DigiCert

Certification Practice Statement for Extended Validation Certificates

DigiCert, Inc.
Version 1.0.1
February 21, 2007

333 South 520 West
Lindon, UT 84042
USA
Tel: 1-801-805-1620
Fax: 1-801-705-0481
www.digicert.com

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Overview

This document is the DigiCert, Inc. (hereafter referred to as “DigiCert” where applicable) Certification Practice Statement (CPS) for Extended Validation Certificates and serves as a statement of the practices that DigiCert employs in providing certification services that meet the "Guidelines for Extended Validation Certificates," version 1.0 (draft 11) (the "Guidelines") of the Certification Authority / Browser Forum ("CA/Browser Forum"). This CPS constitutes DigiCert's Statement of "EV Policies" as that term is used in the Guidelines. DigiCert conforms to the current version of the CA/Browser Forum Guidelines published at http://www.cabforum.org. In the event of any inconsistency between this document and those Guidelines, those Guidelines take precedence over this document.

Extended Validation ("EV") Certificates are intended to provide enhanced assurance of the identity of the legal entity that controls a website, including the entity's name, address of Place of Business, Jurisdiction of Incorporation, and Registration Number. EV Certificates are also intended to help establish the legitimacy of a business claiming to operate a website by confirming its legal and physical existence, and to provide a vehicle that can be used to assist in addressing problems related to phishing and other forms of online identity fraud. By providing more reliable third-party verified identity and address information regarding the owner of a website, EV Certificates may help to:

- Make it more difficult to mount phishing and other online identity fraud attacks using SSL certificates; and
- Assist companies that may be the target of phishing attacks or online identity fraud by providing them with a tool to better identify themselves and their legitimate websites to users.

EV Certificates do not, however, provide any guarantee that the Subject named in the Certificate is trustworthy, honest, reputable in its business dealings, or safe to do business with. EV Certificates only establish that DigiCert verified that the business was legally organized and had the physical address as of the date that the Certificate was issued.

This CPS also defines the underlying certification processes for Subscribers of EV Certificates and describes DigiCert’s Certification Authority (CA) and certificate repository operations. It is also a public statement of the practices of DigiCert, Inc. and serves to notify Subscribers and Relying Parties of their roles and responsibilities concerning Extended Validation ("EV") Certificates. Pursuant to the IETF PKIX RFC 3647 CPS framework, this CPS is divided into nine (9) parts that cover practices and procedures for identifying certificate applicants, issuing and revoking certificates, and the security controls related to managing the physical, personnel, technical and operational components of the CA infrastructure. To preserve the outline specified by RFC 3647, some section headings that do not apply will have the statement "Not applicable" or "No Stipulation."

EV Certificates are issued for use with the SSL 3.0/TLS 1.0 protocol to enable secure transactions of data through privacy, authentication, and data integrity. EV Certificates are valid for one (1) year.

To obtain an EV Certificate, the applicant submits an application via a secure on-line link according to the procedures described herein. Applicants are required to submit a PKCS#10 Certificate Signing Request (PKCS#10 CSR) containing the applicant's identifying information and geographic location and a public key signed with the applicant's corresponding private key. Additional documentation in support of the application may be required so that DigiCert may verify the identity of the applicant. Applicants are required to submit sufficient identifying information to DigiCert prior to receiving certificate approval. Upon verification of identity, DigiCert issues the certificate and sends a notice to the applicant. The applicant downloads and installs the certificate to a network device to be used for authentication and encryption. The applicant must notify DigiCert of any inaccuracy or defect in a certificate promptly after receipt of the EV Certificate or earlier notice of informational content to be included in the EV Certificate. After certificate issuance, if the Subscriber ever suspects that the security of the device containing the private key may have been compromised, he or she must immediately contact DigiCert and request revocation of the EV Certificate. Revoked certificates are published on a Certificate Revocation List (CRL).

1.2 Document name and identification

This document is DigiCert's CPS for Extended Validation Certificates, version 1.0, which was originally adopted and approved for publication on 20 November 2006 by DigiCert senior management, acting as the DigiCert Policy Authority (DCPA). Revisions of this document have been made as follows:

Date	Changes	Version
11-20-2006	New Version	1.0
2-21-2007	Modified section 9.1.5 refund policy and section 9.6 warranty statement.	1.0.1

As detailed in this CPS, DigiCert's EV certificate type is identified by the following object identifier under DigiCert's ANSI-issued arc of joint-iso-ccitt (2) country (16) USA (840) US-company (1) DigiCert (114412) EV (2) ver.1 (1) (i.e., 2.16.840.1.114412.2.1), which DigiCert uses to identify this CPS and EV Certificates issued pursuant hereto.

1.3 PKI participants

1.3.1 Certification authority

DigiCert is a Certification Authority (CA) that issues EV Certificates to entities including private and public companies in accordance with this CPS. In its role as a CA, DigiCert performs functions associated with public key operations that include receiving requests, issuing, revoking and renewing an EV Certificate and the maintenance, issuance and publication of CRLs for users within the DigiCert PKI. In delivering its PKI services DigiCert complies in all material respects with high-level international standards including those on Qualified Certificates pursuant to the European Directive 99/93 and the relevant law on electronic signatures and all other relevant legislation and regulation.

In its role as a CA, DigiCert provides certificate services within the DigiCert PKI and will:

- Conform its operations to this CPS (or other CA business practices disclosures), as the same may from time to time be modified by amendments published in the DigiCert repository (www.digicert.com/ssl-cps-repository.htm);
- Issue and publish certificates in a timely manner in accordance with the issuance periods set out in this CPS;
- Upon receipt of a valid request to revoke the certificate from a person authorized to request revocation using the revocation methods detailed in this CPS, revoke a certificate issued for use within the DigiCert PKI;
- Publish and update CRLs on a regular basis and in a timely manner, in accordance with the provisions described in this CPS;
- Distribute issued certificates in accordance with the methods detailed in this CPS; and
- Notify subscribers via email of the imminent expiry of their DigiCert issued certificate beginning 60 days prior to expiration.

1.3.2 Registration authority

Not applicable.

1.3.3 Subscribers

Subscribers of DigiCert services are companies or organizations that use PKI in relation with DigiCert supported transactions and communications. Subscribers are parties that are identified in an EV Certificate and hold the private key corresponding to the public key that is listed in the EV Certificate. Prior to verification of identity and issuance of a certificate, a Subscriber is an *applicant* for the services of DigiCert.

(a) General. Only the following Private Organizations and Government Entities satisfying the requirements specified below may be Subscribers:

(b) Private Organization Subjects. DigiCert may issue EV Certificates to Private Organizations that satisfy the following requirements:

(1) The Private Organization MUST be a legally recognized entity whose existence was created by a filing with (or an act of) the Incorporating Agency in its Jurisdiction of

Incorporation (e.g., by issuance of a certificate of incorporation);

(2) The Private Organization MUST have designated with the Incorporating Agency a Registered Agent, Registered Office (as required under the laws of the Jurisdiction of Incorporation) or equivalent;

(3) The Private Organization MUST NOT be designated on the records of the Incorporating Agency by labels such as “inactive,” “invalid,” “not current,” or the equivalent;

(4) The Private Organization’s Jurisdiction of Incorporation and/or its Place of Business MUST NOT be in any country where DigiCert is prohibited from doing business or issuing a certificate by the laws of the United States; and

(5) The Private Organization MUST NOT be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the United States.

(c) Government Entity Subjects. The CA may issue EV Certificates to Government Entities that satisfy the following requirements:

(1) The legal existence of the Government Entity MUST be established by the law of the Jurisdiction of Incorporation;

(2) The Government Entity MUST NOT be in any country where DigiCert is prohibited from doing business or issuing a certificate by the laws of the United States; and

(3) The Government Entity MUST NOT be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the United States.

(d) Excluded Subjects. Until additional criteria for validation are defined by the Guidelines, DigiCert does not issue EV Certificates to any person or any organization or entity that does not satisfy the requirements above, including but not limited to the following:

(1) General partnerships

(2) Unincorporated associations

(3) Sole proprietorships

(4) Individuals (natural persons)

Validation criteria for these organizations or entities will be addressed in the next major revision of the Guidelines, at which time DigiCert may issue EV Certificates to such entities in accordance with such revisions.

1.3.4 Relying parties

Relying parties use PKI services in relation with DigiCert-issued EV Certificates and reasonably rely on such certificates and/or digital signatures verifiable with reference to a public key listed in the certificate.

To verify the validity of an EV Certificate they receive, relying parties must refer to the CRL prior to relying on information featured in a certificate to ensure that DigiCert has not revoked the certificate. The location of the CRL distribution point is detailed within the EV Certificate.

1.4 Certificate usage

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 EV Certificate. Typically, the following bits are enabled for EV Certificates: keyEncipherment, dataEncipherment, serverAuthentication and clientAuthentication.

1.4.2 Prohibited certificate uses

Certificates issued under the provisions of this CPS may not be used for: (i) 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) transactions where applicable law prohibits the use of encryption or digital certificates for such transactions or where otherwise prohibited by law.

1.5 Policy administration

1.5.1 Organization administering the document

This CPS and related agreements and security policy documents referenced within this document are maintained by the DigiCert Policy Authority (DCPA). The DCPA may be contacted at:

DigiCert, Inc.
333 South 520 West
Lindon, UT 84042 USA
Tel: 1-801-805-1620
Fax: 1-801-705-0481

1.5.2 Contact person

Attn: Legal Counsel
DigiCert, Inc.
333 South 520 West
Lindon, UT 84042 USA

1.5.3 Person determining CPS suitability for the policy

Attn: DigiCert Policy Authority
333 South 520 West
Lindon, UT 84042 USA

1.5.4 CPS approval procedures

Approval of this CPS and any amendments hereto is by the DCPA. Amendments may be made by updating this entire document or by addendum. The DCPA determines whether changes to this CPS require notice or any change in the OID of a certificate issued pursuant to this CPS. *See also* Section 9.10 and Section 9.12 below.

1.6 Definitions and acronyms

Applicant: The Applicant is an entity applying for a Certificate.

Certificate Approver: A Certificate Approver is a natural person who is employed by the Applicant, or an authorized agent who has express authority to represent the Applicant to: (i) act as a Certificate Requester and to authorize other employees or third parties to act as a Certificate Requesters, and (ii) to approve EV Certificate Requests submitted by other Certificate Requesters.

Certificate Request Form: Any of several forms completed by Applicant or DigiCert and used to process the request for an EV Certificate, including but not limited to agreements signed by Contract Signers and online forms submitted by Certificate Requesters.

Certificate Requester: A Certificate Requester is a natural person who is employed by the Applicant, or an authorized agent who has express authority to represent the Applicant or a third party (such as an ISP or hosting company) that completes and submits an EV Certificate Request on behalf of the Applicant.

Contract Signer: A Contract Signer is a natural person who is employed by the Applicant, or an authorized agent who has express authority to represent the Applicant who has authority on behalf of the Applicant to sign Subscriber Agreements on behalf of the Applicant.

Qualified Government Information Source: A regularly-updated and current online publicly available database maintained by a Government Entity and designed for the purpose of accurately providing information concerning Applicants and Subscribers, and which is generally recognized as a dependable source of such information. To be a qualified source, as that term is used in this CPS, the source must be maintained by a Government Entity, the reporting of data must be required by law, and false or misleading reporting must be punishable with criminal or civil penalties.

Qualified Independent Information Source: A publicly available commercial database that provides a dependable and independent source of information concerning Applicants and Subscribers. To be a qualified source, as that term is used in this CPS, the following must all be true:

(1) data that will be relied upon has been independently verified by other independent information sources;
(2) the database distinguishes between self-reported data and data reported by independent information sources;
(3) the database provider identifies how frequently they update the information in their database;
(4) changes in the data that will be relied upon will be reflected in the database in no more than 12 months; and
(5) the database provider uses authoritative sources independent of the subject or multiple corroborated sources to which the data pertains.

Registrar: The applicable domain name registrar for the Applicant. *See* http://www.icann.org.

Relying Party: The Relying Party is an individual or entity that relies upon the information contained within the Certificate.

Relying Party Agreement: The Relying Party Agreement is an agreement which must be read and accepted by a Relying Party prior to validating, relying on or using a Certificate or accessing or using DigiCert's Repository and is available for reference at http://www.digicert.com/ssl-cps-repository.htm.

Subscriber: The entity that has been issued a Certificate; the Subject of an EV Certificate.

Subscriber Agreement: The Subscriber Agreement is an agreement that must be read and accepted by an Applicant before applying for a Certificate. The Subscriber Agreement is specific to the Digital Certificate product type as presented during the product online order process and is available for reference at http://www.digicert.com/ssl-cps-repository.htm.

Verified Legal Opinion: An opinion letter from attorney verified by DigiCert as follows:

(A) Status of Author. Contacting the licensing authority of the legal practitioner author to confirm licensure as:

(i) A lawyer (or solicitor, barrister, advocate, or equivalent) licensed to practice law in the country of the Applicant's Jurisdiction of Incorporation or any jurisdiction where the Applicant maintains an office or physical facility; or

(ii) A notary that is a member of the International Union of Latin Notaries, and is licensed to practice in the country of Applicant's Jurisdiction of Incorporation or any jurisdiction where the Applicant maintains an office or physical facility (and that such jurisdiction recognizes the role of the Latin Notary).

(B) Basis of Opinion. Reviewing the text of the legal opinion to determine that the Legal Practitioner is acting on behalf of the Applicant and that the conclusions of the Verified Legal Opinion are based on the Legal Practitioner's stated familiarity with the relevant facts and the exercise of the Legal Practitioner's professional judgment and expertise.

(C) Authenticity. Verified by calling or sending a copy of the legal opinion back to the Legal Practitioner at the address, phone number, facsimile, or (if available) e-mail address for the Legal Practitioner listed with the authority responsible for registering or licensing such Legal Practitioner and obtaining confirmation from the Legal Practitioner or the Legal Practitioner's assistant that the legal opinion is authentic.

Verified Accountant Letter: An accountant's letter verified by DigiCert as follows:

(A) Status of Author. Professional status of the author verified by directly contacting the authority responsible for registering or licensing such Accounting Practitioner (s) in the applicable jurisdiction.

(B) Basis of Opinion. Reviewing the text of the accountant letter to confirm that the Accounting Practitioner is acting on behalf of the Applicant and that the information in the accountant letter are based on the Accounting Practitioner's stated familiarity with the relevant facts and the exercise of the practitioner's professional judgment and expertise.

(C) Authenticity. Verified by calling or sending a copy of the accountant letter back to the Accounting Practitioner at the address, phone number, facsimile, or (if available) e-mail address for the Accounting Practitioner listed with the authority responsible for registering or licensing such Accounting Practitioner and obtaining confirmation from the Accounting Practitioner or the Accounting Practitioner's assistant that the accountant letter is authentic.

Acronyms:

CA	Certificate Authority or Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DCPA	DigiCert Policy Authority
EU	European Union
EV	Extended Validation
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
OID	Object Identifier
PED	PIN Entry Device (manufactured by SafeNet – http://www.safenet-inc.com)
PKI	Public Key Infrastructure
PKIX	IETF Working Group on Public Key Infrastructure
PKCS	Public Key Cryptography Standard
QGIS	Qualified Government Information Source
QIIS	Qualified Independent Information Source
SHA-1	Secure Hashing Algorithm
SSL	Secure Sockets Layer
TLS	Transaction Layer Security
URL	Uniform Resource Locator
X.509	The ITU-T standard for Certificates and their corresponding authentication framework

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

DigiCert publishes any revocation data on issued digital certificates, this CPS, certificate terms and conditions, the relying party agreement and the subscriber agreement in the official DigiCert repository http://www.digicert.com/ssl-cps-repository.htm

2.2 Publication of certification information

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

- On the web: www.digicert.com
- By email from admin@digicert.com
- by mail addressed to: DigiCert, Inc., 333 South 520 West, Lindon, Utah 84042
- by telephone Tel: 1-801-805-1620
- by fax: 1-801-705-0481

DigiCert publishes CRLs to allow relying parties to determine the validity of a certificate issued by

DigiCert. Each CRL contains entries for all revoked un-expired certificates issued and is valid for 24 hours. DigiCert maintains revocation entries on its CRLs, or makes certificate status information available via OCSP, until after the expiration date of the revoked EV Certificate.

