
4. PIV-I certificates conform to the PIV-I Profile.
5. An asymmetric X.509 Certificate for Card Authentication is included in each PIV-I card. The Certificate:
    a. conforms to PIV-I Profile,
    b. conforms to [NIST SP 800-73], and
    c. is issued under the PIV-I Card Authentication policy.
6. The CMS includes an electronic representation (as specified in SP 800-73 and SP 800-76) of the cardholder's facial image in each PIV-I card.
7. The X.509 Certificates for Digital Signature and Key Management described in [NIST SP 800-73] are optional for PIV-I Cards.
8. The CMS makes its PIV-I Cards visual distinct from a Federal PIV Card to prevent creation of a fraudulent Federal PIV Card. At a minimum, the CMS does not allowed images or logos on a PIV-I Card to be placed within Zone 11, *Agency Seal*, as defined by [FIPS 201].
9. The CMS requires the following items on the front of a card:
    a. Cardholder facial image,
    b. Cardholder full name,
    c. Organizational Affiliation, if exists; otherwise the issuer of the card, and
    d. Card expiration date.
10. PIV-I cards are issued with an expiration date that is five years or less.
11. All PIV-I Card expire later than the PIV-I Content Signing certificate on the card.
12. A policy OID that has been mapped to the FBCA PIV-I Content Signing policy OID is included in the digital signature certificate used to sign objects on the PIV-I Card. The PIV-I Content Signing certificate conforms to the PIV-I Profile.
13. The PIV-I Content Signing certificate and corresponding private key are managed within a trusted Card Management System.
14. At issuance, the PIV-I Card is activated and released to the subscriber only after a successful 1:1 biometric match of the applicant against the biometrics collected in Section 3.2.3.
15. PIV-I Cards may support card activation by the card management system to support card personalization and post-issuance card update. To activate the card for personalization or

update, the card management system performs a challenge response protocol using cryptographic keys stored on the card in accordance with [SP800-73]. When cards are personalized, card management keys are set to be specific to each PIV-I Card. That is, each PIV-I Card contains a unique card management key. Card management keys meet the algorithm and key size requirements stated in Special Publication 800-78, Cryptographic Algorithms and Key Sizes for Personal Identity Verification. [SP800-78].

7. CERTIFICATE, CRL, AND OCSP PROFILES

Information for interpreting the following Certificate Profiles and CRL Profiles may be found in IETF's RFC 2459 (http://www.ietf.org/rfc/rfc2459.txt). DigiCert uses the ITU X.509, version 3 standard to construct digital certificates for use within the DigiCert PKI. DigiCert adds certain certificate extensions to the basic certificate structure for the purposes intended by X.509v3 as per Amendment 1 to ISO/IEC 9594-8, 1995. For PIV-I Certificates, DigiCert follows the FPKIPA's X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards. For Qualified Certificates, DigiCert follows ETSI TS 101 862.

7.1. CERTIFICATE PROFILE

7.1.1. Version Number(s)

All certificates are X.509 version 3 certificates.

7.1.2. Certificate Extensions

See DigiCert's Certificate Profiles document.

PIV-I Certificates comply with the X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards, Date: April 23 2010, as set forth at: http://www.idmanagement.gov/fpkipa/documents/pivi_certificate_crl_profile.pdf.

7.1.3. Algorithm Object Identifiers

DigiCert certificates are signed using one of the following algorithms:

sha-1WithRSAEncryption	[iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5]
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]

DigiCert does not currently sign certificates using RSA with PSS padding.

