DigiCert

Certificate Policy and Certification Practice Statement

DigiCert, Inc.
Version 3.02
November 9, 2006

333 South 520 West
Orem, 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) Certificate Policy and Certification Practice Statement (CP/CPS) and outlines the legal, commercial and technical principles and practices that DigiCert employs in providing certification services, i.e. it is a statement of the practices that DigiCert uses in approving, issuing, using and otherwise managing ITU X.509 version 3 Digital Certificates and in maintaining a Certificate-based public key infrastructure (PKI) applicable to the Certificates that DigiCert issues. A *digital certificate* is formatted data that cryptographically binds an identified subscriber with a public key. A digital certificate allows an entity taking part in an electronic transaction to prove its identity to other participants in such transaction. Digital certificates are used in commercial environments as a digital equivalent of an identification card.

This CP/CPS also defines the underlying certification processes for Subscribers of 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 all parties involved in the DigiCert PKI of their roles and responsibilities. Pursuant to the IETF PKIX RFC 3647 CP/CPS framework, this CP/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."

DigiCert issues certificates for server and client authentication to organizations and individuals for use with the SSL 3.0/TLS 1.0 protocol to enable secure transactions of data through privacy, authentication, and data integrity ("SSL Certificates"). DigiCert issues both server-specific and wildcard (*.domain.com) SSL certificates. The validity period of a DigiCert-issued certificate is 1 year, 2 years or 3 years. DigiCert reserves the right to, at its sole discretion, issue certificates that may fall outside of these set periods.

To obtain a DigiCert SSL 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 certificate or earlier notice of informational content to be included in the 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 certificate. Revoked certificates are published on a Certificate Revocation List (CRL).

1.2 Document name and identification

This document is the DigiCert, Inc. CP/CPS version 3.02 which was originally approved for publication on 14 July 2006 by DigiCert senior management, acting as the DigiCert Policy Authority (DCPA). Revisions of this document have been made as follows:

Date	Changes	Version
7-14-2006	New Version	3.0
9-16-2006	Changed logo, added this revision table, added method of verifying authorization in sections 3.2.5 and 4.1.2; revised language in section 5.7 to update status of implementation and testing of disaster recovery / business continuity plan; modified section 6.6.1 concerning approval of change requests, and added l = locality and s = state of Subscriber fields to subject	3.01

Date	Changes	Version
	name to certificate profiles for end entity certificates.	
11-9-2006	Removed reference to DigiCert High Assurance CA from section 1.2 and from Appendix B. Updated Appendix B to note changes in common names of DigiCert Assured ID Root CA and removed references to DigiCert High Assurance CA. Also removed extended key usage and certificate policies extensions from Root Certificates and updated Key Identifiers and CRL references.	3.02

As detailed in this CP/CPS, DigiCert issues the following certificate types, which are identified by the following object identifier(s) under DigiCert's ANSI-issued arc of joint-iso-ccitt (2) country (16) USA (840) US-company (1) DigiCert (114412) CP/CPS (1) ver.3.0 (3.0) (i.e., 2.16.840.1.114412.1.3.0), which DigiCert uses to identify this CP/CPS and Certificates issued pursuant hereto:

Root Certification Authority	**DigiCert CP OID**
DigiCert Global CA	2.16.840.1.114412.1.3.0.1
DigiCert Global Root CA	2.16.840.1.114412.1.3.0.3
DigiCert Assured ID Root CA	2.16.840.1.114412.1.3.0.4

1.3 PKI participants

1.3.1 Certification authority

DigiCert is a Certification Authority (CA) that issues high quality and highly trusted digital certificates to entities including private and public companies and individuals in accordance with this CP/CPS. In its role as a CA, DigiCert performs functions associated with public key operations that include receiving requests, issuing, revoking and renewing a digital 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 CP/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 CP/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 CP/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 CP/CPS
- Distribute issued certificates in accordance with the methods detailed in this CP/CPS
- 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 individuals or companies that use PKI in relation with DigiCert supported transactions and communications. Subscribers are parties that are identified in a certificate and hold the private key corresponding to the public key that is listed in a subscriber certificate. Prior to verification of identity and issuance of a certificate, a Subscriber is an *applicant* for the services of DigiCert.

1.3.4 Relying parties

Relying parties use PKI services in relation with DigiCert-issued 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 a digital 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 certificate.

1.4 Certificate usage

1.4.1. Appropriate certificate uses

Certificates issued pursuant to this CP/CPS may be used for all legal authentication, encryption, access control, and digital signature purposes, as designated by the key usage and extended key usage fields found within the certificate. Typically, the following bits are enabled for DigiCert-issued SSL Certificates: keyEncipherment, dataEncipherment, serverAuthentication and clientAuthentication.