2.3 Time or frequency of publication

DigiCert issues a new CRL every 24 hours and prior to the expiry of the current CRL. The CRL includes a monotonically increasing sequence number for each CRL issued. Under special circumstances DigiCert may publish new CRL's prior to the expiry of the current CRL. *See* Section 4.9.7, CRL Issuance Frequency.

2.4 Access controls on repositories

Parties (including Subscribers and Relying Parties) accessing the DigiCert Repository (http://www.digicert.com/ssl-cps-repository.htm) and other DigiCert publication resources are deemed to have agreed with the provisions of this CPS and any other conditions of usage that DigiCert may make available. Parties demonstrate acceptance of the conditions of usage of this CPS by using a DigiCert-issued EV Certificate. Failure to comply with the conditions of usage of the DigiCert Repositories and web site may result in termination of the relationship between DigiCert and the party, at DigiCert's sole discretion, and any unauthorized reliance on an EV Certificate shall be at that party's risk.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

Certificates are issued with a non-null subject Distinguished Name (DN) complying with ITU X.500 standards. Certificates are issued using the Fully Qualified Domain Name (FQDN) name of the server, service or application that has been confirmed with the Subscriber. 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.

3.1.2 Need for names to be meaningful

DigiCert ensures that the Organization (O) and Organizational Unit (OU) attributes in the Subject field accurately identify the legal entity that is the subject of the certificate. Similarly, DigiCert uses non-ambiguous designations in the Issuer field to identify itself as the Issuer of a certificate (e.g., DigiCert High Assurance EV CA-1).

3.1.3 Anonymity or pseudonymity of subscribers

DigiCert does not issue anonymous or pseudonymous certificates.

3.1.4 Rules for interpreting various name forms

Distinguished Names in Certificates shall be 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

Name uniqueness is ensured through the use of the Common Name attribute of the Subject Field, which contains the authenticated domain name, which is controlled under the auspices of the Internet Corporation for Assigned Names and Numbers (ICANN).

3.1.6 Recognition, authentication, and role of trademarks

Subscribers shall solely be responsible for the legality of the information they present for use in certificates issued under this CPS, in any jurisdiction in which such content may be used or viewed. DigiCert subscribers represent and warrant that when submitting certificate requests to DigiCert and using a domain

and distinguished name (and all other certificate application information) they do not interfere with or infringe upon the rights of any third parties in any jurisdiction with respect to their trademarks, service marks, trade names, company names, or any other intellectual property right, and that they are not seeking to use the domain and distinguished names for any unlawful purpose, including, without limitation, tortious interference with contract or prospective business advantage, unfair competition, injuring the reputation of another, or to confuse or mislead any person, whether natural or corporate. Certificate Subscribers shall defend, indemnify, and hold DigiCert harmless for any loss or damage resulting from any such interference or infringement and shall be responsible for defending all actions against DigiCert.

3.2 Initial identity validation

Figure 1 below is a simplified flow chart of the enrollment and certificate issuance process used by DigiCert to issue EV Certificates

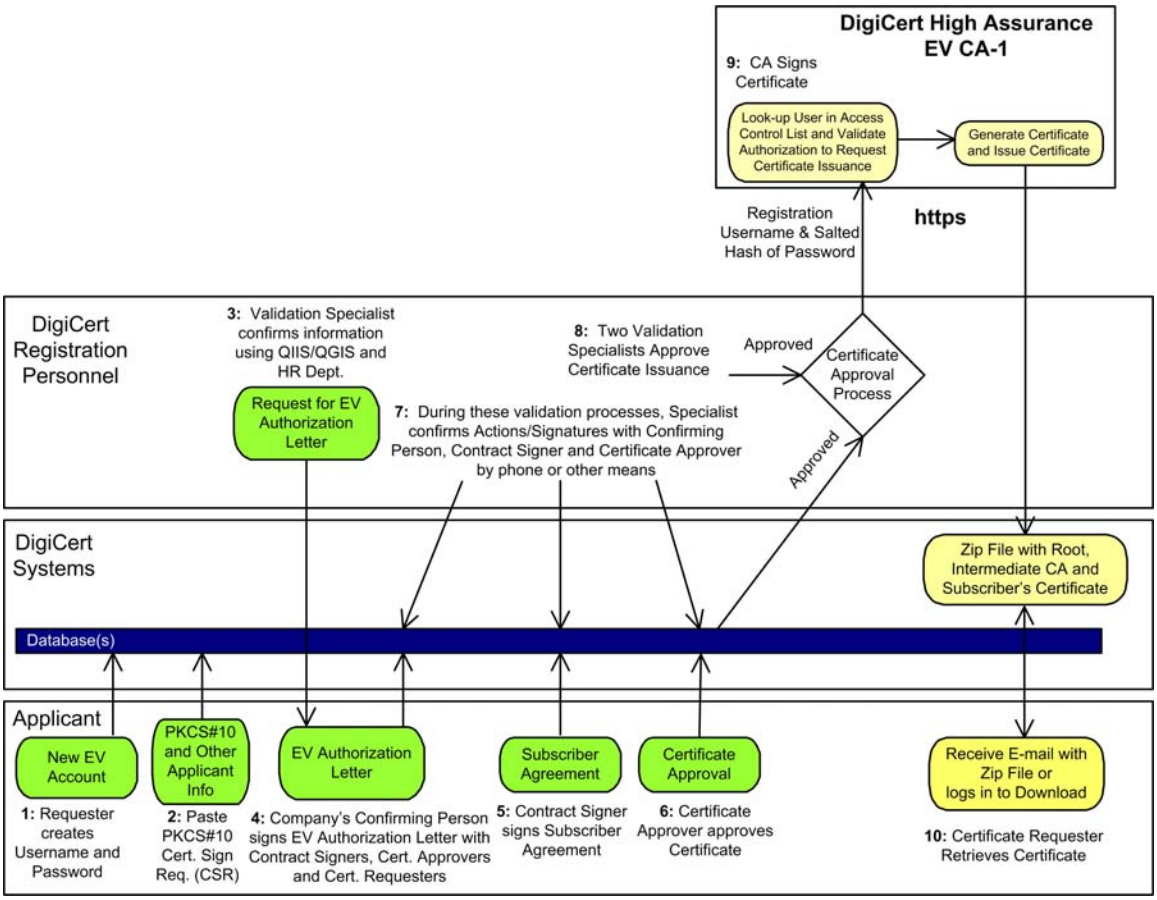

Figure 1.

3.2.1 Method to prove possession of private key

The applicant must submit a digitally signed PKCS#10 CSR to establish that it holds the private key corresponding to the public key to be included in an EV Certificate. DigiCert parses the PKCS#10 CSR submitted by the Applicant in a secure manner and verifies that the Applicant's digital signature on the PKCS#10 was created by the private key corresponding to the public key in the PKCS#10 CSR.

3.2.2 Authentication of organization identity

3.2.2.1 Data Elements Collected

The elements listed in this section are collected and utilized by DigiCert during the certificate issuance process to authenticate identity as discussed above. Elements that are already in the public domain

(e.g., available via WHOIS, etc.) are not treated as confidential for purposes of the privacy and protection of data provisions outlined in Section 9.3 and Section 9.4 of this CPS.

Fields Parsed from the PKCS#10 CSR and used to populate Certificate Request Forms when CSR is submitted during Step 2:

1. Common Name (cn) - Domain Name

The Applicant's Common Name in the CSR must match the Fully Qualified Domain Name(s) of one or more host domain name(s) owned or controlled by the Subject. Such server may be owned and operated by the Subject or another entity (e.g., a hosting service). Wildcard certificates are not allowed for EV Certificates.

2. Organization name (o)

The Applicant's formal legal organization name to be included in EV Certificate, as recorded with the Incorporating Agency in Applicant's Jurisdiction of Incorporation (for Private Organizations), or as specified in the law of Applicant's Jurisdiction of Incorporation (for Government Entities). The "o=" MUST match the Applicant's full legal name and MAY include the Applicant's assumed name (e.g., d/b/a name) to be included in the EV Certificate, as recorded in the Applicant's legal jurisdiction. However, if an assumed name is used, the "o=" MUST be in the format of "Assumed Name (Full Legal Name)."

3. City, State and Country

This is the actual physical location of the Applicant. The legal jurisdiction of the Applicant is requested in the certificate request forms discussed in item 2 below.

4. Subject Public Key

This is the public key corresponding to the Applicant's private key used to sign the PKCS#10.

Additional Information Collected from Certificate Requester in Certificate Request Forms During Step 2:

1. Confirmation of Correct Legal Name by the Applicant of the correct Organization Name (o) as provided above in the PKCS#10 CSR. If the organization information in the CSR is not correct, the Certificate Requester is directed to generate a new CSR with the correct details. See Section 4.1.2.

2. Jurisdiction of Incorporation: Applicant's Jurisdiction of Incorporation to be included in EV Certificate, and consisting of:

(a) City or town (if any),
(b) State or province (if any), and
(c) Country.

3. Incorporating Agency: The name of the Applicant's Incorporating Agency;

4. Registration Number: The unique registration number assigned to Applicant by the Incorporating Agency in Applicant's Jurisdiction of Incorporation and to be included in EV Certificate (for Private Organization Applicants only).

5. Other Identifying Numbers: DUNS Number and VAT Number, etc., if available,

6. Street Address: The address of Applicant's Place of Business, including:

(a) Building number and street,
(b) City or town,
(c) State or province (if any),
(d) Country,
(e) Postal code (zip code), and
(f) Main telephone number.

7. Contract Signer Name: Name and contact information of the Contract Signer who is authorized sign Subscriber Agreements on behalf of the Applicant;

8. Certificate Approver Name: Name and contact information of the Certificate Approver submitting and signing, or that has authorized the Certificate Requester to submit and sign, the

EV Certificate Application on behalf of the Applicant; and

9. Certificate Requester Name: Name and contact information of the Certificate Requester submitting the EV Certificate Request on behalf of the Applicant, if other than the Certificate Approver.

10. Server Software Identification (obtained when CSR is submitted during **Step 2**)

3.2.2.2 EV Guideline Requirements for Authentication of Organizational Identity

This section contains the methods that DigiCert uses to meet the requirements of the Guidelines for establishing organizational identity. The procedural steps used by DigiCert to authenticate organizational identity in accordance with the Guidelines may be found below in Section 4.1 and Section 4.2. DigiCert may use any means of communication at its disposal that are consistent with the Guidelines to ascertain the identity of an Applicant or to confirm the request for an EV Certificate. DigiCert reserves the right to not issue an EV Certificate in its absolute discretion.

A. Operational Existence. Subscribers of EV Certificates must satisfy the requirement of operational existence. If they have been in existence for less than three years, as indicated by the records of the Incorporating Agency, then they must be listed in the current information provided by a Qualified Independent Information Source, or they must have an active current Demand Deposit Account with a Regulated Financial Institution.

Additionally, the Guidelines require that DigiCert verify the following prior to certificate issuance: actual, current legal existence and identity; physical location; telephone number; and ownership or control of the domain name of the Applicant. The Guidelines also require DigiCert to confirm the accuracy of this information on an annual basis. In any case where such requirements cannot be confirmed through the methods identified below, DigiCert will rely on a Verified Legal Opinion from Applicant's legal counsel or a Verified Accountant's Letter from Applicant's accountant as confirmation of the accuracy of the Applicant's assertion in regard to that requirement.

DigiCert follows the allowed verification procedures for confirmation of organizational identity found in the Guidelines as follows:

B. Legal Existence and Identity

Verifying through a Qualified Government Information Source or directly through contact with the Incorporating Agency:

(1) Legal Existence: that the Applicant is a legally recognized entity, in existence and validly formed (e.g., incorporated) with the Incorporating Agency in Applicant's Jurisdiction of Incorporation, and not designated on the records of the Incorporating Agency by labels such as "inactive," "invalid," "not current," or the equivalent;

(2) Organization Name: that the Applicant's formal legal name as recorded with the Incorporating Agency in Applicant's Jurisdiction of Incorporation matches Applicant's name in the EV Certificate Request;

(3) Registration Number: the specific unique Registration Number assigned to Applicant by the Incorporating Agency in the Applicant's Jurisdiction of Incorporation (if such exist); and

(4) Registered Agent: the identity and address of the Applicant's Registered Agent or Registered Office (as applicable) in the Applicant's Jurisdiction of Incorporation.

Assumed names must be registered and similarly verified with the appropriate government agency for such filings in the jurisdiction of the Applicant's Place of Business.

C. Physical Location

For Applicants whose Place of Business is in the same country as the Applicant's Jurisdiction of Incorporation, by obtaining:

(1) **QIIS:** the Applicant's address from the current version of such information maintained by a Qualified Independent Information Source; or

(2) **Site Visit:** documentation of a site visit to the business address which MUST be performed by a reliable individual or firm. The documentation of the site visit MUST:

(a) Verify that the Applicant's business is located at the exact address stated in the EV Certificate Request (e.g., via permanent signage, employee confirmation, etc.);

(b) Identify the type of facility (e.g., office in a commercial building, private residence, storefront, etc.) and whether it appears to be a permanent business location;

(c) Indicate whether there is a permanent sign (that cannot be moved) that identifies the Applicant

(d) Indicate whether there is evidence that Applicant is conducting ongoing business activities at the site (e.g., that it is not just a mail drop, P.O. box, etc.), and

(e) Include one or more photos of (i) the exterior of the site (showing signage indicating the Applicant's name, if present, and showing the street address if possible), and (ii) the interior reception area or workspace.

For Applicants whose Place of Business is not in the same country as the Applicant's Jurisdiction of Incorporation, DigiCert will rely on a Verified Legal Opinion that indicates the address of Applicant's Place of Business and that business operations are conducted there.

D. Business Telephone Number

DigiCert performs the following:

(A) Calls Applicant's telephone number and obtains an affirmative response sufficient to enable a reasonable person to conclude that the Applicant is reachable by telephone at the number dialed; and

(B) Confirms telephone number is listed as Applicant's business telephone number in records provided by the applicable phone company or a Qualified Independent Information Source.

Alternatively, during a site visit, the person who is conducting the site visit could call the telephone number provided and conclude by talking to the person present at Applicant's site during the visit—who is also on the phone with the person calling—that the Applicant is reachable by telephone at the number dialed; provided that the number confirmed is not a mobile phone.

E. Ownership or Exclusive Control of Domain Name

The Guidelines require that the Applicant:

(A) is the registered holder of the domain name; or

(B) has been granted the exclusive right to use the domain name by the registered holder of the domain name; and that

the Applicant is aware of its registration or exclusive control of the domain name.

DigiCert confirms that the Applicant is the registered holder of the domain name or has been granted the exclusive right to use the domain name by the registered holder by performing a WHOIS inquiry on the Internet for the domain name supplied by the Applicant, and:

(A) obtaining a response indicating that the Applicant is the entity registered to the domain name; or

(B) communicating with domain name registrar or the contact listed on the WHOIS record to confirm that the Applicant is the registered holder of the domain name or has the exclusive right to use a domain name.

Registered Domain Holder Contacted to Confirm Applicant's Exclusive Right. In cases where the registered domain holder can be contacted using information obtained from WHOIS, or through the domain registrar, DigiCert obtains positive confirmation from the registered domain holder by paper mail, e-mail, telephone, or facsimile that the Applicant has been granted the exclusive right to use the requested Fully Qualified Domain Name (FQDN). In addition, DigiCert verifies the Applicant's exclusive right to use the domain name by:

(1) Relying on a Verified Legal Opinion to the effect that the Applicant has the exclusive right to use the specified domain name in identifying itself on the Internet; or

(2) Relying on a representation from the Contract Signer, or the Certificate Approver if expressly authorized in a mutually agreed upon contract, coupled with a practical demonstration by the Applicant establishing that it controls the confirmed domain name by making an agreed-upon change in information found online on a web page identified by a uniform resource identifier containing the Applicant's FQDN.