DigiCert and Subscribers may generate Key Pairs using the following:

id-dsa	[iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1]
RsaEncryption	[iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1]
Dhpublicnumber	[iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1]
id-keyExchangeAlgorithm	[joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) algorithms(1) 22]
id-ecPublicKey	[iso(1) member-body(2) us(840) ansi-X9-62(10045) id-publicKeyType(2) 1]

If DigiCert issues a non-CA certificate for an elliptic curve public key, DigiCert specifies one of the following named curves:

ansip192r1	[iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 1]
ansit163k1	[iso(1) identified-organization(3) certicom(132) curve(0) 1]
ansit163r2	[iso(1) identified-organization(3) certicom(132) curve(0) 15]
ansip224r1	[iso(1) identified-organization(3) certicom(132) curve(0) 33]
ansit233k1	[iso(1) identified-organization(3) certicom(132) curve(0) 26]

ansit233r1	[iso(1) identified-organization(3) certicom(132) curve(0) 27]
ansip256r1	[iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 7]
ansit283k1	[iso(1) identified-organization(3) certicom(132) curve(0) 16]
ansit283r1	[iso(1) identified-organization(3) certicom(132) curve(0) 17]
ansip384r1	[iso(1) identified-organization(3) certicom(132) curve(0) 34]
ansit409k1	[iso(1) identified-organization(3) certicom(132) curve(0) 36]
ansit409r1	[iso(1) identified-organization(3) certicom(132) curve(0) 37]
ansip521r1	[iso(1) identified-organization(3) certicom(132) curve(0) 35]
ansit571k1	[iso(1) identified-organization(3) certicom(132) curve(0) 38]
ansit571r1	[iso(1) identified-organization(3) certicom(132) curve(0) 39]

Signature algorithms for PIV-I certificates are limited to those identified by NIST SP 800-78.

7.1.4. Name Forms

Each certificate includes a unique serial number that is never reused. Optional subfields in the subject of an EV Certificate must either contain information verified by DigiCert or be left empty. EV Certificates cannot contain metadata such as '.', '-' and ' ' characters or any other indication that the field is not applicable.

The Distinguished Name in a Certificate may contain the following information:

1) Organization Name – Required in SSL Certificates
2) Domain Name - Required in SSL Certificates
3) Business Category – Required for EV Certificates
4) Organizational Unit – Optional
5) Jurisdiction of Incorporation or Registration – Required in EV Certificates (as applicable)
6) Registration Number - Required in EV Certificates
7) Physical Address of Place of Business Number – Optional for street and postal code
8) E-mail address (E) - Required for email certificates

The contents of the fields in EV Certificates must meet the requirements in Section 8.1 of the EV Guidelines.

7.1.5. Name Constraints

No stipulation.

7.1.6. Certificate Policy Object Identifier

An object identifier (OID) is a unique number that identifies an object or policy. The OIDs used by DigiCert are listed in Section 1.2 and in DigiCert's Certificate Profiles document.

7.1.7. Usage of Policy Constraints Extension

Not applicable.

7.1.8. Policy Qualifiers Syntax and Semantics

DigiCert includes brief statements in certificates about the limitations of liability and other terms associated with the use of a certificate in the Policy Qualifier field of the Certificates policy extension.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2. CRL PROFILE

For PIV-I Certificates, DigiCert follows the FPKIPA's X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards.

7.2.1. Version number(s)

DigiCert issues version 2 CRLs that conform to RFC 3280. CRLs 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-sha284 [1 2 840 10045 4 3]
Issuer Distinguished Name	DigiCert
thisUpdate	CRL issue date in UTC format
nextUpdate	Date when the next CRL will issue in UTC format. The field is set to thisUpdate plus 24 hours
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	Optionally included reason for the revocation

7.3. OCSP PROFILE

For PIV-I Certificates, DigiCert follows the FPKIPA's X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards.

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

The practices in this CPS are designed to meet or exceed the requirements of generally accepted industry standards, including the latest version of the EV Guidelines and the AICPA/CICA WebTrust Program for Certification Authorities, ANS X9.79/ISO 21188 PKI Practices and Policy Framework ("CA WebTrust/ISO 21188"). For purposes of interoperation with the U.S. Government, DigiCert submits an auditor letter of compliance meeting the FPKIPA's Compliance Audit Requirements, dated October 28, 2009 (FPKIPA Audit Requirements).

