DigiCert

Certification Practice Statement for

Extended Validation Certificates

[redacted]

DigiCert, Inc.
Version 1.0.4
May 29, 2009

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

TABLE OF CONTENTS

1. INTRODUCTION 1
1.1 Overview 1
1.2 Document name and identification 2
1.3 PKI participants 2
1.4 Certificate usage 4
1.5 Policy administration 4
1.6 Definitions and acronyms 5
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES 8
2.1 Repositories 8
2.2 Publication of certification information 8
2.3 Time or frequency of publication 8
2.4 Access controls on repositories 8
3. IDENTIFICATION AND AUTHENTICATION 9
3.1 Naming 9
3.2 Initial identity validation 9
3.3 Identification and authentication for re-key requests 17
3.4 Identification and authentication for revocation request 18
4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 18
4.1 Certificate Application 18
4.2 Certificate application processing 18
4.3 Certificate issuance 20
4.4 Certificate acceptance 21
4.5 Key pair and certificate usage 21
4.6 Certificate renewal 22
4.7 Certificate re-key 22
4.8 Certificate modification 23
4.9 Certificate revocation and suspension 23
4.10 Certificate status services 26
4.11 End of subscription 26
4.12 Key escrow and recovery 26
5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 26
5.1 Physical controls 26
5.2 Procedural controls 27
5.3 Personnel controls 28
5.4 Audit logging procedures 29
5.5 Records archival 30
5.6 Key changeover 32
5.7 Compromise and disaster recovery 32
5.8 CA or RA termination 33
6. TECHNICAL SECURITY CONTROLS 33
6.1 Key pair generation and installation 33
6.2 Private Key Protection and Cryptographic Module Engineering Controls 34
6.3 Other aspects of key pair management 36
6.4 Activation data 36
6.5 Computer security controls 36
6.6 Life cycle technical controls 37
6.7 Network security controls 37
6.8 Time-stamping 38
7. CERTIFICATE, CRL, AND OCSP PROFILES 38
7.1 Certificate profile 38
7.2 CRL profile 39
7.3 OCSP profile 39

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS ... 39
8.1 Frequency or circumstances of assessment ... 39
8.2 Identity/qualifications of assessor ... 39
8.3 Assessor's relationship to assessed entity ... 40
8.4 Topics covered by assessment ... 40
8.5 Actions taken as a result of deficiency ... 40
8.6 Communication of results ... 40
9. OTHER BUSINESS AND LEGAL MATTERS ... 40
9.1 Fees ... 40
9.2 Financial responsibility ... 41
9.3 Confidentiality of business information ... 41
9.4 Privacy of personal information ... 42
9.5 Intellectual property rights ... 42
9.6 DigiCert Representations and Warranties ... 43
9.7 Disclaimers of warranties ... 45
9.8 Limitations of liability ... 46
9.9 Indemnities ... 46
9.10 Term and termination ... 47
9.11 Individual notices and communications with participants ... 47
9.12 Amendments ... 47
9.13 Dispute resolution provisions ... 47
9.14 Governing law ... 48
9.15 Compliance with applicable law ... 48
9.16 Miscellaneous provisions ... 48
9.17 Other provisions ... 49

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 the Issuance and Management of Extended Validation Certificates," version 1.0 (6/7/2007) (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 or Registration, and Registration Number. EV Certificates may be issued to Private Organizations, Government Entities, International Organization Entities, and Business Entities. EV Certificates are also intended to help establish the legitimacy of a business claiming to operate a website 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 either one (1) or two (2) years.

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), or their revoked status may be determined by an Online Certificate Status Protocol (OCSP) check.

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

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 or perform an Online Certificate Status Protocol check (http://ocsp.digicert.com) 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, digitalsignature, 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

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 a Private Organization, Government Entity or Business Entity applying for a Certificate.

Application Software Vendor: A developer of Internet browser software or other software that displays or uses certificates and distributes root certificates, such as KDE, Microsoft Corporation, Mozilla Corporation, Opera Software ASA, and Red Hat, Inc.