Registered Domain Holder Cannot Be Contacted to Confirm Applicant's Exclusive Right. In cases where the registered domain holder cannot be contacted, DigiCert may:

(1) Rely on a Verified Legal Opinion to the effect that the Applicant has the exclusive right to use the specified domain name in identifying itself on the Internet, and

(2) Rely on a representation from the Contract Signer, or the Certificate Approver if expressly authorized in a mutually agreed upon contract, coupled with a practical demonstration by the Applicant establishing that it controls the confirmed domain name by making an agreed-upon change in information found online on a web page identified by a uniform resource identifier containing the Applicant's FQDN.

Knowledge. To confirm that the Applicant is aware of such ownership or control of the domain name, DigiCert may rely on a Verified Legal Opinion to the effect that the Applicant is aware that it has exclusive control of the domain name, or it may obtain confirmation from the Contract Signer or Certificate Approver verifying that the Applicant is aware that it has exclusive control of the domain name.

3.2.3 Authentication of individual identity

Not applicable.

3.2.4 Non-verified subscriber information

DigiCert does not include unconfirmed subscriber information in Certificates. DigiCert is not responsible for non-verified Subscriber information submitted to DigiCert or the DigiCert directories or otherwise submitted with the intention to be included in a certificate, except as it may have otherwise been stated in relation to Qualified Certificates issued pursuant to the requirements of the European Directive 99/93.

3.2.5 Validation of authority

For certificates issued at the request of a Subscriber's agent, both the agent and the Subscriber shall jointly and severally indemnify and hold harmless DigiCert, and its parent companies, subsidiaries, directors, officers, employees, agents, and contractors.

The Subscriber shall control and be responsible for the data that an agent of Subscriber supplies to DigiCert. The Subscriber must promptly notify DigiCert of any misrepresentations and omissions made by an agent of Subscriber. The duty of this article is continuous.

The authority of individuals to act as the Subscriber's agents is confirmed by receipt of an EV Authorization Letter from the Subscriber signed by a person with authority (i.e., a "Confirming Person").

(1) Confirmation Request. Persons who have such authority are contacted by DigiCert through an appropriate out-of-band communication requesting verification or confirmation of the particular fact in issue, i.e., the individual's authorization as a Contract Signer, Certificate Approver or Certificate Requester.

The request for the EV Authorization Letter is directed to:

(a) A position within Applicant's organization who qualifies as a Confirming Person (e.g., Secretary, President, CEO, CFO, COO, CIO, CSO, Director, etc.) and who is identified by name and title in a current Qualified Government Information Source (e.g., an SEC filing), a Qualified Independent Information Source, a Verified Legal Opinion, a Verified Accountant Letter, or by contacting the Applicant's Human Resources Department by phone or mail (at the phone number or address for Applicant's Place of Business, verified in accordance with the Guidelines); or

(b) Applicant's Registered Agent or Registered Office in the Jurisdiction of Incorporation as listed in the official records of the Incorporating Agency, with instructions that it be forwarded to an appropriate Confirming Person.

If the request for the EV Authorization Letter is sent by paper mail, it is addressed to:

(a) The verified address of Applicant's Place of Business;

(b) The business address for such Confirming Person specified in a current Qualified Government Information Source (e.g., an SEC filing), a Qualified Independent Information Source, a Verified Legal Opinion, or a Verified Accountant Letter; or
(c) The address of Applicant's Registered Agent or Registered Office listed in the official records of the Jurisdiction of Incorporation.

If the request for the EV Authorization Letter is sent by e-mail, it is addressed to the Confirming Person's business e-mail address as listed in a current Qualified Government Information Source, a Qualified Independent Information Source, a Verified Legal Opinion, or a Verified Accountant Letter.

If the request for the EV Authorization Letter is made by telephone call, then the Confirming Person is contacted by calling the verified main phone number of Applicant's Place of Business, asking to speak to such person, and the person taking the call identifies himself or herself as such person.

When a request for the EV Authorization Letter is sent by facsimile, then it is sent to the facsimile number listed in a current Qualified Government Information Source, a Qualified Independent Information Source, a Verified Legal Opinion, or a Verified Accountant Letter with the fax cover page clearly addressed to the Confirming Person.

(2) Confirmation Response. DigiCert's receipt of the EV Authorization Letter from the Confirming Person is verified by telephone, e-mail or other written communication between DigiCert and the Confirming Person.

(3) Verification of Name, Title, and Authority of Contract Signer and Certificate Approver. The Guidelines require that DigiCert verify the name, title and authority of Contract Signers and Certificate Approvers. The EV Authorization Letter accomplishes these objectives by providing independent confirmation from the Applicant of such name, title, and authority as outlined above. The attestations in the EV Authorization Letter include the employment and signing authority of the Contract Signer and the employment and approval authority of the Certificate Approver.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Prior to certificate expiration, a Subscriber may perform routine re-key by logging into the Subscriber's customer account using his or her user name and password. Through routine re-key, a new certificate is created with the same certificate contents except for a new Public Key and, optionally, a new, extended validity period. Re-keying is allowed in accordance with Section 4.7 provided that the DigiCert has performed all authentication and verification of information tasks required by the Guidelines and that the EV Authorization Letter is still valid (i.e. the Certificate request is made and approved within the specified term stated in the EV Authorization Letter which expressly authorizes designated personnel to exercise authority with respect to future applications for EV Certificates). *See also* Section 4.6.

3.3.2 Identification and authentication for re-key after revocation

There is no re-key after revocation. After revocation a subscriber must submit a new application.

3.4 Identification and authentication for revocation request

See Sections 4.9.1 through 4.9.3 for information about Certificate revocation procedures.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

This Part 4 of the CPS describes the certificate application process.

4.1 Certificate Application

4.1.1 Who can submit a certificate application

Certificate applications MUST be submitted by Certificate Requesters who are persons authorized to request the issuance of EV Certificates on behalf of Applicants. Certificate Requesters are formally recognized by DigiCert only after DigiCert has confirmed their appointment with the Applicant in accordance with Section 3.2.5, Validation of Authority.

4.1.2 Enrollment process and responsibilities

The following Applicant roles are required for the issuance of an EV Certificate:

- **Certificate Requester** – The EV Certificate Request Form MUST be submitted by an authorized Certificate Requester.
- **Certificate Approver** – The EV Certificate Request Form MUST be approved by an authorized Certificate Approver.
- **Contract Signer** – A Subscriber Agreement applicable to the requested EV Certificate MUST be signed by an authorized Contract Signer.

In **Step 2** of the enrollment process, the Requester pastes and submits the PKCS#10 CSR into a web form that is submitted to DigiCert's CA systems. Between **Steps 2 and 3** of the enrollment process, information is collected from the PKCS#10 CSR and compared with information available in the WHOIS record. (*See* Section 3.2.2, Fields Parsed and Automatically Populated from PKCS#10 CSR.) The Requester is presented with information extracted from the PKCS#10 CSR, i.e., the company name from the Organizational name (e.g., O= XYZ, Inc.) and the domain name from the Common Name (CN=XYZ.com) contained in the PKCS#10 CSR. The Requester is required to verify that the full legal name of the organization (and if applicable, any assumed name) in the application is correct and that all records match. If the common name does not match, the Requester must make the necessary corrections and generate and re-submit a new PKCS#10 to proceed. (If other information does not match, a new PKCS#10 may or may not be required, depending on the server platform.) DigiCert registration personnel compare the information submitted by the Requester to ensure that it is consistent with the information in the WHOIS record before allowing the application process to continue.

Requesters must complete the online forms at DigiCert's website. Under special circumstances a Requester may submit the same information in an application via email; however this process is made available to Applicants at the sole discretion of DigiCert.

4.2 Certificate application processing

During the certificate approval process identified in Figure 1 above, DigiCert Registration Personnel employ controls to validate the identity of the Subscriber and other information featured in the certificate application. DigiCert registration personnel review the application information provided by the Applicant to ensure compliance with the Guidelines.

The following steps describe the milestones in the Certificate (as illustrated in Figure 1 above):

Steps 1 and 2: The Requester fills out the online request on DigiCert's web site and submits the required information, including PKCS#10 CSR, common name, organizational information, address, and billing information along with his or her electronic signature. The Requester submits other required information to DigiCert, including contact names of personnel within the organization who have authority to approve the request and sign the Subscriber Agreement. The Requester provides a credit card number and other information to pay for processing the request and issuing the EV Certificate.

Step 3: DigiCert verifies all information that is required to be verified by the Guidelines using a variety of sources, including Qualified Independent Information Sources,

Qualified Government Information Sources, and the Applicant's Human Resources Department.

Steps 3 and 4: DigiCert requests and receives a signed EV Authorization Letter from the Applicant (unless a valid EV Authorization Letter from the Applicant is already in its possession).

Step 5: The Contract Signer is directed to a web page where the Subscriber Agreement is accepted by the Contract Signer.

Step 6: The Certificate Approver is either contacted by telephone or directed to a web page whereby the Certificate Approver's approval of certificate issuance is obtained.

Step 7: All signatures by Certificate Requesters, Certificate Approvers and Contract Signers are verified through follow-up procedures or telephone calls.

Step 8: Two (2) DigiCert Validation Specialists must approve issuance of the Certificate (see Final Cross-Correlation and Due Diligence below).

Step 9: A secure messaging system is used to send a certificate generation request to the DigiCert High Assurance EV CA, and the EV Certificate is created.

Step 10: The Certificate Requester is notified that the Certificate has been created and is ready for download (or is sent to the Requester zipped in an e-mail).

4.2.2 Approval or rejection of certificate applications

Prior to a determination of whether to approve or reject an application for an EV Certificate, DigiCert conducts other verification checks required by the Guideline, including the following:

1. Applications for EV Certificates are screened for high-risk targets of phishing and other fraudulent schemes. DigiCert checks appropriate internal and external lists of organization names that are most commonly targeted in phishing and other fraudulent schemes, and automatically flags such EV Certificate Requests for further scrutiny before issuance.
2. Individual names, applicant names, physical locations and jurisdictions of Applicants for EV Certificates are reviewed to determine whether they are identified on any government denied list, list of prohibited persons, or other list that prohibits doing business with such organization, person or jurisdiction under U.S. law.

Final Cross-Correlation and Due Diligence

Approval of certificate issuance by DigiCert requires two Validation Specialists. (*See* Section 5.2.2, Number of Persons Required per Task, and Section 5.2.4, Roles Requiring Separation of Duties).

(a) DigiCert's procedures ensure that the Validation Specialist who is not responsible for the collection and review of information reviews all of the information and documentation assembled in support of the EV Certificate and looks for discrepancies or other details requiring further explanation.

(b) DigiCert requests, obtains and documents further explanation or clarification from the Applicant, Certificate Approver, Certificate Requester, Qualified Independent Information Sources, and/or other sources of information, as necessary to resolve the discrepancies or details requiring further explanation.

(c) DigiCert does not issue an EV Certificate until the entire corpus of information and documentation assembled in support of the EV Certificate is such that issuance of the EV Certificate will not communicate inaccurate factual information that DigiCert knows, or by the exercise of due diligence should discover, from the assembled information and documentation. If satisfactory explanation and/or additional documentation are not received within a reasonable time, DigiCert will decline the EV Certificate Request and notify the Applicant accordingly.

(d) DigiCert performs the requirements of Final Cross-Correlation and Due Diligence through employees under its control and having appropriate training, experience, and judgment in confirming organizational identification and authorization.

From time to time, DigiCert may modify the requirements related to application information requested, based on DigiCert requirements, business context of the usage of certificates, or as it may be required by law.

Following successful completion of all required validations of a certificate application, DigiCert will approve an application for an EV Certificate.

If the information in the certificate application cannot be confirmed, then DigiCert will reject the certificate application. DigiCert reserves the right to reject an application for an EV Certificate if, in its own assessment, the good and trusted name of DigiCert might be tarnished or diminished and

may do so without incurring any liability or responsibility for any loss or expenses arising out of such refusal. DigiCert reserves the right not to disclose reasons for such a refusal.

Applicants whose applications have been rejected may subsequently re-apply.

4.2.3 Time to process certificate applications

DigiCert makes reasonable efforts to confirm certificate application information and issue an EV Certificate within a reasonable time frame. The time frame is greatly dependent on the Applicant providing the necessary details and documentation in a timely manner. Upon the receipt of the necessary details and documentation, DigiCert aims to confirm submitted application data and to complete the validation process and issue or reject a certificate application within two (2) working days.

From time to time, events outside of the control of DigiCert may delay the issuance process. However, DigiCert will make every reasonable effort to meet its issuance times and to make applicants aware of any factors that may affect issuance times in a timely manner.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Upon determining that all required steps have been completed, DigiCert registration personnel approve the issuance of the EV Certificate. As illustrated in Figure 1, when an EV Certificate is approved, a unique request string is sent to the CA via https. The request string contains the relevant parameters for the EV Certificate to be signed (e.g. PKCS #10 CSR, validity period, etc.) and authentication information for the DigiCert employee who is the Requester. The Requester's password is stored in the CA's access control database as a salted SHA-1 hash. Certificate access rights of DigiCert registration personnel (e.g. issue, revoke, retrieve) are managed by the CA system's access control database. The access control database determines whether the Requester has authorization to request certificate issuance from the specified CA key pair. If so, the CA system verifies the applicant's signature on the PKCS#10 CSR and extracts the subject fields and public key for insertion into the certificate template. The EV Certificate is constructed with additional extensions listed in Section 7.1 (e.g. CRL distribution points, Extended Key Usage, etc.). The new certificate is then signed with the CA private key and stored inside the database with a certificate retrieval number. To pick up the new EV Certificate, the calling application sends its username and password along with the certificate retrieval number. If the calling application has certificate retrieval access, then the certificate is returned to the calling application for storage in the web server database. The calling application also creates a ZIP file with the Subscriber's certificate and other certificates in the DigiCert trust chain (i.e. the root CA certificate and any intermediate CA certificates). The zip file is stored in the database.

4.3.2 Notification to subscriber by the CA of issuance of certificate

EV Certificates are delivered in a zip file via email to the email address designated by the Certificate Requester during the application process. The Certificate Requester is also provided a hypertext link to a userid/password-protected location on DigiCert's web server where the Requester 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

The Certificate Requester is responsible for installing the issued certificate on the Subscriber's computer or hardware security module according to the Subscriber's system specifications. A Subscriber is deemed to have accepted a certificate when:

- The subscriber uses the certificate; or
- 30 days pass since issuance of the certificate.

4.4.2 Publication of the certificate by the CA

DigiCert publishes the certificate by delivering it to the Subscriber. No other publication or notification to others occurs.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

Subscribers shall protect their private keys from access by unauthorized personnel or other third parties. Subscribers shall use private keys only in accordance with the usages specified in the key usage extension. See Sections 1.4.1, 6.1.7 and 7.1.

4.5.2 Relying party public key and certificate usage

DigiCert assumes that all user software will be compliant with X.509, the SSL/TLS protocol, and other applicable standards that enforce the requirements and requirements set forth in this CPS and the Certificate Profile (Appendix A). DigiCert does not warrant that any third party's software will support or enforce such controls or requirements, and all relying parties are advised to seek appropriate technical or legal advice.

Parties relying on an EV Certificate must adhere to the SSL/TLS protocol and verify a digital signature at all times by checking the validity of a digital certificate against the relevant CRL published by DigiCert. Relying Parties are alerted that an unverified digital signature cannot be assigned as a valid signature of the Subscriber.

The final decision concerning whether or not to rely on a verified digital signature or the security of an SSL/TLS session is exclusively that of the relying party. Reliance on a digital signature or SSL/TLS handshake should only occur if:

- The digital signature or SSL/TLS session was created during the operational period of a valid certificate and it can be verified by referencing a validated certificate.
- The relying party has checked the revocation status of the certificate by referring to the relevant CRLs and the certificate has not been revoked.
- The relying party understands that a digital certificate is issued to a subscriber for a specific purpose and that the private key associated with the digital certificate may only be used in accordance with the usages specified in this CPS and contained in the certificate.