8.1. FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

DigiCert has an annual audit by an independent external auditor to assess DigiCert's compliance with this CPS, any applicable CPs, and the CA WebTrust/ISO 21188 and WebTrust EV Program criteria. The audit covers DigiCert's RA systems, Sub CAs, and OCSP Responders.

8.2. IDENTITY/QUALIFICATIONS OF ASSESSOR

Auditors must meet the requirements of Section 14.1.14 of the EV Guidelines. Specifically:

(1) *Qualifications and experience*: Auditing must be the auditor's primary business function. The individual or at least one member of the audit group must be qualified as a Certified Information Systems Auditor (CISA), an AICPA Certified Information Technology Professional (CPA.CITP), a Certified Internal Auditor (CIA), or have another recognized

information security auditing credential. Auditors must be subject to disciplinary action by its licensing body.

(2) *Expertise*: The individual or group must be trained and skilled in the auditing of secure information systems and be familiar with Public Key infrastructures, certification systems, and Internet security issues.

(3) *Rules and standards*: The auditor must conform to applicable standards, rules, and best practices promulgated by the American Institute of Certified Public Accountants (AICPA), the Canadian Institute of Chartered Accountants (CICA), the Institute of Chartered Accountants of England & Wales (ICAEW), the International Accounting Standards adopted by the European Commission (IAS), Information Systems Audit and Control Association (ISACA), the Institute of Internal Auditors (IIA), or another qualified auditing standards body.

(4) *Reputation*: The firm must have a reputation for conducting its auditing business competently and correctly.

(5) *Insurance*: EV auditors must maintain Professional Liability/Errors and Omissions Insurance, with policy limits of at least $1 million in coverage.

8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

DigiCert uses an independent auditor that does not have a financial interest, business relationship, or course of dealing that could foreseeably create a significant bias for or against DigiCert.

8.4. TOPICS COVERED BY ASSESSMENT

The audit conforms to the FPKIPA Audit Requirements and the annual CA WebTrust/ISO 21188 and WebTrust EV Program audit programs, and covers DigiCert's business practices disclosure, the integrity of DigiCert's PKI operations, and DigiCert's compliance with the EV Guidelines.

8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY

If an audit reports any material noncompliance with applicable law, this CPS, the CP, 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

DigiCert performs self-audits and RA audits on EV Certificates in accordance with section 14.1.2, of the EV Guidelines.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. FEES

9.1.1. Certificate Issuance or Renewal Fees

DigiCert charges the fees posted on its website for certificate issuance and renewal. DigiCert may change its fees at any time. Notice of a fee change is given by posting the updated fees on DigiCert's website.

9.1.2. Certificate Access Fees
DigiCert may charge a reasonable fee for access to its database of certificates.

9.1.3. Revocation or Status Information Access Fees
DigiCert does not charge a fee for revoking a certificate or for checking the validity status of an issued certificate using a CRL. DigiCert may establish and charge a reasonable fee for providing certificate status information services via OCSP.

9.1.4. Fees for Other Services
No stipulation.

9.1.5. Refund Policy
DigiCert offers a limited 30-day refund on issued certificates. Subscribers must request refunds in writing, within 30 days after the certificate issues. After receiving the refund request, DigiCert will revoke the certificate and refund the amount paid by the Applicant, minus any applicable application processing fees.

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. DigiCert's insurance policies include coverage for (1) claims for damages arising out of an act, error, or omission, unintentional breach of contract, or neglect in issuing or maintaining EV Certificates, and (2) claims for damages arising out of infringement of the proprietary rights of any third party (excluding copyright, and trademark infringement), invasion of privacy, and advertising injury. Insurance is carried through companies rated no less than A- as to Policy Holder's Rating in the current edition of Best's Insurance Guide (or with an association of companies each of the members of which are so rated).