Business Entity: Any entity that is neither a Private Organization nor a Government Entity as defined in the Guidelines. Examples include general partnerships, unincorporated associations, and sole proprietorships.

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

Principal Individual(s): Individuals of a Private Organization, Government Entity or Business Entity that are either owners, partners, managing members, directors or officers, as identified by their title of employment, or an employee, contractor or agent authorized by such entity or organization to conduct business related to the request, issuance and use of EV Certificates.

Private Organization: A non-governmental legal entity (whether ownership interests are privately held or publicly traded) whose existence was created by a filing with (or an act of) a Government Agency in its Jurisdiction of Incorporation or Registration. Examples include corporations, limited partnerships, limited liability companies, and government-chartered financial institutions.

Qualified Government Information Source: A regularly-updated and current 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 Government Tax Information Source: A Qualified Governmental Information Source that specifically contains tax information relating to Private Organizations, Business Entities or Individuals (e.g. the I.R.S. in the United States).

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.

Registration Agency: a Governmental Agency that registers business information in connection with an entity's business formation or authorization to conduct business under a license, charter or other certification. A Registration Agency MAY include, but is not limited (i) a State Department of Corporations or a Secretary of State; (ii) a licensing agency, such as a State Department of Insurance; or (iii) a chartering agency, such as a state office or department of financial regulation, banking or finance, or a federal agency such as the Office of the Comptroller of Currency (OCC) or the Office of Thrift Supervision (OTC).

Relying Party: The Relying Party is an individual9ss2(p)-5.4GS1 Tf0 c.3(a).3(dien)-5.3(ti1(o)-45.3(e)1.3(t)-10.8(h)-4)-5.3(v)-

QGTIS	Qualified Government Tax 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:

x On the web: www.digicert.com
x By email to admin@digicert.com
x By mail addressed to: DigiCert, Inc., 355 South 520 West, Lindon, Utah 84042
x By telephone Tel: 1-801-877-2100
x 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 a period from 24 hours up to 7 days. 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

CRLs for end-user Subscriber Certificates are issued at least once per day. CRLs for CA Certificates are issued twice annually, but also whenever a CA Certificate is revoked. Each 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, the Relying Party Agreement, and any other conditions of

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:

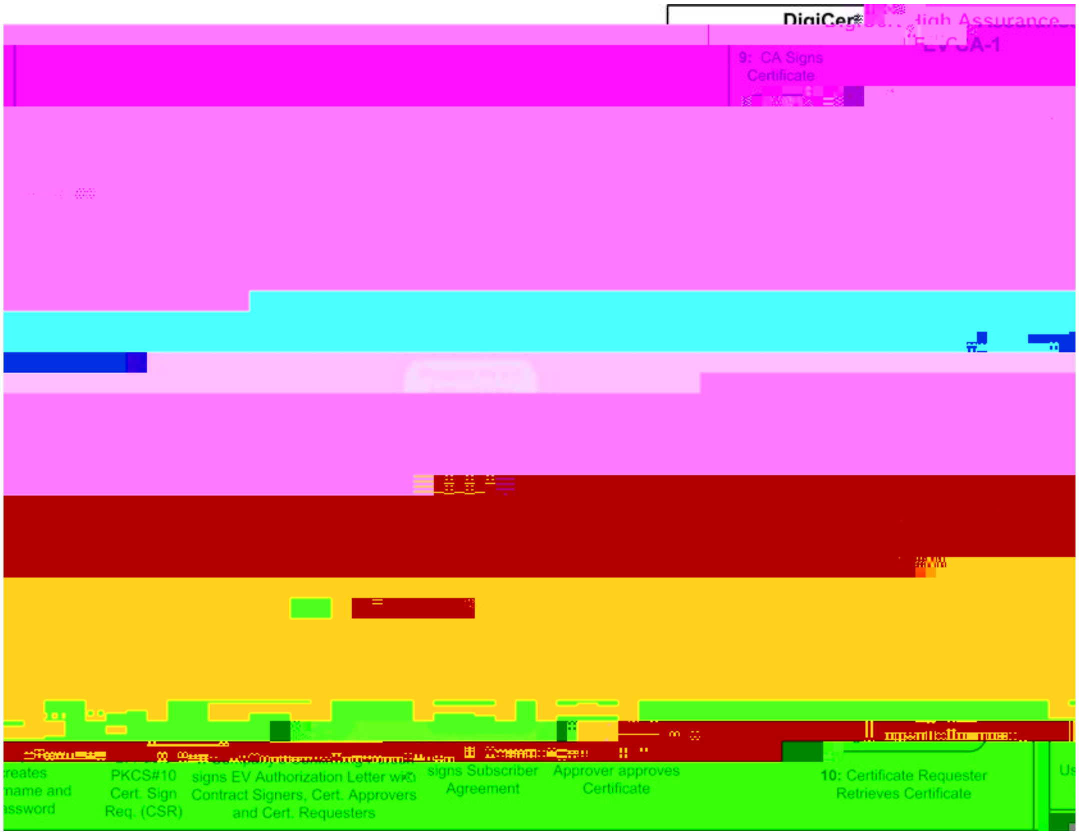
DigiCert High Assurance EV CA-1
9: CA Signs Certificate
reates
name and
ssword
PKCS#10 Cert. Sign Req. (CSR)
signs EV Authorization Letter w/ Contract Signers, Cert. Approvers and Cert. Requesters
signs Subscriber Agreement
Approver approves Certificate
10: Certificate Requester Retrieves Certificate
Us