Reliance is accepted as reasonable under the provisions made for the relying party under this CPS and within the Relying Party Agreement. If the circumstances of reliance exceed the assurances delivered by DigiCert under the provisions made in this CPS, the relying party must obtain additional assurances.

Warranties are only valid if the steps detailed above have been carried out.

Relying on an unverifiable digital signature or SSL/TLS session may result in risks that the relying party assumes in whole and which DigiCert does not assume in any way.

By means of this CPS, DigiCert has adequately informed relying parties on the usage and validation of digital signatures and SSL/TLS sessions through this CPS and other documentation published in its public repository available at http://www.digicert.com/ssl-cps-repository.htm or also due to DigiCert availability via the contact addresses specified in Sections 2.2 and 9.11 of this CPS.

4.6 Certificate renewal

DigiCert makes reasonable efforts to notify subscribers via e-mail, of the imminent expiration of a digital certificate. Beginning sixty (60) days prior to the expiration of the certificate, DigiCert provides the subscriber with notice of pending expiration.

Renewal fees are detailed on the official DigiCert website and within communications sent to subscribers approaching the certificate expiration date.

Renewal application requirements and procedures are generally the same as those employed for the application validation and issuance requirements detailed for new customers. The maximum validity period for validated data that can be used to support issuance of an EV Certificate (before

revalidation is required) is one year, except for the Identity and authority of individuals appointed as Certificate Approvers in a currently valid written agreement with DigiCert and the Address of Place of Business where data has been refreshed by checking a Qualified Independent Information Source, even where a site visit was originally required.

In the case of outdated information, DigiCert repeats the verification processes required by the Guidelines. In other words, at least once each year DigiCert registration personnel reconfirm (1) domain name ownership using current WHOIS information, (2) legal existence, any assumed names, and identity with state or other jurisdictional records for geographic location, company control and good standing in the jurisdiction of organization, (3) Telephone number for Place of Business, (4) Bank account verification. If a company is no longer in good standing, or if any of the other foregoing information cannot be verified, the certificate is not renewed.

Other aspects of certificate renewal (e.g., who may request renewal, notification of issuance, conduct constituting acceptance, and publication of the certificate) are the same as they are for initial certificate issuance. *See* Sections 4.1, 4.2, 4.3 and 4.4.

4.7 Certificate re-key

Re-keying a certificate means to request a new certificate with the same certificate contents except for a new Public Key. This might occur, for instance, if the subscriber accidentally deletes the corresponding private key. 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, DigiCert can use the same PKCS#10 CSR as was used for the previous certificate. Otherwise, a new PKCS#10 CSR must be submitted and a new certificate is issued, provided that the subscriber meets the application validation and issuance requirements detailed for new customers, or otherwise qualifies for certificate renewal, above, or certificate modification/re-issue, below. Other aspects of certificate re-key (e.g., who may request re-key, notification of issuance, conduct constituting acceptance, and publication of the certificate) are the same as they are for initial certificate issuance. *See* Sections 3.3.1, 4.1, 4.2, 4.3 and 4.4.

4.8 Certificate modification

DigiCert will reissue or replace a certificate during the certificate's lifetime when the Subscriber's common name, organization name, device name, or geographic location changes. These situations might occur as the result of a merger or acquisition, new branding campaign, company move or network reconfiguration. Then, certificate modification processes may be used to issue a new certificate provided that the modified information for the subscriber meets the application validation and issuance requirements detailed for new customers (because the new organizational information must be confirmed). Except for when only a minor change is made to one of the names in the certificate, all replaced certificates are revoked because the identifying information in the certificate is no longer true. Other aspects of certificate modification (e.g., who may request certificate modification, notification of issuance, conduct constituting acceptance, and publication of the certificate) are the same as they are for initial certificate issuance. *See* Sections 4.1, 4.2, 4.3 and 4.4.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

Revocation of an EV Certificate is to permanently end the operational period of the certificate prior to reaching the end of its stated validity period. DigiCert may revoke any EV Certificate for any reason or no reason. An EV Certificate may be revoked based on information confirmed in a Certificate Problem Report, as discussed elsewhere in this Section 4.9.

DigiCert will revoke an EV Certificate if:

- The Subscriber requests revocation of its EV Certificate;
- The Subscriber indicates that the original EV Certificate Request was not authorized and does not retroactively grant authorization;
- DigiCert obtains reasonable evidence that there has been loss, theft, modification, unauthorized disclosure, or other compromise of the Private Key corresponding to the Public Key within the EV Certificate;

- DigiCert receives notice or otherwise becomes aware that a Subscriber has breached a material obligation under the Subscriber Agreement;
- Either the subscriber's or DigiCert's obligations under this CPS are delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's reasonable control, and as a result another person's information is materially threatened or compromised;
- DigiCert ceases operations for any reason and has not arranged for another EV CA to provide revocation support for the EV Certificate;
- DigiCert's right to issue and manage EV Certificates under the Guidelines expires or is revoked or terminated (unless arrangements have been made to continue maintaining the CRL/OCSP Repository);
- A DigiCert CA Private Key used to issue that EV Certificate has been compromised;
- DigiCert receives a lawful and binding order from a government or regulatory body to revoke the EV Certificate;
- DigiCert receives notice or otherwise become aware that a court or arbitrator has revoked a Subscriber's right to use the domain name listed in the EV Certificate, or that the Subscriber has failed to renew its domain name;
- DigiCert determines, in its sole discretion, that the EV Certificate was not issued in accordance with the terms and conditions of the Guidelines or DigiCert's EV Policies;
- DigiCert determines that any of the information appearing in the EV Certificate is not accurate;
- DigiCert receives notice or otherwise becomes aware that there has been some other modification of the information pertaining to the Subscriber that is contained within the EV Certificate; or
- If DigiCert receives notice or otherwise become aware that a Subscriber has been added as a denied party or prohibited person to a blacklist, or is operating from a prohibited destination under U.S. law as described in Section 23 of the Guidelines.

4.9.2 Who can request revocation

The Subscriber and its appropriately authorized parties can request revocation of an EV Certificate (e.g., a Contract Signer, Certificate Approver or Certificate Requester identified by the Subscriber in EV Authorization Letter of the Subscriber). DigiCert may, if necessary, also request that the revocation request be made by either an organizational contact, billing contact or the domain registrant.

For a party who is not the Subscriber, the filing of a "Certificate Problem Report" is the first step in initiating a certificate revocation request. These persons include Relying Parties, Application Software Vendors, and other third parties who may make reports to DigiCert of complaints or suspected Private Key compromise, EV Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to EV Certificates.

4.9.3 Procedure for revocation request

DigiCert employs the following procedure for processing a certificate revocation request:

- In the case of Certificate Problem Reports made by third parties or Certificate Revocation Requests made by the Subscriber, DigiCert validation personnel log the identity of the person making the request or problem report and the reason stated for the requested revocation.
- DigiCert personnel will confirm a Subscriber's revocation request through out-of-band mean, e.g., via telephone
- DigiCert personnel will begin an investigation of all Certificate Problem Reports within twenty-four (24) hours and decide whether revocation or other appropriate action is warranted based on at least the following criteria:
  (i) The nature of the alleged problem;
  (ii) Number of Certificate Problem Reports received about a particular EV Certificate or website;
  (iii) 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
  (iv) Relevant legislation in force.
- DigiCert will maintain a continuous 24/7 ability to internally respond to any high priority

Certificate Problem Report, and where appropriate, forward such complaints to law enforcement and/or revoke an EV Certificate that is the subject of such a complaint.

- Prior to approving revocation, DigiCert personnel approving the revocation request will create a record in the logging system containing DigiCert's reason for revocation.
- A command to revoke the EV Certificate is processed and the CRL is updated. Upon revocation of an EV Certificate, the operational period of that certificate is immediately considered terminated. The serial number of the revoked certificate is placed within the CRL and remains until one additional CRL is published after the end of the certificate's validity period.
- Revocation logs are maintained in accordance with the logging procedures covered in Section 5.5.1.2 of this CPS.

4.9.4 Revocation request grace period

There is no revocation grace period.

4.9.5 Time within which CA must process the revocation request

DigiCert revokes the EV Certificate and issues a CRL as soon as it has determined that a properly supported revocation request has been made.

4.9.6 Revocation checking requirement for relying parties

Users and relying parties are strongly urged to consult the directories of issued and revoked certificates at all times prior to relying on information featured in a certificate.

4.9.7 CRL issuance frequency

DigiCert manages and makes publicly available directories of revoked certificates through the use of CRLs. All CRL's issued by DigiCert are X.509v2 CRL's, in particular as profiled in RFC3280.

The DigiCert High Assurance EV CA updates and publishes a new CRL of revoked EV Certificates on a 24-hour basis or more frequently under special circumstances. On at least an annual basis, the DigiCert High Assurance EV Root CA publishes a CRL for its subordinate EV CA. The CRLs for certificates issued pursuant to this CPS can be accessed via the URLs contained in the Certificate Profile for that certificate. *See* Appendix A.

DigiCert also publishes a repository of legal notices regarding its PKI services, including this CPS, agreements and notices references within this CPS as well as any other information it considers essential to its services. The DigiCert legal repository may be accessed at: http://www.digicert.com/ssl-cps-repository.htm.

4.9.8 Maximum latency for CRLs

CRLs are generated every day at 6:05± AM GMT and are valid until 6:20± AM GMT the next day.

4.9.9 On-line revocation/status checking availability

DigiCert provides Online Certificate Status Protocol (OCSP) checking. The URL for the OCSP responder may be found within the Authority Information Access extension of the EV Certificate.

4.9.10 On-line revocation checking requirements

Users and relying parties are strongly urged to utilize OCSP to check the validity of an EV Certificate prior to relying on information featured in the EV Certificate.

4.9.11 Other forms of revocation advertisements available

None.

4.9.12 Special requirements re key compromise

DigiCert will use commercially reasonable efforts to notify potential Relying Parties if it discovers or suspects that a CA's Private Key has been compromised.

4.9.13 Circumstances for suspension

DigiCert does not utilize certificate suspension.

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

Not applicable.

4.11 End of subscription

A Subscriber may terminate its subscription to certificate services by allowing the term of a Certificate or applicable agreement to expire without renewal. *See* Section 4.6. A Subscriber may also voluntarily revoke a Certificate as explained in Section 4.9.

4.12 Key escrow and recovery

DigiCert does not perform escrow or recovery of subscriber private keys.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

This Part 5 of the CPS outlines the security policy, physical and logical access control mechanisms, service levels and personnel policy in use by DigiCert to provide trustworthy and reliable CA operations.

5.1 Physical controls

5.1.1 Site location and construction

DigiCert performs its CA operations in a secure data center located in a hosted co-location facility in the State of Utah, United States of America. The building is constructed of steel and masonry. DigiCert houses its CA platform inside a locked computer cabinet located inside the data center in a room with no windows to the outside (the "Data Center"). Customer support and organizational identity vetting operations take place inside a separate room within the same secure facility (the "Support and Vetting Room"). The site operates under a security policy designed to detect, deter and prevent unauthorized logical or physical access to DigiCert's operations.

5.1.2 Physical access

Three layers of physical security exist between the outside of the building and DigiCert's operations. Access to the secure part of DigiCert facilities is limited through the use of physical access control and is only accessible to appropriately authorized individuals. DigiCert employees are issued photo ID access cards imprinted with a serial number to record ingress and egress through controlled access doors located throughout the facility.

During regular business hours, entry to the building is accessed through a reception area with a receptionist on duty. After hours, an access card is required to enter the building. A security guard is also on duty at the facility 24 hours a day, 7 days a week, and 365 days a year. Access to all areas beyond the reception area requires the use of an "access" or "pass" card. All access card use is logged. The building is equipped with motion detecting sensors, and the exterior and internal passageways of the building are also under constant video surveillance.

5.1.2.1 Data Center

Access to the Data Center housing the CA platform requires two-factor authentication—the individual must have his or her access card, and the doors to the room are equipped with biometric access control authenticators. The doors are programmed to require that the same access card be used to exit the room (anti-passback control). The security guard's office is located adjacent to the data center, and the security guard makes rounds to check on the security of the data center at least every half hour.

5.1.2.2 Support and Vetting Room

A controlled access door secures the area of the facility hosting the Support and Vetting Room. The room is also equipped with motion detectors and a locked door. Video surveillance cameras are located in the passageways leading to the room.

5.1.3 Power and air conditioning

The Data Center has primary and secondary power supplies that ensure continuous, uninterrupted access to electric power. Redundant backup power is provided by battery uninterrupted power supplies (UPS) and two diesel generators.

Multiple, load-balanced HVAC systems for heating, cooling and air ventilation through perforated-tile, raised flooring are used to prevent overheating and to maintain a suitable humidity level for sensitive computer systems located in the Data Center.

5.1.4 Water exposures

The cabinet housing DigiCert's CA systems is located on raised flooring, no water lines exist above DigiCert's equipment, and the Data Center is equipped with a monitoring system to detect excess moisture.

5.1.5 Fire prevention and protection

The Data Center is equipped with an FM200 dry chemical fire suppression.

5.1.6 Media storage

DigiCert performs a daily backup of its computer systems on external hard disks that are rotated and stored either on-site or off-site according to an established backup rotation schedule. Media designated for storage on-site are kept in a fire-proof safe located in DigiCert's business offices. *See* Section 5.1.8 below for media designated for storage off-site.

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

On at least a weekly basis, media designated for storage off-site are taken to a safe deposit box at a federally insured and regulated financial institution. Media designated by the rotation schedule for storage on-site are retrieved at that time.

Backup copies of CA Private Keys and activation data (blue PED key and black PED key) are stored off-site at a federally insured financial institution in separate safe deposit boxes accessible only by trusted personnel. Activation material owned by the HSM Administrator/Security Officer role (blue PED key) is kept in a separate safe deposit box from activation material owned by personnel filling the Partition Administrator role (black PED key).

5.2 Procedural controls

5.2.1 Trusted roles

DigiCert personnel in trusted roles include, but are not limited to, CA and system administration personnel and personnel involved with customer support and vetting. An additional role external to DigiCert is the Auditor role, performed by DigiCert's auditor in accordance with Part 8 below. 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.

5.2.1.1 During Normal Operations

Operations Manager
During day-to-day operations, the DigiCert Operations Manager is a trusted role. The Operations Manager provides administrative and management oversight of DigiCert's operations. The Operations Manager may assist the CA Administrator, System Administrator or Security Officer in the performance of their roles. However, the Operations Manager does not serve in these roles unless circumstances dictate otherwise.

CA Administrator
The DigiCert CA Administrator is a trusted role. The CA Administrator is responsible for the installation and configuration of the CA software, including key generation and key management. The CA Administrator is responsible for performing and securely storing regular system backups of the CA system. The CA Administrator may also serve in the Security Officer role.

System Administrator/ System Engineer
The DigiCert System Administrator / System Engineer is a trusted role. The DigiCert System Administrator is responsible for the installation and configuration of the system hardware, including servers, routers, firewalls, and network configurations. The System Administrator / Engineer is also responsible for keeping systems updated with software patches and other maintenance needed for system stability and recoverability.

Customer Support Personnel
Customer support and vetting personnel serve in a trusted role. They are responsible for interacting with Applicants and Subscribers, managing the certificate request queue and completing the certificate approval checklist as identity vetting items are successfully completed. Customer support and vetting personnel may not serve in the Operations Manager role.

5.2.1.2 During Key Management Procedures

DigiCert uses the Safenet Luna PIN Entry Device (PED) to access its key storage system (i.e. hardware security cryptographic module or "HSM"). The PED connects to the HSM and bypasses computer systems that could introduce vulnerabilities into the key generation process. The PED comes with keys (PED keys) that are initialized with unique digital identifiers (secret keys) that are made specific to the HSM during the initialization process. The gray PED Key is used for initialization. During initialization, blue and black PED Keys are initialized and imprinted with secret keys specific to HSM so that the blue and black keys must be used to access the cryptomodule partitions where the key pairs are generated and stored. During key management procedures (e.g. activating the cryptomodule, root key generation and back-up, etc.), three trusted roles are implemented: the HSM Administrator/Security Officer who holds the blue PED key; the Partition Administrator, who holds the black PED key; and a third party acting as a witness.