9.2.2. Other Assets
No stipulation.

9.2.3. Insurance or Warranty Coverage for End-Entities
DigiCert's insurance coverage for end-entities is specified in DigiCert's Subscriber Agreements and Relying Party Agreements.

9.3. CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1. Scope of Confidential Information
The following information is considered confidential information and protected against disclosure using a reasonable degree of care:

1. Private Keys;
2. Activation data used to access Private Keys or to gain access to the CA system;
3. Business continuity, incident response, contingency, and disaster recovery plans;
4. Other security practices used to protect the confidentiality, integrity, or availability of information;
5. Information held by DigiCert as private information in accordance with Section 9.4;
6. Audit logs and archive records, including certificate application records and documentation submitted in support of certificate applications whether successful or rejected; and
7. Transaction records, financial audit records, and external or internal audit trail records and any audit reports (with the exception of an auditor's letter confirming the effectiveness of the controls set forth in this CPS)

9.3.2. Information Not Within the Scope of Confidential Information

Any information not listed as confidential information is considered public information. Published certificate and revocation data is 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 required by law or when requested by the subject of 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 shall protect private information in its possession using a reasonable degree of care and appropriate safeguards.

9.4.3. Information Not Deemed Private

Certificates, CRLs, and the personal or corporate information appearing in them are not considered private information.

9.4.4. Responsibility to Protect Private Information

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

9.4.5. Notice and Consent to Use Private Information

Personal data provided during the application, registration, and identity verification process that is not contained in Certificates is considered private information. DigiCert may only use private information with the subject's express written consent or as required by applicable law or regulation. Notwithstanding the foregoing, personal information contained in Certificates may be published in online public repositories. All Subscribers consent to the global transfer of any personal data contained in Certificates.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

DigiCert may disclose private information, without notice, when required to do so by law or regulation.

9.4.7. Other Information Disclosure Circumstances

No stipulation.

9.5. INTELLECTUAL PROPERTY RIGHTS

DigiCert, or its business partners, own all 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.

Certificates and revocation information are the exclusive property of DigiCert. DigiCert grants permission to reproduce and distribute certificates on a non-exclusive, 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 will 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:

1. DigiCert complies, in all material aspects, with the CP, this CPS, DigiCert's internal and published policies and procedures, and all applicable laws and regulations,
2. DigiCert publishes and updates CRLs and OCSP responses on a regular basis,
3. All certificates issued under this CPS will be verified in accordance with this CPS and meet the minimum requirements found herein,
4. DigiCert will maintain a repository of public information on its website,
5. The certificate applicant held the Private Key when the certificate issued, and
6. Information published on a qualified certificate meets the requirements specified in EU Directive 99/93.

To the extent allowed under EU Directive 99/93, DigiCert:

1. Does not warrant the accuracy, authenticity, completeness, or fitness of any unverified information, including name verification for (1) certificates intended for email and intranet use, (2) Unified Communications Certificates, and (3) other certificates issued to individuals and intranets.
2. Is not responsible for information contained in a certificate except as stated in this CPS,
3. Does not warrant the quality, functions or performance of any software or hardware device, and
4. Is not responsible for failing to comply with this CPS because of circumstances outside of DigiCert's control.

For EV Certificates, DigiCert represents to Subscribers, Subjects, Application Software Vendors that distribute DigiCert's root certificates, and Relying Parties that use a DigiCert certificate while the certificate is valid that DigiCert followed the EV Guidelines when verifying information and issuing EV Certificates. This representation is limited solely to DigiCert's compliance with the EV Guidelines (e.g., DigiCert may rely on erroneous information provided in an attorney's opinion or accountant's letter that is checked in accordance with the Guidelines).

For PIV, DigiCert maintains an agreement with Affiliated Organizations that includes obligations related to authorizing affiliation with Subscribers of PIV-I certificates.