1.4.2 Prohibited certificate uses

Certificates issued under the provisions of this CP/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 CP/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 CP/CPS suitability for the policy

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

1.5.4 CP/CPS approval procedures

Approval of this CP/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 CP/CPS require notice or any change in the OID of a certificate issued pursuant to this CP/CPS. *See also* Section 9.10 and Section 9.12 below.

1.6 Definitions and acronyms

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

Registrar: The global 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.

Subscriber: The Subscriber is an individual or entity that has been issued a 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 www.digicert.com/ssl-cps-repository.htm.

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 www.digicert.com/ssl-cps-repository.htm.

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
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
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 CP/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.

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.

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 CP/CPS and any other conditions of usage that DigiCert may make available. Parties demonstrate acceptance of the conditions of usage of this CP/CPS by using a DigiCert-issued 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 a 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. Non-wildcard SSL Certificates are issued using the Fully Qualified Domain Name (FQDN) name of the server, service or application that has been confirmed with the Subscriber. Wildcard SSL Certificates have a wildcard asterisk character for the server name in the Subject field. The FQDN or authenticated domain name is placed in the Common Name (CN) attribute of the Subject field and, when applicable, the Subject Alternative Name.

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 Global CA).

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 CP/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

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 a 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

The elements listed in this section are utilized by DigiCert during the certificate issuance process to authenticate identity. 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 9.4 of this CP/CPS.

Fields Parsed and Automatically Populated from PKCS#10 CSR:

- Common Name / Fully Qualified Domain Name / Network Server Name / Public or Private IP ("CN=" in CSR must match registered domain name or IP address)
- Organization name ("O=" in CSR must match full legal company/organization name)
- Organizational unit ("OU=" in Subject field of CSR)
- City, State and Country (Automatically populated from CSR)
- Public Key (from CSR)
- Server Software Identification (obtained when CSR is submitted during **Step 4**)

Additional Information Collected from Organization Represented During Step 6

- Legal Name of Organization Contact Person
- E-mail address of Organization Contact Person
- Street Address and Postal Area Code
- DUNS Number (if available)
- VAT-number (if applicable)
- Payment Information

- Technical contact full name, email address and telephone (optional)
- Proof of right to use name
- Proof of existence and professional status of the Individual
- Subscriber agreement – accepted during **Step 7** of the application process

If the Common Name populated automatically from the CSR is not correct, the applicant is requested to generate a new CSR with the correct Common Name. *See* Section 4.1.2. If other organization information or geographic location information are incorrect, that information is replaced with correct information in DigiCert's subscriber database.

Documentation requirements for organizational applicants are the following:

- Articles of Association
- Business License
- Certificate of Compliance
- Certificate of Incorporation
- Certificate of Authority to Transact Business
- Tax Certification
- Corporate Charter
- Official letter from an authorized representative of a government organization
- Official letter from office of Dean or Principal (for Educational Institutions)

DigiCert may accept at its discretion other official documentation supporting an application.

DigiCert may use the services of a third party to confirm information on a business entity that applies for a digital certificate. DigiCert accepts confirmation from third party organizations, other third party databases and government entities.

DigiCert controls include the use of online data resources to confirm the registration of the applicant company and to verify members of the board, management, and officers and directors representing the company.

DigiCert may use any means of communication at its disposal to ascertain the identity of an organizational or individual applicant. DigiCert reserves the right to not issue a Certificate in its absolute discretion.

3.2.3 Authentication of individual identity

The elements listed in this section are utilized by DigiCert during the certificate issuance process to authenticate identity. Elements that are already in the public domain (e.g., available via WHOIS) are not treated as confidential for purposes of the privacy and protection of data provisions outlined in Section 9.4 of this CP/CPS.

Documentation requirements for Individual applicants include the following:

- Passport
- Driver's License with photo or non-driver's license identification card with photo;
- Military ID with photo;
- Alien registration card or naturalization certificate (with photograph);
- National health card (in jurisdictions where it contains a photograph); or
- Other similarly trustworthy, valid photo ID issued by a Government Agency.

DigiCert may accept at its discretion other official documentation supporting an application.

Upon receipt of an application for a digital certificate and based on the submitted information, DigiCert will confirm the following information:

- The certificate applicant is the same person as the person identified in the certificate request.
- The certificate applicant holds the private key corresponding to the public key to be included in the certificate
- The information to be published in the certificate is accurate, except for non-verified subscriber information.