Figure 1.

3.2.1 Method to prove possession of private key

charter (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

For those Business Entities that register with a Government Agency in a jurisdiction that does not issue numbers pursuant to government registration, the date of the registration SHALL be entered into this field in any one of the common date formats.

For Government Entities that do not have a Registration Number, DigiCert obtains the Applicant's date of incorporation, registration, or formation, or the identifier for the legislative act that created the Government Entity. If none of the foregoing are available, DigiCert enters appropriate language to indicate that the Subject is a Government Entity.

For International Organization Entities, DigiCert obtains evidence that the Applicant was created under a Charter, Treaty, Convention or equivalent instrument that was signed by, or on behalf of, more than one country's government.

(4) Registered Agent/Principal Individual: for Private Organizations, obtain the identity and address of the Applicant's Registered Agent or Registered Office (as applicable) in the Applicant's Jurisdiction of Incorporation or Registration; or for Business Entities, verify the identity of the identified Principal Individual in accordance with Section 3.2.3 below.

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, a Qualified Government Information Source, a Qualified Independent Information Source provided that the QIIS has verified the assumed name with the appropriate Government Agency, or by relying on a Verified Legal Opinion or Verified Accountant Letter that indicates the assumed name under which Applicant conducts business, the government agency with which the assumed name is registered, and that such filing continues to be valid.

Government Entities: The foregoing information concerning the legal existence and identity of a Government Entity may also be provided by a superior governing Government Entity in the same political subdivision as Applicant (e.g. a Secretary of State may verify the legal existence of a specific state department), a judge that is an active member of the federal, state or local judiciary within that political subdivision, or an attorney representing the Government Entity.

International Organization Entities: Legal existence and identity may be confirmed:

(a) With reference to the constituent document under which the International Organization was formed; or

(b) Directly with a signatory country's government (i.e. from an appropriate government agency or from the laws of that country, or by verifying that the country's government has a mission to represent it at the International Organization); or

(c) Directly against any current list of qualified entities that the CAB Forum may maintain at www.cabforum.org.

In cases where the International Organization applying for the EV certificate is an organ or agency - including a non-governmental organization (NGO) of a verified International Organization, then DigiCert may verify the International Organization applicant directly with the verified umbrella International Organization of which the applicant is an organ or agency.

C. Physical Location

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

(1) **QIIS/QGTIS:** the Applicant's address from the current version of such information maintained by a Qualified Independent Information Source, or a Qualified Governmental Tax Information Source, or for Government Entity Applicants, the QGIS in Applicant's Jurisdiction; 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.

(3) **Verified Legal Opinion or Account Letter:** DigiCert also accepts and relies on Verified Legal Opinions and Verified Accountant Letters to establish the address of Applicant's Place of Business and that business operations are conducted there.