9.6.2. RA Representations and Warranties

RAs represent that:

1. The RA's certificate issuance and management services conform to the DigiCert CP and 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 Subscriber's Private Key, regardless of whether such use was authorized.

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,
7. Abide by the Subscriber Agreement and this CPS when requesting or using a Certificate, and
8. Promptly cease using the certificate and related Private Key after the certificate's expiration.

In addition, organizations that apply for a CDS certificate for an individual Subscriber are required to (i) implement processes that prevent anyone from using the associated Private Key without the knowledge and explicit action of the Subscriber and (ii) maintain information that permits a determination of who signed a particular document. Organizations that apply for a CDS certificate on behalf of the organization are required to (i) maintain processes that assure that Private Keys can be used only with the knowledge and explicit action of one human being within the organization, (ii) maintain information that permits a determination of who signed a particular document, and (iii) prevent sharing of organizational certificates amongst members of the organization.

9.6.4. Relying Party Representations and Warranties

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

1. Made reasonable efforts to acquire sufficient knowledge on using digital certificates and PKI,
2. Studied the limitations on the usage of certificates and is aware of DigiCert's limitations on liability with respect to reliance on issued certificates,
3. Has read, understands, and agrees to the DigiCert Relying Party Agreement and this CPS,
4. Verified both the DigiCert certificate and any 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 of relying on a digital signature created by an invalid, revoked, or expired certificate, including only relying on a DigiCert certificate if appropriate 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.

CDS Relying Parties have the obligations set forth in the Acrobat End User License Agreement. Reliance on a CDS-signed document is only permitted if verified on a supported platform as specified on Adobe's website.

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 ARE PROVIDED "AS IS" AND "AS AVAILABLE". TO THE MAXIMUM EXTENT PERMITTED BY LAW, DIGICERT DISCLAIMS ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. DIGICERT DOES NOT WARRANT THAT ANY 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

EXCEPT FOR LIABILITY RELATED TO FRAUD, FRAUDULENT STATEMENTS, OR DEATH OR PERSONAL INJURY RESULTING FROM DIGICERT'S NEGLIGENCE, DIGICERT'S MAXIMUM LIABLITY RESULTING FROM CERTIFICATES AND SERVICES PROVIDED UNDER THIS CPS IS LIMITED AS FOLLOWS:

1. NO LIABILTY IF THE CERTIFICATE OR SERVICE IS PROVIDED IN ACCORDANCE WITH THIS CPS,
2. AN AGGREGATE OF $2,000 PER SSL CERTIFICATE USED TO CONDUCT TRANSACTIONS VALUED AT LESS THAN $1 MILLION AND WHERE THE CERTIFICATE IS NOT ISSUED IN COMPLIANCE WITH THIS CPS,
3. AN AGGREGATE OF $2,000 PER CODE SIGNING CERTIFICATE WHERE THE CERTIFICATE WAS NOT ISSUED IN COMPLIANCE WITH THIS CPS,
4. AN AGGREGATE OF $5,000 FOR ALL CDS CERTIFICATES THAT WERE NOT ISSUED IN COMPLIANCE WITH THIS CPS,
5. NO LIABILITY FOR ANY OTHER CERTIFICATE TYPES, AND
6. AN AGGREGATE LIABILITY OF $1 MILLION FOR ALL CLAIMS, REGARDLESS OF THE NUMBER OR SOURCE OF THE CLAIMS.

THE LIMITATIONS OF LIABILITY IN THIS SECTION APPLY ON A CERTIFICATE-BY-CERTIFICATE BASIS, REGARDLESS OF THE NUMBER OF TRANSACTIONS OR CLAIMS RELATED TO EACH CERTIFICATE AND ARE APPORTIONED TO THE FIRST CLAIMS THAT ACHIEVE FINAL RESOLUTION.