- Any agents who apply for a certificate listing the certificate applicant's public key are duly authorized to do so.

In all types of DigiCert certificates the Subscriber has a continuous obligation to monitor the accuracy of the submitted information and notify DigiCert of any changes that would affect the validity of the certificate. Failure to comply with the obligations as set out in the Subscriber Agreement will result in the revocation of the Subscriber's certificate without further notice to the Subscriber and the Subscriber shall pay any charges payable but not yet paid under the Subscriber Agreement.

In all cases and for all types of DigiCert certificates the Subscriber has a continuous obligation to monitor the accuracy of the submitted information and notify DigiCert of any such changes.

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.

Authority to use domain name or IP address is confirmed by a WHOIS check or a reverse IP address lookup to ensure that the Organization owns or controls the Domain Name or IP address.

The authority of the applicant's agent is confirmed with an Authority of Subscriber Agreement acknowledged by an authorized contact listed with the Domain Name Registrar ("Registrar"). The registered domain administrator may be contacted to confirm authorization to receive a Certificate for the URL requested. Contact information is obtained from WHOIS and presented for review by the Subscriber's agent during **Step 5** of the application process. After application submittal, authorization from the domain contact person and/or others such as persons with administrative control over the domain (e.g. webmaster@domain.com, postmaster@domain.com, admin@domain.com) is received through one of the following methods:

- These persons are contacted via e-mail and directed to a secure URL where at least one of them must enter an authorization code and accept the Authority of Subscriber Agreement to allow the application for a certificate to proceed. The name, e-mail address and IP address of the organizational representative acknowledging authority is also recorded;
- An Authorization Letter (e.g. Appendix A) is received from the Subscriber as explained in Sections 3.2.2, 4.1.1 and other portions of this CP/CPS; or
- Other comparable methods of establishing authority.

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.

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 Section 4.9.3 (Procedure for Revocation Request)

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

This Part 4 of the CP/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 the individual who is the subject of the certificate or by persons who are duly authorized to request a certificate on behalf of the applicant. The WHOIS record maintained by the domain registrar presumptively indicates who the persons are with authority over the domain. If an application is being submitted by someone else as the agent of the domain owner, the agent must submit a Domain Authorization Letter (Appendix A) authorizing the use of the domain.

All Certificate applicants must complete the enrollment process which includes:

- Generate an RSA key pair and submit a valid PKCS#10 CSR to demonstrate to DigiCert ownership and control of the private key corresponding to the public key of the key pair
- Make all reasonable efforts to protect the security and integrity of the private key
- Submit to DigiCert a certificate application, including application information as detailed in this CP/CPS,
- Agree to the terms of the Subscriber Agreement, and
- Provide proof of identity through the submission of official documentation as requested by DigiCert during the enrollment process.

4.1.2 Enrollment process and responsibilities

Below as Figure 1 is a simplified flow chart of the enrollment and certificate issuance process:

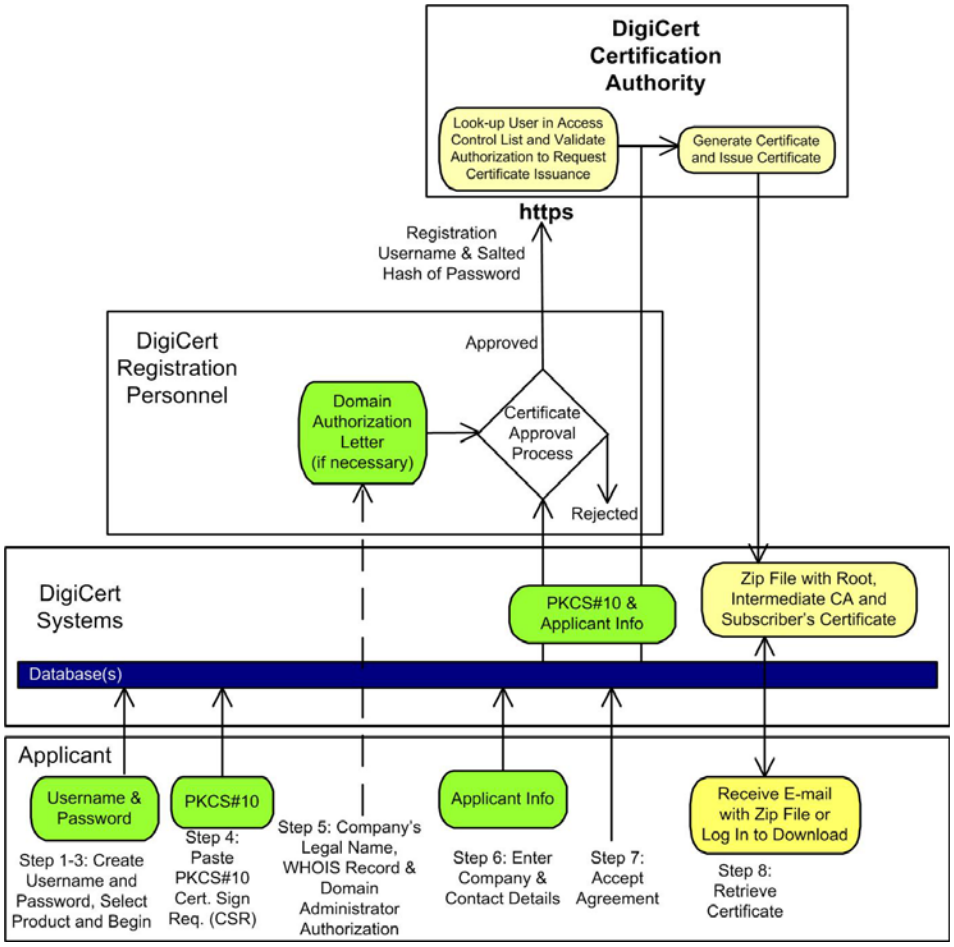

Figure 1.

In **Step 4** of the enrollment process, the Applicant pastes and submits the PKCS#10 CSR into a web form that is submitted to DigiCert's CA systems. In **Step 5** 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 applicant 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 and is required to verify that the full legal name of the individual or organization 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.

Applicants must complete the online forms at DigiCert's website. Under special circumstances the applicant may submit the same information in an application via email; however this process is available at the sole discretion of DigiCert.
If the application is being made by a third-party for the company listed in the WHOIS record, the following must also be provided to DigiCert:

- the Domain Authorization Letter (Appendix A), completed and signed by the Registrant (domain owner) or the Administrative Contact on the WHOIS record, and
- a photocopy of that person's photo ID (see Section 3.2.3).

DigiCert registration personnel compare the information submitted by the Registrant or the Administrative Contact to ensure that it is consistent with the information in the WHOIS record.

DigiCert reserves the right to use other comparable and acceptable methods to establish the authorization of the individual requesting a certificate on behalf of the Subscriber.

4.2 Certificate application processing

During the certificate approval process identified in Figure 1 above, DigiCert employs 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 that:

1. **The applicant has the right to use the domain name used in the application**
   - Validated by reviewing domain name ownership records available publicly from the Domain Name Registrar
   - Validation may be supplemented by communicating with the Administrative Contact listed in the WHOIS record
   - Validation may also be supplemented by communicating with generic emails which ordinarily are only available to persons with administrative control over the domain, for example, webmaster@domain.com, postmaster@domain.com, admin@domain.com, etc.

2. **The applicant is an accountable legal entity, whether an organization or an individual.**
   - Validated by requesting official company documentation, such as Business License, filed or certified Articles of Incorporation/Organization, Sales License or other relevant documents. For non-corporate applications, documentation listed in Section 3.2.3.
   - Documentation of organizational existence/individual identity is cross-checked for consistency with other available records, including those maintained by official government repositories and commercial providers of such information.

The following steps describe the milestones to issue a Certificate:

a) The applicant fills out the online request on DigiCert's web site and the applicant submits the required information, including PKCS#10 CSR, e-mail address, common name, organizational information, address, and billing information .
b) The applicant accepts the Subscriber Agreement.
c) The applicant submits the required information to DigiCert.
d) The applicant pays the certificate fees.
e) DigiCert verifies the submitted information using a variety of sources, including third

party databases and government records.

f) Upon successful validation of the application information, DigiCert may issue the certificate to the applicant or should the application be rejected, DigiCert will alert the applicant that the application has been unsuccessful.
g) Renewal is conducted as per the procedures outlined in this CP/CPS and on DigiCert's website.
h) Revocation is conducted as per the procedures outlined in this CP/CPS.

4.2.2 Approval or rejection of certificate applications

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 a digital 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 a 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 a digital 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 certificate. As illustrated in Figure 1, when a certificate is approved, a unique request string is sent to the CA via https. The request string contains the relevant parameters for the certificate to be signed (e.g. PKCS #10 CSR, validity period, etc.) and authentication information for the DigiCert employee who is the requestor. The requestor'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 requestor 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 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 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

DigiCert SSL Certificates are delivered in a zip file via email to the email address designated by the subscriber during the application process. The Subscriber is also provided a hypertext link to

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

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

The subscriber 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 CP/CPS and the Certificate Profile (Appendix B). 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 a digital 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 CP/CPS and contained in the certificate.