For Applicants whose Place of Business is not in the same country as the Applicant's Jurisdiction of

(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 an EV Authority Letter / Master Agreement.

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

(b) Applicant's Registered Agent, registered Principal Individual, or Registered Office in the Jurisdiction of Incorporation or Registration as listed in the official records of the Government Agency, with instructions that it be forwarded to an appropriate Confirming Person; or
(c) A named individual verified to be in the direct line of management above the Contract Signer or Certificate Approver by contacting 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 EV Guidelines).

(B) Means of Communication. Based on (A) above, the Confirmation Request is directed to the Confirming Person in a manner reasonably likely to reach such person. The following options are acceptable:
(i) If the request for the EV Authority Letter / Master Agreement 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 or Registration.

(ii) If the request for the EV Authority Letter / Master Agreement is sent by e-mail, it is addressed to the Confirming Person's business e-mail address provided by Applicant's Human Resources Department pursuant to (A) above, or as listed in a current Qualified Government Information Source, a Qualified Independent Information Source, a Verified Legal Opinion, or a Verified Accountant Letter.

(iii) If the request for the EV Authority Letter / Master Agreement 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.

(iv) When a request for the EV Authority Letter / Master Agreement 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 Authority Letter / Master Agreement 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 Authority Letter / Master Agreement accomplishes these objectives by providing independent confirmation from the Applicant of such name, title, and authority as outlined above. The attestations in the EV Authority Letter / Master Agreement include the employment and signing authority of the Contract Signer and the employment and approval authority of the Certificate Approver.

(4) In accordance with Section 22(d)(3) of the Guidelines, DigiCert may rely on a verified Confirming Person to confirm their own contact information: email address, telephone number, and facsimile number. DigiCert may also rely on this verified contact information for future correspondence with the Confirming Person if:
(i) The domain of the e-mail address is owned by the Applicant and is the Confirming Person's own e-mail address and not a group e-mail alias.
(ii) The Confirming Person's telephone/fax number is verified by the CA to be a telephone number that is part of the organization's telephone system, and is not the personal phone number for the person.

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 username 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 DigiCert has performed all authentication and verification of information tasks required by the Guidelines and that the EV Authority

Letter / Master Agreement is still valid (i.e. the Certificate request is made and approved within the specified term stated in the EV Authority Letter / Master Agreement 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

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, Verified Accountant Letters, Verified Legal Opinions, and the Applicant's Human Resources Department.

Steps 4 and 5: DigiCert requests and receives a signed EV Authority Letter / Master Agreement from the Applicant (unless a valid

(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.

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 533 Lv
  relevant CRTJ12(n)-4.6(g to t)-9.5(.01)6.9(l.9(b(d)-40 TD-.8.1(a dTJ1.c.016)6.9(le)-5(5VD]5ǎǎǎǎǎǎǎǎǎǎǎǎǎǎǎǎǎǎ

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 thirteen months, except for the exceptions allowed by Section 25(c) of the Guidelines, which allow DigiCert to rely on its prior authentication and verification of:

(a) A Principal Individual of a Business Entity under Section 3.2.3(a) if the Principal Individual is the same as the Principal Individual verified in connection with the previously issued EV Certificate;

(b) Applicant's Place of Business (Section 3.2.2.2.C);

(c) The verification of telephone number of Applicant's Place of Business (Section 3.2.2.2.D), except that DigiCert still calls the telephone number to obtain an affirmative response sufficient to enable a reasonable person to conclude the Applicant is reachable by telephone at the number dialed;

(d) Applicant's Operational Existence (Section 3.2.2.2.A);

(e) The name, title, and authority of the Contract Signer, Certificate Approver, and Certificate Requester, for the duration specified in the EV Authority Letter / Master Agreement (Section 3.2.5); and

(f) The prior verification of the email address used by DigiCert (Section 3.2.5(1)(B)(ii)).

The Guidelines also allow DigiCert to rely on prior Verified Legal Opinions (see Section 3.2.2.2.E) that establish Applicant's awareness and exclusive right to use the specified domain name, provided that either:

a. The WHOIS record still shows the same registrant as indicated when DigiCert received the prior Verified Legal Opinion, or
b. The Applicant establishes domain control via a practical demonstration.