All liability is limited solely 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, or (iv) whether any other provisions of this Agreement were breached or 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

DigiCert shall indemnify each Application Software Vendor against any claims, damages, and losses suffered by the Application Software Vendor related to an EV Certificate issued by DigiCert, regardless of the cause of action or legal theory involved, except where the claim, damages, or loss suffered by the Application Software Vendor was directly caused by the Application Software Vendor's software displaying either (1) a valid and trustworthy EV Certificate as not valid or trustworthy or (2) displaying as trustworthy (i) an EV Certificate that has expired, or (ii) a revoked EV Certificate where the revocation status is available online but the Application Software Vendor's software failed to check or ignored the status.

9.9.2. Indemnification by Subscribers

To the extent permitted by law, each 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 (i) a misrepresentation or omission of material fact by Subscriber, regardless of whether the misrepresentation or omission was intentional; (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 negligence of Subscriber; 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) reliance on a certificate that is unreasonable under the circumstances; or (iii) failure to check the status of the certificate prior to use.

9.10. TERM AND TERMINATION

9.10.1. Term

This CPS and any amendments are effective when published to DigiCert's online repository 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 the DigiCert Repository. The communication will specify which provisions survive termination. At a minimum, responsibilities related to protecting confidential information will survive termination. Subscriber Agreements remain effective until the end of the certificate's validity, even if this CPS terminates.

9.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

DigiCert accepts digitally signed or paper notices related to this CPS that are addressed to the locations specified in Section 2.2 of this CPS. 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 its Subscriber Agreements.

9.12. AMENDMENTS

9.12.1. Procedure for Amendment

The DCPA determines what amendments should be made to this CPS. Amendments are made by posting an updated version of the CPS to the online repository. Controls are in place to reasonably ensure that this CPS is not amended and published without the prior authorization of the DCPA. This CPS is reviewed at least annually.

9.12.2. Notification Mechanism and Period

DigiCert will post notice on its website of any proposed significant revisions to this CPS. The notice will include a final date for receipt of comments and the proposed effective date. DigiCert does not have a fixed notice and comment period. DigiCert may make editorial and typographical corrections, changes to contact details, and other changes that do not materially impact the parties without notice and without changing the version of this CPS.

9.12.1. Circumstances under which OID Must Be Changed

If the DCPA determines an amendment necessitates a change in an OID, then the revised version of this CPS will also contain a revised OID. Otherwise, amendments do not require an OID change.

9.13. DISPUTE RESOLUTION PROVISIONS

Before resorting to any dispute resolution mechanism, including adjudication or any type of alternative dispute resolution, a party must notify DigiCert of the dispute with a view to seek dispute resolution.

9.14. GOVERNING LAW

For disputes involving Qualified Certificates, the national law of the relevant Member State shall govern. The laws of the state of Utah govern the interpretation, construction, and enforcement of this CPS and all proceedings that are 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. Subject to section 9.4.5's Notice and Consent to Use Private Information contained in Certificates, DigiCert meets the requirements of the European data protection directive 95/46/EC and has established appropriate technical and organization measures against unauthorized or unlawful processing of personal data against the loss, damage, or destruction of personal data.

9.16. MISCELLANEOUS PROVISIONS

9.16.1. Entire Agreement

DigiCert contractually obligates every RA involved in certificate issuance to comply with this CPS and applicable industry guidelines. DigiCert also requires parties using its products and services, such as Subscribers and Relying Parties, to enter into agreements. These agreements may have provisions that differ from this CPS. In each case, the agreement with that party controls, but solely with respect to that party. No third party may rely on or bring action to enforce any such agreement.

9.16.2. Assignment
Entities operating under this CPS may not assign their obligations without the prior written consent of DigiCert.

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 is an exclusion of damages is intended to be 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 any 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 a 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.