5.2.2 Number of persons required per task

Handling of CA Private Keys (throughout the entire CA key lifecycle) requires the involvement of at least two persons. Physical and logical access controls exist for the key activation material in order to maintain multi-party control over the Hardware Security Modules containing CA Private Keys.

Certificate issuance requires the approval of at least two persons, acting in their trusted roles, per above.

Certificate revocation requires the approval of at least two persons, acting in their trusted roles, per above.

5.2.3 Identification and authentication for each role

DigiCert personnel in trusted roles must first authenticate themselves to the certificate management system before they are allowed access to the components of the system necessary to perform their trusted roles. For normal operations systems, access is controlled by user account and password, IP address subnet, and SSL. These mechanisms restrict access to those who are authorized and make actions directly attributable to the individual taking such action while fulfilling the trusted role.

5.2.4 Roles requiring separation of duties

Roles requiring separation of duties include, as stated above in Section 5.2.1. The HSM Administrator/ Security Officer and the Partition Administrator roles require separation of duties. No person who has acted in the HSM Administrator/Security Officer role may fill the Partition Administrator role, and vice versa, unless the PINs associated with the key held by both roles are changed or re-set.
The role of Validation Specialist requires participation of two people to approve certificate issuance as discussed " Final Cross-Correlation and Due Diligence" in Section 4.2.2 above. A Validation Specialist reviews and verifies all Applicant information and another Validation Specialist approves issuance of the EV Certificate.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

Consistent with this CPS, DigiCert maintains personnel and management practices that provide reasonable assurance of the trustworthiness and competence of its employees and of the satisfactory performance of their duties.

5.3.2 Background check procedures

Prior to the commencement of employment of any person by DigiCert for engagement in the EV Certificate issuance and management process, whether as an employee, agent, or an independent contractor of DigiCert, an identity check is performed that includes in-person physical appearance of the person before a trusted person whose responsibility it is verify identity. The trusted person must verify 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). Pre-employment checks include confirmation of previous employment, a check of professional references and confirmation of highest degree obtained. A criminal background check is performed on all trusted personnel before access is granted to DigiCert's certificate management system. These checks include, but are not limited to, verification of social security number, previous residences, driving records and criminal background.

5.3.3 Training requirements

DigiCert provides all personnel performing validation duties ("Validation Specialists") with skills training that covers basic Public Key Infrastructure (PKI) knowledge, authentication and verification policies and procedures, common threats to the validation process, including phishing and other social engineering tactics, and the Guidelines. Training of personnel is undertaken via a mentoring process involving senior members of the team to which they are attached. All new personnel must undergo this training process for at least two months. DigiCert maintain records of such training and ensures that personnel entrusted with Validation Specialist duties meet a minimum skills requirement that enable them to perform such duties satisfactorily. DigiCert ensures that its Validation Specialists qualify for each skill level required by the corresponding validation task before granting privilege to perform said task. All Validation Specialists are required to pass an internal examination on the EV Certificate validation criteria outlined in the Guidelines.

5.3.4 Retraining frequency and requirements

Validation Specialists engaged in EV Certificate issuance must maintain adequate skill levels in order to have issuance privilege, consistent with DigiCert's training and performance programs.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

Failure of any DigiCert employee or agent to comply with the provisions of this CPS, whether through negligence or malicious intent, will subject such individual to appropriate administrative and disciplinary actions, which may include termination as an employee or agent and possible civil and criminal sanctions. Any trusted personnel cited by management for unauthorized or inappropriate actions shall be immediately removed from the trusted role pending management review. Subsequent to management review, and

discussion of actions or investigation results with the employee, he or she may be reassigned to a non-trusted role or dismissed 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 the role to which they are assigned, including a copy of this CPS and all technical and operational documentation needed to maintain the integrity of DigiCert's CA operations. The information also includes internal system and security documentation, identity vetting policies and procedures, discipline-specific books, treatises and periodicals, and other information developed by DigiCert, provided to DigiCert by third parties or available over the Internet.

5.4 Audit logging procedures

5.4.1 Types of events recorded

All systems require identification and authentication at system logon with unique user name and password. Important system actions are logged to establish the accountability of the operators who initiate such actions. For audit purposes DigiCert maintains electronic or manual logs of (i) date and time, (ii) type of event, (iii) success or failure, and (iv) the user the initiating action, for the auditable events listed in the chart below.

Legend: OS = Automatically logged by Operating System, AP = Automatically logged by an audit reporting application, CM = Manually Logged through the Change Management process, ML = Manually logged by other means

Auditable Event	CA System	Vetting Interface
SECURITY AUDIT		
Any changes to the audit parameters, e.g., audit frequency, type of event audited	OS/AP	OS/AP
Any attempt to delete or modify the audit logs	OS/AP	OS/AP
AUTHENTICATION TO SYSTEMS		
The value of maximum number of authentication attempts is changed	OS/CM	OS/CM
Maximum number of authentication attempts occur during user login	OS/AP	OS/AP
An administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts	OS	AP/CM
An administrator changes the type of authenticator, e.g., from a password to a biometric (changes in configuration files, security profiles and administrator privileges)	N/A	CM
LOCAL DATA ENTRY		
All security-relevant data that is entered in the system (who is logged into the system when data is entered)	OS/AP	AP
REMOTE DATA ENTRY		
All security-relevant messages that are received by the system (including digital signature/authentication mechanism and message)	AP	AP
DATA EXPORT AND OUTPUT		
All successful and unsuccessful requests for confidential and security-relevant information	AP/ML	AP/ML
KEY GENERATION		
Whenever a CA generates a key (not mandatory for single session or one-time use symmetric keys)	AP/ML	N/A

Auditable Event	CA System	Vetting Interface
PRIVATE KEY LOAD AND STORAGE		
The loading of Component private keys	ML	N/A
All access to certificate subject Private Keys retained within the CA for key recovery purposes	N/A	N/A
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE	AP/ML	AP/ML
SECRET KEY STORAGE		
The manual entry of secret keys used for authentication	ML	N/A
PRIVATE AND SECRET KEY EXPORT		
The export of private and secret keys (keys used for a single session or message are excluded)	ML	N/A
CERTIFICATE REGISTRATION		
All certificate requests	N/A	AP
CERTIFICATE REVOCATION		
All certificate revocation requests	N/A	AP
CERTIFICATE STATUS CHANGE APPROVAL	N/A	AP
CA CONFIGURATION		
Any security-relevant changes to the configuration of a CA system component	CM	CM
ACCOUNT ADMINISTRATION		
Roles and users are added or deleted	CM/AP	CM/AP
The access control privileges of a user account or a role are modified	CM/AP	CM/AP
CERTIFICATE PROFILE MANAGEMENT		
All changes to the certificate profile	CM	N/A
REVOCATION PROFILE MANAGEMENT		
All changes to the revocation profile	CM	N/A
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT		
All changes to the certificate revocation list profile	CM	N/A
MISCELLANEOUS		
Installation of the Operating System	CM	CM
Installation of the PKI Application	CM	CM
Installation of Hardware Security Modules	ML	N/A
Removal of HSMs	ML	N/A
Destruction of HSMs	ML	N/A
System Startup	OS	OS
Logon attempts to PKI Application	AP	AP
Receipt of hardware / software	ML	ML
Attempts to set passwords	OS/AP	OS/AP
Attempts to modify passwords	OS/AP	OS/AP
Back up of the internal CA database	ML/AP	ML/AP
Restoration from back up of the internal CA database (date and time of restoration tests are kept in a disaster recovery log)	ML	ML
File manipulation (e.g., creation, renaming, moving)	OS/AP	OS/AP
Posting of any material to a repository	AP/ML	AP/ML
Access to the internal CA database	AP/ML	AP/ML
All certificate compromise notification requests	ML	ML
Loading HSMs with Certificates	ML	N/A
Shipment of HSMs	ML	N/A
Zeroizing HSMs	ML	N/A
Re-key of the Component	AP/ML	N/A
CONFIGURATION CHANGES		
Hardware	CM	CM
Software	CM	CM
Operating System	CM	CM
Patches	CM	CM
Security Profiles	CM	CM
PHYSICAL ACCESS / SITE SECURITY		
Personnel Access to room housing CA component	ML	N/A

Auditable Event	CA System	Vetting Interface
Access to a CA component	AP/ML	N/A
Known or suspected violations of physical security (with description of event)	ML	ML
ANOMALIES		
Software error conditions (with description of event)	OS/AP/CM	OS/AP/CM
Network attacks (suspected or confirmed) (with description of event, name of person reporting the event and resolution)	AP/ML	AP/ML
Equipment failure (with description of event, name of person reporting the event and resolution)	ML	ML
Electrical power outages (with description of event, name of person reporting the event and resolution)	ML	ML
Uninterruptible Power Supply (UPS) failure (with description of event, name of person reporting the event and resolution)	ML	ML
Obvious and significant network service or access failures (with description of event, name of person reporting the event and resolution)	ML	ML
Violations of this CPS (with description of event, name of person reporting the event and resolution)	ML	ML
Resetting Operating System clock	CM/ML	CM/ML

5.4.2 Frequency of processing log

On at least a monthly basis, the CA Administrator reviews the logs generated by the CA and vetting system applications, operating system logs and network device logs. The CA Administrator uses automated tools to scan for anomalies or specific conditions. These reviews include system and file integrity checks and vulnerability assessments. A written summary of the monthly review and vulnerability assessment is prepared that contains findings and recommendations for consideration by DigiCert's Operations Manager. These written reviews are also made available to DigiCert's auditor.

5.4.3 Retention period for audit log

DigiCert maintains its written monthly summaries of audit log reviews for a period not less than 7 years, or as necessary to comply with applicable laws. Audit logs are also kept until the completion of the next full CA Web Trust audit.

5.4.4 Protection of audit log

DigiCert personnel are obligated by this CPS to keep the audit logging information generated by them on their equipment until it is copied by the System Administrator. Audit logs are retained on-site in the office safe for at least two (2) months and are otherwise protected until after the next CA Web Trust audit.

5.4.5 Audit log backup procedures

No stipulation.

5.4.6 Audit collection system (internal vs. external)

No stipulation.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessments

See Section 5.4.2.

5.5 Records archival

5.5.1 Types of records archived

5.5.1.1 Certificate Issuance

All certificate issuance records (copies of certificates are held, regardless of their status as

expired or revoked) are retained as records in electronic and/or in paper-based archives for the period detailed below in Section 5.5.2. DigiCert may require Applicants to submit appropriate documentation in support of a certificate application. In such circumstances, DigiCert retains such records as stated in this CPS.

DigiCert records the following information related to certificate issuance as part of its certificate approval checklist process:

- the subscriber's PKCS#10 CSR;
- Documentation of organizational existence for organizational applicants as listed in Section 3.2.2;
- Documentation of individual identity for individual applicants as listed in Section 3.2.3;
- Verification of organizational existence and status received from third party databases and government entities (including screen shots of web sites reporting such information);
- Screen shot of WHOIS record for domain name to be listed in the certificate;
- Mailing address validation (if different than those identified through the resources listed above);
- Letter of authorization for web sites managed by third party agents of Applicants (if applicable);
- Submission of the certificate application, including acceptance of the Subscriber Agreement;
- Name, e-mail, and IP address of person acknowledging authority of the Applicant/Subscriber collected pursuant to Section 3.2.5;
- Screen shot of web site;
- Other relevant contact information for the Applicant/Subscriber; and
- Copy of Digital Certificates issued.

5.5.1.2 Certificate Revocation

Requests for certificate revocation are recorded and archived, including the name of the person requesting revocation, the reason for the request and the DigiCert personnel involved in authorizing revocation. This information and all resulting CRLs are retained as records in electronic archives for the period detailed in Section 5.5.2 below.

5.5.1.3 Other Information

DigiCert also archives the following information concerning its CA operations:

- Versions of this CPS
- Contractual obligations
- Records of CA System equipment configuration and CA Private Key access and usage
- Security and compliance audit data (*see* Section 5.4); and
- Any other data or applications necessary to verify the contents of the archive.

5.5.2 Retention period for archive

DigiCert retain the records of EV Certificates and the associated documentation for a term of no less than 7 years. The retention term begins on the date of certificate expiration or revocation.

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.

5.5.4 Archive backup procedures

No stipulation.

5.5.5 Requirements for time-stamping of records

System time for DigiCert computers are updated using the Network Time Protocol (NTP) to synchronize system clocks at least once every eight hours (Windows default). The following archived items on the

certificate approval checklist are time-stamped with the date, the time and the name of the DigiCert employee checking the information and making the record:

- Organizational status screen shot;
- WHOIS screen shot; and
- Screen shot of web site.

The following records are time-stamped by the certificate administration system when an item is either automatically received or is checked in by the DigiCert employee:

- Receipt of certificate application and PKCS#10 CSR;
- Letter of authorization;
- Name, e-mail, and IP address of person acknowledging organizational authority; and
- Other application information, as 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 proper request (see Sections 9.3 and 9.4) and payment of associated costs, DigiCert will create, package and send copies of archive information. Archived information is provided and verified by reference to the time stamps associated with such records as described in Section 5.5.5. Access to archive data is restricted to authorized personnel in accordance with DigiCert's internal security policies.

5.6 Key changeover

Key changeover procedures enable the smooth transition from expiring CA Certificates to new CA Certificates. Towards the end of the CA Private Key's lifetime, DigiCert ceases using its expiring CA Private Key to sign Certificates (well in advance of expiration) and uses the old Private Key only to sign CRLs. A new CA signing key pair is commissioned and all subsequently issued certificates and CRL's 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

To maintain the integrity of its services, DigiCert implements data backup and recovery procedures. DigiCert has developed a Disaster Recovery and Business Continuity Plan (DRBCP). DigiCert's CA system is redundantly configured at its primary facility and is mirrored with a tertiary system located at a separate, geographically diverse location for automatic failover in the event of a disaster (Disaster Recovery / Mirror Site). The DRBCP and supporting procedures are reviewed and tested periodically (at least on an annual basis) and are revised and updated as needed.

At its primary facility, DigiCert maintains a fully redundant CA system. The backup CA at the primary facility is readily available in the event that the primary CA should cease operation. All critical computer equipment is housed in a co-location facility run by a commercial data-center, and all of the critical computer equipment is duplicated within the primary facility.

At the Disaster Recovery / Mirror Site, DigiCert maintains a tertiary CA system that is a mirror of the primary system for failover in the event that the primary and secondary CAs should cease operation. All critical computer equipment at the Disaster Recovery / Mirror Site is also housed in a co-location facility run by a commercial data-center.

Incoming power and connectivity feeds are redundant at both facilities. The redundant equipment is ready to take over the role of supporting the CA and provides a maximum system outage time (in case of critical systems failure) of one hour.

5.7.2 Computing resources, software, and/or data are corrupted

DigiCert performs system back-ups on a daily basis. Back-up copies are made of CA Private Keys and are stored off-site in a secure location. In the event of a disaster whereby the primary and disaster recovery CA operations become inoperative at DigiCert's primary facility and the Disaster Recovery / Mirror Site, DigiCert will re-initiate its operations on replacement hardware using backup copies of its software, data and CA private keys at a comparable, secured facility.

5.7.3 Entity private key compromise procedures

In the event that a DigiCert CA private key has been or is suspected to have been compromised, 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 implementation of DigiCert's Incident Response Plan, outlined as follows:

- Collect all information related to the incident (and if the event is ongoing, ensure that all data are being captured and recorded);
- Begin investigating incident and determine degree and scope;
- Incident Response Team determines the course of action or strategy that should be taken, (and in the case of Key Compromise, determining the scope of certificates that must be revoked);
- Contact government agencies, law enforcement, and other interested parties and activate any other appropriate additional security measures;
- Monitor system, continue investigation, ensure that data is still being recorded as evidence, and make a forensic copy of data collected;
- Isolate, contain and stabilize the system, applying any short-term fixes needed to return the system to a normal operating state (contact browser software providers to discuss revocation/damage mitigation mechanisms if trust anchors may be affected);
- Prepare an incident report that analyzes the cause of the incident and documents the lessons learned, and circulate the report; and
- Incorporate lessons learned into the implementation of long term solutions and also into the Incident Response Plan for future use.