If a company is no longer in good standing, or if any of the other required 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

Pursuant to Section 25(b) (Validation of Re-issuance requests) of the Guidelines, DigiCert may rely on previously verified information to issue a Replacement Certificate where:

1. The expiration date of the Replacement Certificate is the same as the expiration date of

the currently valid EV Certificate being replaced, and

2. The certificate subject of the Replacement Certificate is the same as the certificate subject contained in the currently valid EV certificate.

Re-keying, or replacing 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. (Note that 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 issue a Replacement Certif

Certificate; or

x If DigiCert receives notice or otherwise become aware that a Subscriber has been added as

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 in another building (the "Support and Vetting Room"). The physical site where the CA is located 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 CA 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 where the CA is housed 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. In other words, the card holder must use his card to exit the Data Center in order to use the card again to re-enter the Data Center. The security guard's office is located adjacent to the Data Center door, 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 Support and Vetting Room. The room is also equipped with motion-activated video surveillance cameras.

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 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 quarterly 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 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 is kept in a separate safe deposit box from activation material owned by personnel filling the Partition Administrator role.

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.

Operations Manager
During day-to-day operations, the DigiCert Operations Manager is a trusted role.

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.

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 Validation Specialists serve in truste

5.3.3 Training requirements

DigiCert provides all personnel performing validation duties (“Validation Specialists”) with skills

- System crashes, hardware failures and other anomalies

Log entries (automatic and manual) include the following:

- Date and time of the entry
- Type of entry
- Source of entry (customer or staff identity, IP address or other)
- Kind of entry
- Description

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;

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 Re use the USB authentication tokens 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.

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 a set of iKey USB-based two-factor authentication tokens 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 6.2.2 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. DigiCert requires that passwords to workstations be changed on a regular basis.

6.4.2 Activation data protection

Activation data for Luna SAs are protected by keeping the USB authentication tokens under separate, role-based physical control with backups 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 change control data entries that are 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 change control data entries that are 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 firehgi.7(y)12.4(fir)367(vendors, o6s)-selecteertcert 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

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 5280 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

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 Ce

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 observes 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 or Registration;

(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 Government Agency in the Subject's Jurisdiction of Incorporation or Registration, 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:**

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.

status is currently available from DigiCert online, and the browser software either failed to check such status or ignored an indication of revoked status).

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 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 impair or be construed as a waiver of such right, remedy or power. A waiver by any party of any

Appendix A

Certificate Profiles

1a. 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

1b. DigiCert's High Assurance EV Root CA Cross-Certified by Entrust

Field	Value
Version	V3 (2)
Serial Number	Unique number
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}

Issuer Distinguished Name	CN = Entrust.net Secure Server Certification Authority
	OU = (c) 1999 Entrust.net Limited
	OU = www.entrust.net/CPS incorp. by ref. (limits liab.)
	O = Entrust.net
	C = US

Validity Period	September 30, 2006 to July 26, 2014

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; f0 17 62 13 55 3d b3 ff 0a 00 6b fb 50 84 97 f3 ed 62 d0 1a
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; Certificate Signing , Off-line CRL Signing, CRL Signing (06)
Extended Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)
Entrust Secure Networks (1.2.840.113533.7.65.0)	V.7.1
Authority Information Access	[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.entrust.net
CRL Distribution Points	[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.entrust.net/server1.crl
Certificate Policies	Not present
Basic Constraints	c=yes; Subject Type=CA Path Length Constraint=1

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.

Basic2cb.48004 .5.6(49 1)-6.mra

3. DigiCert End Entity EV Certificates

Field	Value	Comments
Version	V3 (2)	
Serial Number	Unique number	
Issuer Signature Algorithm	sha-1WithRSAEncryp 14.4 (En79.743f92.52 678.7orit)-1.3(yp 14.ri8j0059 re2yp 14.ri8j00.9(SA)(W)-4970	

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.

	(2.5.4.6)	
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	