APPENDIX A: DOMAIN AUTHORIZATION LETTER

Dear DigiCert,

_____ ("Certificate Applicant") recently submitted a request to DigiCert for one or more digital certificates under Certificate Applicant's name. Certificate Applicant wishes to install the digital certificates on server(s) for the domain(s) listed below:

I am the registrant or employed by the registrant ("Registrant") of the domain name(s) referenced above and am duly authorized to (i) sign this Domain Authorization Letter and (ii) to deal with all matters related to the registration of the domain. On behalf of Registrant, I confirm that Registrant has granted and/or acknowledges that Certificate Applicant has the right to use the domain(s) referenced above in connection with its business and as common name(s) in digital certificate(s) to be issued by DigiCert. Registrant authorizes the Certificate Applicant to request digital certificates for any subdomain on the domain(s) listed above.

DigiCert may rely on this authorization for any subsequent digital certificate renewals and/or additional digital certificates obtained by the Certificate Applicant until such time as this authorization is revoked. To revoke the rights herein appointed, I acknowledge that I must contact DigiCert, Inc. by written notification using one of the following methods: 1) Email to admin@digicert.com or 2) Mail to DigiCert, Inc. (Attention: Legal) - 355 South 520 West - Canopy Building II, Suite 200 - Lindon, Utah 84042.

Registrant agrees that it will indemnify DigiCert and its officers, directors and agents for any losses, costs, damages, and attorneys' fees that arise out of Registrant's breach of the representations made in (a) this letter, (b) any domain name registration agreement between Registrant and the Registry governing the Domain name registration, or (c) any assignment or other transfer of the domain name to a third party. Registrant agrees to defend, at its expense and after receiving appropriate notice, any claim that gives rise to an indemnification obligation of Registrant.

Regards,

Full Name: _____

Signature:_____

Job Title: _____

[** This document should be faxed to 1-801-705-0481]

APPENDIX B: SAMPLE LEGAL OPINION

[*Law Firm Letterhead*]
[*Date*]

To: DigiCert, Inc.
355 South 520 West
Canopy Building II, Suite 200
Lindon, Utah 84042

Re: EV Certificate Request No. *[Certificate request number]*
Client: *[Exact company name of client – see footnote 1]*
Client Representative: *[Exact name of the client's representative who signed the certificate application – see footnote 2]*
Application Date: *[Insert date of client's certificate application]*

This firm represents *[exact company name of client – see footnote 1]* ("Client"), who submitted an application for an EV Certificate to you. The Client asked that we, as [*lawyers*, *solicitors*, *barristers*, *advocates*, *or equivalent*] licensed to practice law in [*Country of the Client's Jurisdiction of Incorporation or Registration or any jurisdiction where the Client maintains an office or physical facility*], provide an opinion letter on certain aspects of the Client's legal and operational existence.

[Insert customary preliminary matters for opinion letters in your jurisdiction.]

Based on our stated familiarity with the relevant facts and our professional judgment and expertise, our opinion is that:

1. Client is a duly formed [*corporation, LLC, etc.*] under the laws of the [*state/province*] of [*name of governing jurisdiction where Client is incorporated or registered*]; is "active," "valid," "current," or the equivalent; and is not under any known legal disability.

2. [*If applicable*] The Romanized transliteration of Client's formal legal name is: [*Romanized name]*.

3. [*If applicable*] Client conducts business under the [*assumed/DBA/trade*] name of *[assumed name of Client].* Client has a currently valid registration of the name with the government agency that has jurisdiction over the place of business listed below.

4. The address where [*Client, Client's parent, or Client's subsidiary – select one*] conducts business operations is:
[Insert place of business – this should match the address on the certificate application]

5. A main telephone number at Client's place of business is:
[Insert primary telephone number of business]

6. *[Name of Client's Representative – see footnote 2]* is an individual with the authority to act on behalf of Client to:
[select as appropriate]
   a) Provide the information about the Client contained in the referenced application,
   b) Request one or more EV Certificates and designate other persons to request EV Certificates, and
   c) Agree to the contractual obligations contained in [*Name of CA*]'s Subscriber Agreements.