Following revocation of a CA Certificate and implementation of the Incident Response Plan, a new CA Key Pair should be generated and a new CA Certificate should be signed in accordance with procedures outlined in Part 6 of this CPS.

5.7.4 Business continuity capabilities after a disaster

See Sections 5.7.1 through 5.7.3 above.

5.8 CA or RA termination

In case of termination of CA operations for any reason whatsoever, DigiCert will provide timely notice and transfer of responsibilities to succeeding entities, maintenance of records, and remedies. Before terminating its own CA activities, DigiCert will where possible take the following steps:

- Provide subscribers of valid certificates with ninety (90) days notice of its intention to cease acting as a CA.
- Revoke all certificates that are still un-revoked or un-expired at the end of the ninety (90)-day notice period without seeking Subscriber's consent.
- Give timely notice of revocation to each affected Subscriber.
- Make reasonable arrangements to preserve its records according to this CPS.
- Reserve its right to provide succession arrangements for the re-issuance of certificates by a successor CA that has all relevant permissions to do so and complies with all necessary rules, while its operation is at least as secure as DigiCert's.

The requirements of this article may be varied by contract, to the extent that such modifications affect only the contracting parties.

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

DigiCert's CA Key Pairs are generated in a Safenet Luna SA device as part of scripted and videotaped key generation ceremony. The Luna SA with Trusted Path Authentication is evaluated to FIPS 140-1 Level 3 and EAL 4+. Activation of the Luna SA requires that it be connected to the PED. Key generation is performed in the Data Center where the cabinet containing the CA system is located. The serial cable on the PED is connected to the serial port on the Luna SA. The key generation ceremony is performed by DigiCert personnel in trusted roles who use the gray, blue and black keys at the appropriate times to perform key generation, certificate generation or other key management operations. Documentation supporting the integrity of the key generation ceremony and other sensitive key operations is stored in a locked safe in DigiCert's business offices and is made available to its auditors for review.

6.1.2 Private key delivery to subscriber

Subscribers are solely responsible for the generation of the private keys used in their certificate requests. DigiCert does not provide key generation, escrow, recovery or backup facilities.

6.1.3 Public key delivery to certificate issuer

Upon making a certificate application, the Subscriber is solely responsible for generating an RSA key pair and submitting it to DigiCert in the form of a PKCS#10 CSR. EV Certificate requests are generated using the key generation facilities available in the Subscriber's webserver software. Delivery of the public key occurs during the same initial enrollment session where the applicant provides all certificate application details.

6.1.4 CA public key delivery to relying parties

DigiCert's CA Public Keys are either signed by roots of other CAs whose Public Keys are embedded in the most predominant web browsers and other trusted software used on the Internet or DigiCert's Public Keys are securely delivered to software providers to serve as trust anchors in commercial browsers and operating system root stores, or may be specified in a certificate validation or path discovery policy file. Relying Parties may also obtain DigiCert's self-signed CA Certificates containing its Public Key from DigiCert's web site or by e-mail.

6.1.5 Key sizes

DigiCert generates and uses a 2048-bit RSA Key with Secure Hash Algorithm version 1 (SHA-1) to sign the EV Certificates and the CRLs that it issues. Subscribers may submit 1024-bit or 2048-bit keys to DigiCert.

6.1.6 Public key parameters generation and quality checking

The Luna SA has a mandatory parameter of 3, 17 or 65537 for the public exponent (e) value used to generate an RSA key pair. The Luna SA's K3 cryptomodule has been validated as conforming to FIPS 186-2 and provides random number generation (http://csrc.nist.gov/cryptval/rng/rngval.html) and on-board creation of 1024-bit and 2048-bit key lengths for RSA public key generation (http://csrc.nist.gov/cryptval/dss/rsaval.html).

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

DigiCert's CA certificates include key usage extension fields to specify the purposes for which the CA Certificate may be used and also to technically limit the functionality of the certificate when used with X.509v3 compliant software. Reliance on key usage extension fields is dependent on correct software implementations of the X.509v3 standard and is outside of the control of DigiCert. Key usages are specified in the Certificate Profile set forth in Section 7.1 and in Appendix A.

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 Federal Information Processing Standard (FIPS) 140-2 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). When following the CWA 14169 standard, a Subscriber's Private Key associated with the Public Key should be protected according to Annex III of the EU Directive 1999/93/EC.

6.2.2 Private key (n out of m) multi-person control

DigiCert's PED keys (secret keys for accessing/activating cryptomodule partitions) are kept under multi-person control which is manually logged for audit purposes in accordance with Section 5.4.1.

The PED Keys are kept in tamper-evident envelopes kept in separate safes. In accordance with Section 5.2.1.2, at least two people are needed to activate the CA private key. Both of the Luna Security Officer (Blue Key) and the Luna Partition Administrator (Black Key) are required. The blue and the black PED keys are protected by a different four-digit PIN known only to the authorized holder of that key. Additionally, pursuant to this CPS the additional presence of a witness or auditor is required to activate and use the CA private keys.

For purposes of disaster recovery, backups of CA private keys are stored on Luna PCMCIA cards, associated PED keys are made under two-person control (see Section 6.2.4), and these CA key materials are stored securely off-site. Re-activation of the backed-up CA private keys (unwrapping) requires the same PED Keys and PCMCIA devices under multi-person control as when performing other sensitive CA private key operations. The separation-of-duties/multi-party control provided by the PED and PED keys prevents a single individual from gaining access to the CA private key.

6.2.3 Private key escrow

DigiCert does not escrow private keys.

6.2.4 Private key backup

DigiCert's CA Private Keys are generated and stored inside the Luna SA module, which has been evaluated to at least FIPS 140 Level 3 and EAL 4+. Where such keys must be transferred to other media for backup and disaster recovery purposes, they are transferred and stored in an encrypted form protected by the PED keys (which have been imprinted with secret keys specific to the Luna SA containing the keys) using the Luna manufacturer's specified PCMCIA token cloning processes. All CA private keys are backed up in accordance with controls described in Section 6.1.1. Backup tokens containing CA private keys are stored securely off-site for backup and disaster recovery purposes.

6.2.5 Private key archival

DigiCert does not archive private keys.

6.2.6 Private key transfer into or from a cryptographic module

See Section 6.2.4.

6.2.7 Private key storage on cryptographic module

See Section 6.2.4.

6.2.8 Method of activating private key

As discussed above, DigiCert's CA private keys are activated by PED Key entry and PIN into the PIN Entry Device (PED) as described in Section 5.2.1.2. The private key is activated by use of the blue PED key and the black PED key during a scripted, videotaped and witnessed key generation or certificate signing ceremony.

Subscribers are solely responsible for protection of their private keys. DigiCert maintains no involvement in the generation, protection or distribution of such keys. DigiCert suggests that its subscribers use a

strong password or equivalent authentication method to prevent unauthorized access and usage of the subscriber private key. *See also* Section 6.4.

6.2.9 Method of deactivating private key

The private key stored on the Luna SA is deactivated via logout procedures on the Luna SA when it is not in use. Root private keys are further deactivated by removing them entirely from the storage partition on the Luna SA device. The Luna SA is never left in an unlocked, unattended state or otherwise left active to unauthorized access. When unattended and active, the Luna SAs are kept locked inside steel cabinets inside the Data Center.

Subscribers should also deactivate their private keys via logout and removal procedures when they are not in use.

6.2.10 Method of destroying private key

Initially, the CA private key can be destroyed by deleting it from all known storage partitions. However, the Luna SA device and associated PCMCIA backup tokens are also zeroized by performing ten (10) consecutive failed login attempts. This reinitializes the device and overwrites all of the data on it with binary zeros. In cases when this 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 retains copies of all Public Keys for archival in accordance with Section 5.5.

6.3.2 Certificate operational periods and key pair usage periods

All certificates and corresponding keys shall have maximum validity periods (not exceeding):

Root CA	25 years
Sub CA	15 years
Subscriber	1 year

Pursuant to Section 5.6, DigiCert voluntarily retires its CA Private Keys from signing subordinate certificates before the periods listed above to accommodate the key changeover process (i.e., the retiring CA Private Key is still used to sign CRLs to provide validation services for certificates issued with that retiring CA Private Key.)

6.4 Activation data

6.4.1 Activation data generation and installation

DigiCert uses its PIN-protected PED Keys and PED device to activate the Luna SA cryptographic module containing its CA private keys. This method has been evaluated as meeting the requirements of FIPS 140-2 Level 3. The Luna SA is held under two-person control as explained in Section 5.2.1.2 and elsewhere in this CPS.

All DigiCert personnel and Subscribers are instructed to use Strong Passwords and to protect PINs and passwords. DigiCert employees are required by policy to create non-dictionary passwords with at least eight characters and one number/special character and mixed case letters.

6.4.2 Activation data protection

Activation data for Luna SAs are protected by keeping the PED keys under separate, role-based physical control and keeping the associated PED key PINs in separate safe deposit boxes under the same separate, role-based control. Access to additional administrative passwords and keys to access the Luna SA are similarly protected. All DigiCert personnel are instructed not to write down their password or ever share it with or disclose it to another individual.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

In accordance with the Guidelines and the AICPA/CICA CA Web Trust Principles, DigiCert has developed, implemented, and maintains an Information Security Policy ("Security Plan") and a program of regular/periodic Risk Assessments that are reasonably designed to:

(1) Protect the confidentiality, integrity, and availability of: (i) all EV Certificate Requests and data related thereto (whether obtained from the Applicant or otherwise) in its possession or control or to which DigiCert has access (“EV Data”), and (ii) the keys, software, processes, and procedures by which DigiCert verifies EV Data, issues EV Certificates, maintains a Repository, and revokes EV Certificates (“EV Processes”);

(2) Protect against any anticipated threats or hazards to the confidentiality, integrity, and availability of the EV Data and EV Processes;

(3) Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any EV Data or EV Processes;

(4) Protect against accidental loss or destruction of, or damage to, any EV Data or EV Processes; and

(5) Comply with all other security requirements applicable to DigiCert by law.

6.5.1 Specific computer security technical requirements

DigiCert's CA computer systems are equipped with Intel 64-bit processors/Intel chip sets. DigiCert's CA servers and support-and-vetting workstations run on Windows 2003, Windows XP Professional, and Linux operating systems. DigiCert's computer systems are configured and hardened using industry best practices. All operating systems require individual identification and authentication for authenticated logins and provide discretionary access control, access control restrictions to services based on authenticated identity, security audit capability and a protected audit record for shared resources, self-protection, and process isolation. All systems are scanned for malicious code and also protected by anti-spyware/anti-virus software.

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 control processes consist of a change control form (electronic) that is processed, logged and tracked for any non-security-related changes to CA systems, equipment and software. Change requests require the approval of at least one Senior Administrator (e.g. the Operations Manager, CA Administrator or System Administrator/ System Engineer) who may not be the same person who submitted the request. In this manner, DigiCert can verify whether a change to the system has been properly evaluated for risk mitigation and authorized by management. 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 generically without identifying the purpose for which the component will be used. All hardware and software are shipped under standard conditions with controls in place 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 to provide CA services are developed in-house or by consultants using standard software development methodologies, 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, discussed above. Updates of equipment or 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.

6.6.2 Security management controls

DigiCert has mechanisms in place to control and monitor the security-related configurations of its CA systems. Change control processes consist of a change control form (electronic) that is processed, logged and tracked for any security-related changes to CA systems, firewalls, routers, software and other access controls. In this manner, DigiCert can verify whether a change to the system has been properly evaluated for risk mitigation and authorized by management.

6.6.3 Life cycle security controls

No stipulation.

6.7 Network security controls

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 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. It is DigiCert's security policy 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. All firewall configurations and changes thereto are documented, authorized, tested and implemented in accordance with change management policies and procedures. 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

See Section 5.5.5.

7. CERTIFICATE, CRL, AND OCSP PROFILES

Information for interpreting the following Certificate 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. X.509v3 allows a CA to add certain certificate extensions to the basic certificate structure. DigiCert use a number of certificate extensions for the purposes intended by X.509v3 as per Amendment 1 to ISO/IEC 9594-8, 1995.

7.1 Certificate profile

7.1.1 Version number(s)

All certificates are X.509 version 3 certificates.

7.1.2 Certificate extensions

See Appendix A.

7.1.3 Algorithm object identifiers

See Appendix A.

7.1.4 Name forms

See Appendix A and Section 3.1.

7.1.5 Name constraints

No stipulation.

7.1.6 Certificate policy object identifier

An object identifier (OID) is a number unique within a specific domain that allows for the unambiguous identification of a policy, including a Certificate Policy and/or Certification Practice Statement, such as this CPS. The CP OIDs that incorporate this CPS into a given certificate by reference (which identify that this CPS applies to a given digital certificate containing the OID) are listed in Section 1.2 and in the Certificate Profile attached as Appendix A.

7.1.7 Usage of Policy Constraints extension

Not applicable.

7.1.8 Policy qualifiers syntax and semantics

DigiCert certificates include a brief statement in the Policy Qualifier field of the Certificate Policy extension to put all potential Relying Parties on notice of the limitations of liability and other terms and conditions on the use of the certificate, including those contained in this CPS, which are incorporated by reference into the certificate. *See* Appendix A.

7.1.9 Processing semantics for the critical Certificate Policies extension

No stipulation.

7.2 CRL profile

7.2.1 Version number(s)

DigiCert issues version two (2) CRLs (i.e. populated with integer "1"). CRLs conform to RFC 3280 and contain the basic fields listed below:

Version
Issuer Signature Algorithm (sha-1WithRSAEncryption {1 2 840 113549 1 1 5})
Issuer Distinguished Name (DigiCert)
thisUpdate (UTC format)
nextUpdate (UTC format – thisUpdate plus 24 hours)
Revoked certificates list
    Serial Number
    Revocation Date (see CRL entry extension for Reason Code below)
Issuer's Signature

7.2.2 CRL and CRL entry extensions

CRL Number (monotonically increasing integer - never repeated)
Authority Key Identifier (same as Authority Key Identifier in certificates issued by CA)
CRL Entry Extensions
    Invalidity Date (UTC - optional)
    Reason Code (optional)

7.3 OCSP profile

Reserved for future use.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The practices specified in this CPS have been designed to meet or exceed the requirements of generally accepted and developing industry standards including the AICPA/CICA WebTrust Extended Validation Program for Certification Authorities ("WebTrust EV Program for CAs"), ISO 21188, and other industry standards related to the operation of CA's.

8.1 Frequency or circumstances of assessment

An annual audit is performed by an independent external auditor to assess DigiCert's compliance with WebTrust EV Program for CAs criteria.

8.2 Identity/qualifications of assessor

(1) Qualifications and experience. Auditing must be the individual's or group'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.
(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 the like, as well as Internet security issues (such as management of a security perimeter), operations of secure data centers, personnel controls, and operational risk management.
(3) Rules and standards: The individual or group 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) Disinterest: The firm must have no financial interest, business relationship, or course of dealing that could foreseeably create a significant bias for or against DigiCert.

8.3 Assessor's relationship to assessed entity

In addition to the foregoing prohibition on conflicts of interest, the assessor shall have a contractual relationship with DigiCert for the performance of the audit, but otherwise, shall be independent. The assessor shall maintain a high standard of ethics designed to ensure impartiality and the exercise of independent professional judgment, subject to disciplinary action by its licensing body.