7. Client has either operated as a business for three or more years or has an active deposit account held at a bank or other financial institution where funds deposited are payable on demand.

8. Client has the exclusive right to use the following domain name(s) in identifying itself on the Internet and is aware that it has such control:
   [Insert domain names]

[Insert customary limitations and disclaimers for opinion letters in your jurisdiction.

[Name and signature]
*[Jurisdiction(s) in which attorney / Latin notary is admitted to practice]**3***

cc: *[Send copy to Client]*

Note 1: This must be the Client's exact corporate name as registered with the relevant Incorporating Agency in the Client's Jurisdiction of Incorporation.
Note 2: A Power of Attorney from an officer of the Client who has the power to delegate authority is sufficient to establish the Client Representative's actual authority. Multiple representatives may be listed.
Note 3: In-house counsel of the Client may submit this letter if permitted by the rules of your jurisdiction.
Note 4: This letter may be submitted by mail, fax, or email.

APPENDIX C: SAMPLE ACCOUNTANT LETTER

This is a sample letter only and is subject to change. This letter has not been approved or endorsed by any professional accounting organization.

To: DigiCert, Inc. and Management of [*Client*]:

As specifically agreed to with the Management of [*Client*], we/I have performed the following procedures in connection with the company's application for an Extended Validation (EV) Certificate, dated....., 20..... No representations are made regarding the sufficiency of these procedures.

Specified Information:	**Procedure:** ***(Note 1: These are illustrative of the procedures that would be undertaken and are designed to meet the needs of the Certification Authorities issuing Extended Validation Certificates)***	**Results:** ***(Note 2: If you are unavailable to perform any of the stated procedure, this should be noted in this column. Any exceptions should be noted in a separate paragraph below)***
Legal Name – [*Legal name of Client*]	Agree legal name to permanent audit file information *(If audit has been completed)*	Legal name on the application agrees with the information contained in our/my permanent files *(If there is no permanent file, state this fact)*
[*If applicable*] The Romanized translation of Client's formal legal name - [*Romanized name]*.	Agree Romanization to legal name and accepted transliteration methods	Checked Romanization of name with legal name and accepted transliteration methods
[*If applicable*] Doing business as – [*Name*]	Agree name to government agency registration database and check whether registration of the name is still valid	[*Name*] is registered with [*database used to agree name*] and continues to be valid
Physical location – [*Address*]	Visit the location at the specified address and confirm that operations are conducted there	Site visit completed at [*Address*] and operations appeared to be conducted
Business Phone Number – [*Main telephone number of Client*]	Phone the number provided and confirm that it was answered by the named organization	Phoned [*Telephone number*] and noted that it was answered by [*Name of organization*] as provided by the receptionist
Bank Account – [*Bank Name and account number*]	Request a letter directly from [*Bank name*] confirming the existence of the account for the benefit of [*Client Name*]	Received letter directly from [*Bank Name*] confirming the existence of the account for the benefit of [*Client Name*]
The corporate officers are [*Name of verified officers*]	Agree names to annual shareholders meeting minutes *(Note - not required to personally know the officers)*	Agreed [*Names*] listed as corporate officers on the application to minute books maintained by the Client
Name of application signer and approver	Obtain letter from verified officer confirming the names of the application signer and approver	Obtained letter from [*Name and title*] confirming the names of the duly authorized names of the application signer and approver as they appear in the application

Domain names [*List domain names*]	Verify that Client hosts the domain names on servers under its control or that Client has a contractual relationship with a hosting company or the registered domain owner that provides Client exclusive control.	Verified that Client hosts the domain names on servers under its control Verified that Client has a contractual relationship providing Client exclusive control

We/I did not examine and do not express any opinion on the application for the Extended Validation Certificate. Additional procedures may have brought additional items to our/my attention.

This report is intended solely for the information and use of DigiCert, Inc. and management of [*Client*]. This report should not be used by anyone other than these specified parties.

[Signature]
[Date]