8.4 Topics covered by assessment

Topics covered by the annual WebTrust EV Program for CAs audit include but are not limited to DigiCert's CA business practices disclosure (i.e., this CPS), the service integrity of DigiCert's CA operations, the environmental controls that DigiCert implements to ensure a trustworthy system 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, or any other contractual obligations related to the CA services described herein, DigiCert shall develop a plan to cure such noncompliance, subject to the approval of the DigiCert Policy Authority and any third party to whom DigiCert is legally obligated to satisfy. In the event DigiCert fails to take appropriate action in response to the report, then the DigiCert Policy Authority may instruct DigiCert's Operations Manager to revoke the certificates affected by such non-compliance.

8.6 Communication of results

The results of any inspection or audit are reported to DigiCert management, acting as the DigiCert Policy Authority, and any appropriate entities, as may be required by law, regulation or agreement. At its option, DigiCert will provide interested parties with the letter containing the attestation of management and its auditor's letter concerning the effectiveness of controls. Otherwise, all audit information will be considered confidential business information in accordance with Section 9.3.

8.7 Self-Audits

During the period in which it issues EV Certificates, DigiCert will control its service quality by performing ongoing self audits against a randomly selected sample of at least three percent (3%) of the EV Certificates it has issued in the period beginning immediately after the last sample was taken.

9. OTHER BUSINESS AND LEGAL MATTERS

This part describes the legal representations, warranties and limitations associated with each of DigiCert's digital certificates.

9.1 Fees

9.1.1 Certificate issuance or renewal fees

DigiCert charges Subscriber fees for certificate issuance and renewal. Such fees are detailed on its web site (http://www.digicert.com). DigiCert retains its right to effect changes to such fees. DigiCert customers will be suitably advised of price amendments as detailed in relevant customer agreements.

9.1.2 Certificate access fees

DigiCert reserves the right to establish and charge a reasonable fee for access to its database of certificates.

9.1.3 Revocation or status information access fees

DigiCert does not charge fees for the revocation of a certificate or for a Relying Party to check the validity status of a DigiCert issued certificate through the use of Certificate Revocation Lists. DigiCert reserves the right to 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 charges the credit card submitted with Applicant's request for an EV Certificate. Applicants agree that the applicable certificate issuance fee includes a non-refundable application processing fee of $99. If Applicant's request is canceled or rejected, DigiCert will refund the certificate issuance fee minus the application processing fee. DigiCert will apply the $99 application processing fee to the Applicant's account for the purchase of a different type of certificate from DigiCert. After issuance, DigiCert offers a 30-day refund policy. During a 30-day period (beginning when a certificate is first issued) the Subscriber may request a refund for the refundable portion of their certificate. Under such circumstances, the original certificate may be revoked and a refund provided to the applicant. DigiCert is not obliged to provide a refund for a certificate after the 30-day reissue policy period has expired.

9.2 Financial responsibility

9.2.1 Insurance coverage

DigiCert carries at least $2 million in Commercial General Liability insurance coverage and Professional Liability/Errors & Omissions insurance, with policy limits of at least $5 million in coverage, including coverage for (i) claims for damages arising out of an act, error, or omission, unintentional breach of contract, or neglect in issuing or maintaining EV Certificates, and (ii) claims for damages arising out of infringement of the proprietary rights of any third party (excluding copyright, and trademark infringement), and 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

Subscribers should refer to the Subscriber Agreement that they have with DigiCert.
Relying Parties should refer to the Relying Party Agreement. Both are located at:
http://www.digicert.com/ssl-cps-repository.htm.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

DigiCert keeps the following types of information confidential and maintains reasonable controls to prevent the exposure of such records to non-trusted personnel.

- All private keys
- Any activation data used to access private keys or gain access to the CA system
- Any business continuity, incident response, contingency, and disaster recovery plans
- Any other security practices, measures, mechanisms, plans, or procedures used to protect the confidentiality, integrity or availability of information
- Any information held by DigiCert as private information in accordance with Section 9.4
- Any transactional, audit log and archive record identified in Section 5.4 or 5.5, including certificate application records and documentation submitted in support of certificate applications whether successful or rejected.
- 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

Subscriber application data identified herein as being published in a digital certificate is considered public and not within the scope of confidential information. Subscribers acknowledge that revocation data of all certificates issued by the DigiCert CA is public information and is periodically published every 24 hours at the DigiCert repository.

9.3.3 Responsibility to protect confidential information

DigiCert observe applicable rules on the protection of personal data deemed by law or the DigiCert privacy policy (see Section 9.4 of this CPS) to be confidential.

9.4 Privacy of personal information

9.4.1 Privacy plan

DigiCert has implemented a privacy policy, which is in compliance with this CPS. The DigiCert privacy policy is published at http://www.digicert.com/digicert-privacy-policy.htm

9.4.2 Information treated as private

Personal information about an individual that is not publicly available in the contents of a certificate or CRL is considered private.

9.4.3 Information not deemed private

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

9.4.4 Responsibility to protect private information

Each party shall protect the confidentiality of private information that is in its possession, custody or control with the same degree of care that it exercises with respect to its own information of like import, but in no event less than reasonable care, and shall use appropriate safeguards and otherwise exercise reasonable precautions to prevent the unauthorized disclosure of private information.

9.4.5 Notice and consent to use private information

A party may use private information with the subject's express written consent or as required by applicable law or court order.

9.4.6 Disclosure pursuant to judicial or administrative process

DigiCert shall not release any confidential information, unless as otherwise required by law, without an authenticated, reasonably specific request by an authorized party specifying:

- The party to whom DigiCert owes a duty to keep information confidential.
- The party requesting such information.
- A court order, if any.

9.4.7 Other information disclosure circumstances

All personnel in trusted positions handle all information in strict confidence, including those requirements of US and European law concerning the protection of personal data.

9.5 Intellectual property rights

DigiCert, its strategic partners, and other business associates, each own all their respective intellectual property rights associated with their databases, web sites, DigiCert digital certificates and any other publication originating from DigiCert including this CPS.

The trademarks “DigiCert” and “DigiCertSSL” are registered trademarks of DigiCert, Inc. DigiCert may have other trade and service marks that have not been registered, but that nonetheless are and shall remain the property of DigiCert.

Certificates are the exclusive property of DigiCert. DigiCert gives permission to reproduce and distribute certificates on a non-exclusive, royalty-free basis, provided that they are reproduced and distributed in full. DigiCert reserves the right to revoke the certificate at any time and at its sole discretion.

Private and public keys are the property of the Subscribers who rightfully issue and hold them.

All secret shares (distributed elements) of the DigiCert private keys remain the respective property of DigiCert.

9.6 DigiCert Representations and Warranties

DigiCert makes the following EV Certificate Warranties solely to Certificate Subscribers, Certificate Subjects, Application Software Vendors with whom DigiCert has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Vendors, and all Relying Parties that actually rely on such EV Certificate during the period when it is Valid, that it followed the requirements of the Guidelines and this CPS in issuing the EV Certificate and in verifying the accuracy of the information contained in the EV Certificate (“EV Certificate Warranties”). Subject to the limitations below, the EV Certificate Warranties specifically include, but are not limited to, warranties that:

(A) Legal Existence: DigiCert has confirmed in accordance with the Guidelines that, as of the date the EV Certificate was issued, the Subject named in the EV Certificate legally exists as a valid organization or entity in the Jurisdiction of Incorporation;

(B) Identity: DigiCert has confirmed that, as of the date the EV Certificate was issued, the legal name of the Subject named in the EV Certificate matches the name on the official government records of the Incorporating Agency in the Subject’s Jurisdiction of Incorporation, and if an assumed name is also included, that the assumed name is properly registered by the Subject in the jurisdiction of its Place of Business;

(C) Right to Use Domain Name: DigiCert has taken all steps reasonably necessary to verify that, as of the date the EV Certificate was issued, the Subject named in the EV Certificate has the exclusive right to use the domain name listed in the EV Certificate;

(D) Authorization for EV Certificate: DigiCert has taken all steps reasonably necessary to verify that the Subject named in the EV Certificate has authorized the issuance of the EV Certificate;

(E) Accuracy of Information: DigiCert has taken all steps reasonably necessary to verify that all of the other information in the EV Certificate is accurate, as of the date the EV Certificate was issued;

(F) Subscriber Agreement: The Subject named in the EV Certificate has entered into a legally valid and enforceable Subscriber Agreement with DigiCert that satisfies the requirements of the Guidelines;

(G) Status: DigiCert will follow the requirements of the Guidelines and maintain a 24 x 7 online-accessible Repository with current information regarding the status of the EV Certificate as Valid or revoked; and

(H) Revocation: DigiCert will follow the requirements of the Guidelines and revoke the EV Certificate upon the occurrence of any revocation event as specified in the Guidelines.

DigiCert makes reasonable efforts to independently confirm the information provided by the Applicant for an EV Certificate, including confirmation that Verified Legal Opinions and Verified Accountant Letters are authentic and provided by attorneys or accountants licensed in the Applicant’s jurisdiction. The foregoing warranties and representations are limited, however, to DigiCert’s compliance with the Guidelines (e.g.,

where DigiCert has relied on erroneous information provided in an attorney's opinion or accountant's letter that is checked in accordance with the Guidelines).

Except as it may have otherwise been stated in relation to Qualified Certificates issued pursuant to the requirements of the European Directive 99/93, DigiCert:

- Does not warrant the accuracy, authenticity, completeness or fitness of any unverified information contained in certificates or otherwise compiled, published, or disseminated by or on behalf of DigiCert except as it may be stated in the relevant product description contained in this CPS.
- Shall incur no liability for representations of information contained in a certificate except as it may be stated in the relevant product description in this CPS.
- Does not warrant the quality, functions or performance of any software or hardware device.
- Shall have no liability if it cannot execute the revocation of a certificate for reasons outside its own control.

9.6.2 RA representations and warranties

Not applicable

9.6.3 Subscriber representations and warranties

The EV Authorization Letter references the Subscriber Agreement and is signed by the Contract Signer. The EV Authorization Letter contains provisions meeting the requirement that the Subscriber Agreement be signed by an authorized Contract Signer acting on behalf of the Applicant in accordance with Section 20 of the Guidelines for the initial EV Certificate Request. Subsequent separate, online Subscriber Agreements are used for each or multiple future EV Certificate Requests and resulting EV Certificates.

Subsequent EV Certificates are clearly covered by the Subscriber Agreement through the language of the EV Authorization Letter, which states, "Applicant/Organization hereby appoints the following employee(s) as authorized representative(s) to act as "Contract Signer" to represent Applicant/Organization and bind it with respect to Subscriber Agreement(s) and related documents. This authorization applies to both written and electronic signatures made by the Contract Signer. … Applicant/Organization hereby agrees to be bound by all Certificate requests, Subscriber Agreements, and related documents submitted to DigiCert, Inc. by the individuals listed above."

As part of the standard Subscriber Agreement agreed to by all Subscribers, the following commitments and warranties are made for the express benefit of DigiCert and all Relying Parties and Application Software Vendors:

(A) Accuracy of Information: An obligation and warranty to provide accurate and complete information at all times to DigiCert, both in the EV Certificate Request and as otherwise requested by DigiCert in connection with the issuance of the EV Certificate(s) to be supplied by DigiCert;

(B) Protection of Private Key: An obligation and warranty by the subscriber or a subcontractor (e.g. hosting provider) to take all reasonable measures necessary to maintain sole control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested EV Certificate(s) (and any associated access information or device – e.g., password or token);

(C) Acceptance of EV Certificate: An obligation and warranty that it will not install and use the EV Certificate(s) until it has reviewed and verified the accuracy of the data in each EV Certificate;

(D) Use of EV Certificate: An obligation and warranty to install the EV Certificate only on the server accessible at the domain name listed on the EV Certificate, and to use the EV Certificate solely in compliance with all applicable laws, solely for authorized company business, and solely in accordance with the Subscriber Agreement;

(E) Reporting and Revocation Upon Compromise: An obligation and warranty to promptly cease using an EV Certificate and its associated Private Key, and promptly request that DigiCert revoke the EV Certificate, in the event that: (a) any information in the EV Certificate is or becomes incorrect or inaccurate, or (b) there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key listed in the EV Certificate; and

(F) Termination of Use of EV Certificate: An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key listed in an EV Certificate upon expiration or revocation of that EV Certificate.

Without limiting other Subscriber obligations stated in this CPS, Subscribers are solely liable for any misrepresentations they make in certificates to third parties that reasonably rely on the representations contained therein.

Upon accepting a certificate the Subscriber represents to DigiCert and to Relying Parties that at the time of acceptance and until further notice:

- Transactions effectuated using the private key corresponding to the public key included in the certificate are the acts of the Subscriber and that the certificate has been accepted and is properly operational at that time and until further notice to DigiCert.
- The Subscriber retains control of the Subscriber's private key, uses a trustworthy system, and takes reasonable precautions to prevent its loss, disclosure, modification, or unauthorized use and that no unauthorized person has ever had access to the Subscriber's private key.
- All representations made by the Subscriber to DigiCert regarding the information contained in the certificate are accurate and true to the best of the Subscriber's knowledge or to the extent that the Subscriber receives notice of such information, the Subscriber shall act promptly to notify DigiCert of any material inaccuracies contained in the certificate.
- The certificate is used exclusively for authorized and legal purposes, consistent with this CPS, and that the Subscriber will use the certificate only in conjunction with the entity named in the organization field of the certificate
- The Subscriber agrees with the terms and conditions of this CPS and other agreements and policy statements of DigiCert.
- The Subscriber abides by the laws applicable in his/her country or territory including those related to intellectual property protection, fair trade practices and computer fraud and abuse,
- The Subscriber complies with all export laws and regulations for dual usage goods as may be applicable.

9.6.4 Relying party representations and warranties

A Relying Party accepts that in order to reasonably rely on a DigiCert certificate, the Relying Party must:

- Make reasonable efforts to acquire sufficient knowledge on using digital certificates and PKI.
- Study the limitations to the usage of digital certificates and be aware through the Relying Party Agreement of the limitations of liability of DigiCert for reliance on a DigiCert-issued certificate.
- Read and agree with the terms of the DigiCert Relying Party Agreement.
- Verify the DigiCert certificates by referring to the relevant CRL and also the CRL's of any intermediate CA or root CA as available through DigiCert's repository.
- Trust a DigiCert certificate only if it is valid and has not been revoked or has expired.
- Take any other reasonable steps to minimize the risk of relying on a digital signature created by an invalid, revoked, expired or rejected certificate; and finally,
- Rely on a DigiCert certificate, only as may be reasonable under the circumstances, given:
  - any legal requirements for the identification of a party, the protection of the confidentiality or privacy of information, or the legal enforceability of the transaction in accordance with any laws that may apply;
  - all facts listed in the Certificate, or of which the Relying Party has or should have notice, including this CPS;
  - the economic value of the transaction or communication, if applicable;
  - the potential losses or damage which might be caused by an erroneous identification or a loss of confidentiality or privacy of information in the application, transaction or communication;
  - the applicability of the laws of a particular jurisdiction, including the jurisdiction specified in an agreement with the Subscriber or in this CPS;

- the Relying Party's previous course of dealing with the Subscriber, if any;
- usage of trade, including experience with computer-based methods of trade; and
- any other indicia of reliability or unreliability, or other facts of which the Relying Party knows or has notice, pertaining to the Subscriber and/or the application, communication or transaction.

9.6.5 Representations and Warranties of Other Participants

Not applicable.

9.7 Disclaimers of warranties

DigiCert disclaims all warranties and obligations of any type, including any warranty of fitness for a particular purpose, and any warranty of the accuracy of unverified information provided, save as contained herein and as cannot be excluded at law. In no event and under no circumstances (except for fraud or willful misconduct) shall DigiCert be liable for any or all of the following and the results thereof:

- Any indirect, incidental or consequential damages.
- Any costs, expenses, or loss of profits.
- Any death or personal injury.
- Any loss of data.
- Any other indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, performance or non-performance of certificates or digital signatures.
- Any other transactions or services offered within the framework of this CPS.
- Any other damages except for those due to reliance, on the information featured on a certificate, or on the verified information in a certificate.
- Any liability incurred in this case or any other case if the fault in this verified information is due to fraud or willful misconduct of the applicant.
- Any liability that arises from the usage of a certificate that has not been issued or used in conformance with this CPS.
- Any liability that arises from the usage of a certificate that is not valid.
- Any liability that arises from usage of a certificate that exceeds the limitations in usage and value and transactions stated upon it or in this CPS.
- Any liability that arises from security, usability, integrity of products, including hardware and software a Subscriber uses.
- Any liability that arises from compromise of a Subscriber's private key.

9.8 Limitations of liability

DigiCert certificates may only be used in connection with data transfer and transactions having a US dollar (US$) value of less than $1 million. In no event and under no circumstances (except for fraud or willful misconduct) will the aggregate liability of DigiCert, whether jointly or severally, to all parties including without any limitation a Subscriber, an applicant, a recipient, or a Relying Party for all digital signatures and transactions related to such certificate exceed $1 million.

9.9 Indemnities

By accepting or using a certificate, each Subscriber and Relying Party agrees to indemnify and hold DigiCert, as well as any of its respective parent companies, subsidiaries, directors, officers, employees, agents, and contractors harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind, including reasonable attorneys' fees, that DigiCert, and/or the above mentioned parties may incur, that are caused by the use or publication of a certificate, and that arises from that party's: (i) misrepresentation or omission of material fact in order to obtain or use a Certificate, whether or not such misrepresentation or omission was intentional; (ii) violation of the Subscriber Agreement, Relying Party Agreement, this CPS, or any applicable law; (iii) compromise or unauthorized use of a Certificate or Private Key caused by the negligence of that party and not by DigiCert (unless prior to such unauthorized use DigiCert has received an authenticated request to revoke the Certificate); or (iv) misuse of the Certificate or Private Key.

9.10 Term and termination

9.10.1 Term

This CPS and any amendments hereto shall become effective upon publication in the Repository and shall remain in effect perpetually until terminated in accordance with this Section 9.10.

9.10.2 Termination

This CPS as amended from time to time shall remain in force until it is replaced by a new version or is otherwise terminated in accordance with this Section 9.10.

9.10.3 Effect of termination and survival

The conditions and effect resulting from termination of this document will be communicated via the DigiCert Repository (http://www.digicert.com/ssl-cps-repository.htm) upon termination. That communication will outline the provisions that may survive termination of this CPS and remain in force. The responsibilities for protecting business confidential and private personal information shall survive termination, and the terms and conditions for all existing Certificates shall remain valid for the remainder of the Validity Periods of such Certificates.

9.11 Individual notices and communications with participants

DigiCert accepts notices related to this CPS by means of digitally signed messages or in paper form addressed to the locations specified in Section 2.2 of this CPS. Upon receipt of a valid, digitally signed acknowledgment of receipt from DigiCert, the sender of the notice shall deem their communication effective. The sender must receive such acknowledgment within five (5) days, or else written notice must then be sent in paper form through a courier service that confirms delivery or via certified or registered mail, postage prepaid, return receipt requested, addressed to the street address specified in Section 2.2.

9.12 Amendments

9.12.1 Procedure for amendment

Revisions not denoted “significant” shall be those deemed by the DigiCert Policy Authority to have minimal or no impact on Subscribers and Relying Parties using certificates and CRL’s issued by DigiCert. Such revisions may be made without notice to users of this CPS and without changing the version number of this CPS. Controls are in place to reasonably ensure that the DigiCert CPS is not amended and published without the prior authorization of the DigiCert Policy Authority.

9.12.2 Notification mechanism and period

DigiCert will notify all interested persons of proposed changes, the final date for receipt of comments, and the proposed effective date of proposed changes on its Web site. There is no fixed notice and comment period. Editorial and typographical corrections, changes to contact details and other minor changes that do not materially impact the parties may be changed without notice and are not subject to the notification requirements herein.

9.12.3 Circumstances under which OID must be changed

If a change in DigiCert's Certificate Policy or Certification Practices is determined by the DigiCert Policy Authority to warrant a change in the currently specified OID for a particular type of certificate, then the revised version of this CPS will also contain a revised OID for that type of certificate.

9.13 Dispute resolution provisions

Before resorting to any dispute resolution mechanism including adjudication or any type of Alternative Dispute Resolution (including without exception mini-trial, arbitration, mediation, umpire, binding expert’s advice, co-operation monitoring and normal expert’s advice) the parties agree to notify DigiCert of the dispute with a view to seek dispute resolution.

9.14 Governing law

This CPS is governed by, and construed in accordance with the law of the State of Utah. This choice of law is made to ensure uniform interpretation of this CPS, regardless of the place of residence or place of use of DigiCert digital certificates or other products and services. Utah law applies in all of DigiCert's commercial or contractual relationships in which this CPS may apply or quoted implicitly or explicitly in relation to DigiCert products and services where DigiCert acts as a provider, supplier, beneficiary receiver or otherwise.

Each party, including DigiCert, Subscribers and Relying Parties, irrevocably agree that a tribunal (court or arbitration body) located in Utah shall have exclusive jurisdiction to hear and decide any suit, action or proceedings, and to settle any disputes, which may arise out of or in connection with this CPS or the provision of DigiCert PKI services.

9.15 Compliance with applicable law

This CPS shall be subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees and orders including but not limited to restrictions on exporting or importing software, hardware or technical information.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

This CPS shall be interpreted consistently within the boundaries of business customs, commercial reasonableness under the circumstances, and intended usage of the product or service described herein. In interpreting this CPS the parties shall also take into account the international scope and application of the services and products of DigiCert as well as the principle of good faith as it is applied in commercial transactions.

The headings, subheadings, and other captions in this CPS are intended for convenience and reference only and shall not be used in interpreting, construing, or enforcing any of the provisions of this CPS.

Appendices and definitions to this CPS are for all purposes an integral and binding part of the CPS. If/when this CPS conflicts with other rules, guidelines, or contracts, this CPS, dated 14 July 2006, shall prevail and bind the Subscriber and other parties. If there is any conflict between the sections of this CPS and any other document that relate to DigiCert, then the sections benefiting DigiCert and preserving DigiCert’s best interests, at DigiCert’s sole determination, shall prevail and bind the applicable parties.

9.16.2 Assignment

Parties to this CPS may not assign any of their rights or obligations under this CPS or applicable agreements without the written consent of DigiCert.

9.16.3 Severability

If any provision of this CPS or the application thereof, is for any reason and to any extent found to be invalid or unenforceable, the remainder of this CPS (and the application of the invalid or unenforceable provision to other persons or circumstances) shall remain in full force and effect and shall be interpreted in such manner as to implement the original intention of the parties to the fullest extent possible.

Each and every provision of this CPS that provides for a limitation of liability, disclaimer of or limitation upon any warranties or other obligations, or exclusion of damages is intended to be severable and independent of any other provision and is to be enforced as such.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

DigiCert reserves the right to seek indemnification and attorneys' fees from any party related to that party's conduct described in Section 9.9. Except where an express time frame is set forth in this CPS, no delay or omission by any party to exercise any right, remedy or power it has under this CPS shall impair or be construed as a waiver of such right, remedy or power. A waiver by any party of any breach or covenant in this CPS shall not be construed to be a waiver of any other or succeeding

breach or covenant. Bilateral agreements between DigiCert and the parties to this CPS may contain additional provisions governing enforcement.

9.16.5 Force Majeure

DIGICERT INCURS NO LIABILITY IF IT IS PREVENTED, FORBIDDEN OR DELAYED FROM PERFORMING, OR OMITS TO PERFORM, ANY ACT OR REQUIREMENT BY REASON OF: ANY PROVISION OF ANY APPLICABLE LAW, REGULATION OR ORDER; CIVIL, GOVERNMENTAL OR MILITARY AUTHORITY; THE FAILURE OF ANY ELECTRICAL, COMMUNICATION OR OTHER SYSTEM OPERATED BY ANY OTHER PARTY OVER WHICH IT HAS NO CONTROL; FIRE, FLOOD, OR OTHER EMERGENCY CONDITION; STRIKE; ACTS OF TERRORISM OR WAR; ACT OF GOD; OR OTHER SIMILAR CAUSES BEYOND ITS REASONABLE CONTROL AND WITHOUT ITS FAULT OR NEGLIGENCE.

9.17 Other provisions

This CPS shall be binding upon the successors, executors, heirs, representatives, administrators, and assigns, whether express, implied, or apparent, of the parties that this CPS applies to. The rights and obligations detailed in this CPS are assignable by the parties, by operation of law (including as a result of merger or a transfer of a controlling interest in voting securities) or otherwise, provided such assignment is undertaken consistent with this CPS articles on termination or cessation of operations, and provided that such assignment does not effect a novation of any other debts or obligations the assigning party owes to other parties at the time of such assignment.

Appendix A

Certificate Profiles

1. DigiCert's High Assurance EV Root CA

Field	Value
Version	V3 (2)
Serial Number	Unique number
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Issuer Distinguished Name	Unique X.500 CA DN. CN = DigiCert High Assurance EV Root CA OU = www.digicert.com O = DigiCert Inc C = US
Validity Period	25 years expressed in UTC format
Subject Distinguished Name	CN = DigiCert High Assurance EV Root CA OU = www.digicert.com O = DigiCert Inc C = US
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Extension	**Value**
Authority Key Identifier	c=no; b1 3e c3 69 03 f8 bf 47 01 d4 98 26 1a 08 02 ef 63 64 2b c3
Subject Key Identifier	c=no; b1 3e c3 69 03 f8 bf 47 01 d4 98 26 1a 08 02 ef 63 64 2b c3
Key Usage	c=yes; Digital Signature, Certificate Signing , Off-line CRL Signing, CRL Signing (86)
Extended Key Usage	Not present
Certificate Policies	Not present
Basic Constraints	c=yes; cA=True; path length constraint is absent

2. DigiCert's High Assurance EV CA-1 Certificate

Field	Value
Version	V3 (2)
Serial Number	Unique number
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Issuer Distinguished Name	Unique X.500 CA DN. CN = DigiCert High Assurance EV Root CA OU = www.digicert.com O = DigiCert Inc C = US
Validity Period	15 years expressed in UTC format
Subject Distinguished Name	CN = DigiCert High Assurance EV CA-1 OU = www.digicert.com O = DigiCert Inc C = US
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Extension	**Value**
Authority Key Identifier	c=no; b1 3e c3 69 03 f8 bf 47 01 d4 98 26 1a 08 02 ef 63 64 2b c3
Subject Key Identifier	c=no; 4c 58 cb 25 f0 41 4f 52 f4 28 c8 81 43 9b a6 a8 a0 e6 92 e5
Key Usage	c=yes; Digital Signature, Certificate Signing , Off-line CRL Signing, CRL Signing (86)
Extended Key Usage	c=no; Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2) Code Signing (1.3.6.1.5.5.7.3.3) Secure Email (1.3.6.1.5.5.7.3.4) Time Stamping (1.3.6.1.5.5.7.3.8)
Certificate Policies	c=no; Certificate Policies; {2.16.840.1.114412.2.1} [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.digicert.com/ssl-cps-repository.htm [1,2] Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text= Any use of this Certificate constitutes acceptance of the DigiCert EV CPS and the Relying Party Agreement which limit liability and are incorporated herein by reference.
Basic Constraints	c=yes; cA=True; path length constraint is absent
Authority Information Access	c=no; Access Method= - Id-ad-ocsp (On-line Certificate Status Protocol - 1.3.6.1.5.5.7.48.1); URL =https://ocsp.digicert.com
CRL Distribution Points	c = no; CRL HTTP URL =http://crl3.digicert.com/DigiCertHighAssuranceEVRootCA.crl CRL HTTP URL =http://crl4.digicert.com/DigiCertHighAssuranceEVRootCA.crl

3. DigiCert End Entity EV Certificates

Field	Value	Comments
Version	V3 (2)	
Serial Number	Unique number	
Issuer Signature Algorithm	sha-1WithRSAEncryption (1.2.840.113549.1.1.5)	
Issuer Distinguished Name	Unique X.500 CA DN. CN = DigiCert High Assurance EV CA-[X] OU = www.digicert.com O = DigiCert Inc C = US	Where [X] is an integer that identifies the EV CA that issued the certificate.
Validity Period	1 year expressed in UTC format	
Subject Distinguished Name		
Organization Name	subject:organizationName (2.5.4.10)	This field MUST contain the Subject's full legal organization name as listed in the official records of the Incorporating Agency in the Subject's Jurisdiction of Incorporation. In addition, an assumed name or d/b/a name used by the Subject MAY be included at the beginning of this field, provided that it is followed by the full legal organization name in parenthesis. If the combination of the full legal organization name and the assumed or d/b/a name exceeds 64 characters as defined by RFC 3280, only the full legal organization name will be used.
Common Name	subject:commonName (2.5.4.3) cn = Common name	SubjectAlternativeName:dNSName is found below in this table. This field MUST contain one or more host domain name(s) owned or controlled by the Subject and to be associated with Subject's publicly accessible server. Such server may be owned and operated by the Subject or another entity (e.g., a hosting service). Wildcard certificates are not allowed for EV certificates.
City or Town of Incorporation	subject:jurisdictionOfIncorporationLocalityName (1.3.6.1.4.1.311.60.2.1.1)	ASN.1 - X520LocalityName as specified in RFC 3280 Full name of Jurisdiction of Incorporation for an Incorporating Agency at the city or town level, including both country and state or province information as follows.
State/Province of	subject:jurisdictionOfIncorporationS	ASN.1 -

Incorporation	tateOrProvinceName (1.3.6.1.4.1.311.60.2.1.2)	X520StateOrProvinceName as specified in RFC 3280 Full name of Jurisdiction of Incorporation for an Incorporating Agency at the state or province level, including country information as follows, but not city or town information above.
Country of Incorporation	subject:jurisdictionOfIncorporationCountryName (1.3.6.1.4.1.311.60.2.1.3)	ASN.1 - X520countryName as specified in RFC 3280 Jurisdiction of Incorporation for an Incorporating Agency at the country level would include country information but would not include state or province or city or town information. Country information MUST be specified using the applicable ISO country code. Optionally, qcStatements extension for EU countries per RFC 3739.
Registration Number	Subject:serialNumber (2.5.4.5)	This field MUST contain the unique Registration Number assigned to the Subject by the Incorporating Agency in its Jurisdiction of Incorporation (for Private Organization Subjects only)
Number & street (optional)	subject:streetAddress (2.5.4.9)	
City or town	subject:localityName (2.5.4.7)	
State or province (if any)	subject:stateOrProvinceName (2.5.4.8)	
Country	subject:countryName (2.5.4.6)	
Postal code (optional)	subject:postalCode (2.5.4.17)	
Subject Public Key Information	1024 or 2048-bit RSA key modulus, rsaEncryption (1.2.840.113549.1.1.1)	
Issuer's Signature	sha-1WithRSAEncryption (1.2.840.113549.1.1.5)	
Extension	**Value**	
Authority Key Identifier	c=no; Octet String – Same as Issuer's	4c 58 cb 25 f0 41 4f 52 f4 28 c8 81 43 9b a6 a8 a0 e6 92 e5
Subject Key Identifier	c=no; Octet String – Same as calculated by CA from PKCS#10	
Key Usage	c=yes; Digital Signature, Key Encipherment (a0)	
Extended Key Usage	c=no; Server Authentication (1.3.6.1.5.5.7.3.1)	

	Client Authentication (1.3.6.1.5.5.7.3.2)	
Certificate Policies	Same as Issuer's	
Subject Alternative Name	c=no; DNS = FQDN of Device (e.g., domain.com)	
Authority Information Access	c=no; Access Method= - Id-ad-ocsp (On-line Certificate Status Protocol - 1.3.6.1.5.5.7.48.1); URL =https://ocsp.digicert.com	
CRL Distribution Points	c = no; CRL HTTP URL = http://crl3.digicert.com/DigiCertHighAssuranceEVCA-[X].crl CRL HTTP URL = http://crl4.digicert.com/DigiCertHighAssuranceEVCA-[X].crl	Where [X] is an integer that identifies the EV CA that issued the certificate.