Reliance is accepted as reasonable under the provisions made for the relying party under this CP/CPS and within the Relying Party Agreement. If the circumstances of reliance exceed the assurances delivered by DigiCert under the provisions made in this CP/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 CP/CPS, DigiCert has adequately informed relying parties on the usage and

validation of digital signatures and SSL/TLS sessions through this CP/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 CP/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.

Depending on the option selected during application, the validity period of a DigiCert certificate is one year (365 days), two years (730 days) or three years (1095 days) from the date of issuance and is detailed in the relevant field within the certificate. Time remaining on the expiring certificate is added to the certificate lifetime of the new certificate.

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. DigiCert registration personnel reconfirm domain name ownership using current WHOIS information. State or other jurisdictional records are checked to confirm geographic location, company control and good standing the jurisdiction of organization. If a company is no longer in good standing, the certificate is not renewed.

However, for individuals, provided that the individual's location and WHOIS information have not changed, no additional identity vetting is required.

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.

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. 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 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 a certificate is to permanently end the operational period of the certificate prior to reaching the end of its stated validity period. DigiCert will revoke a digital certificate if:

- There has been loss, theft, modification, unauthorized disclosure, or other compromise of the Private Key associated with the certificate.
- The subscriber or DigiCert has breached a material obligation under this CP/CPS.
- Either the subscriber's or DigiCert's obligations under this CP/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 receives a lawful and binding order from a government or regulatory body to revoke the certificate.
- There has been a modification of the information pertaining to the subscriber that is contained within the certificate.

4.9.2 Who can request revocation

The subscriber or other appropriately authorized parties can request revocation of a certificate. The revocation request must be received from the Administrative Contact associated with the certificate application. DigiCert may, if necessary, also request that the revocation request be made by either the organizational contact, billing contact or domain registrant.

Prior to the revocation of a certificate, DigiCert will verify that the revocation request has been:

- Made by the organization or individual entity that has made the certificate application.
- Made by an entity with legal jurisdiction and authority to request revocation.

DigiCert may revoke any certificate for any reason or no reason.

4.9.3 Procedure for revocation request

DigiCert employs the following procedure for authenticating a revocation request:

- Upon receipt of the revocation request, DigiCert will request confirmation from the known administrator via out-of-band communication (e.g., telephone, fax, etc.).
- DigiCert validation personnel will then log the identity of the person making the request, the DigiCert personnel approving the revocation request, and the reason stated for revocation.
- A command to revoke the certificate is processed and the CRL is updated. Upon revocation of a 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 CP/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 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 on 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.

DigiCert updates and publishes a new CRL on a 24-hour basis or more frequently under special circumstances. The CRLs for certificates issued pursuant to this CP/CPS can be accessed via the URLs contained in the Certificate Profile for that certificate. *See* Appendix B.

DigiCert also publishes a repository of legal notices regarding its PKI services, including this CP/CPS, agreements and notices references within this CP/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

No stipulation.

4.9.10 On-line revocation checking requirements

Not applicable.

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 CP/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.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

Consistent with this CP/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

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

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.

5.3.4 Retraining frequency and requirements

No stipulation.

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 CP/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 CP/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

Auditable Event	CA System	Vetting Interface
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
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

Auditable Event	CA System	Vetting Interface
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
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 CP/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 CP/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 CP/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 CP/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 DigiCert digital 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 CP/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 CP/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. Typically, SSL 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 SSL 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 B.

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 CP/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	3 years

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 CP/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

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 B.

7.1.3 Algorithm object identifiers

See Appendix B.

7.1.4 Name forms

See Appendix B 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 CP/CPS. The CP OIDs that incorporate this CP/CPS into a given certificate by reference (which identify that this CP/CPS applies to a given digital certificate containing the OID) are listed in Section 1.2 and in the Certificate Profile attached as Appendix B.

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 CP/CPS, which are incorporated by reference into the certificate. *See* Appendix B.

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 CP/CPS have been designed to meet or exceed the requirements of

generally accepted and developing industry standards including the AICPA/CICA WebTrust Program for Certification Authorities, ANS X9.79/ISO 21188 PKI Practices and Policy Framework ("CA WebTrust/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 CA WebTrust/ISO 21188 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 CA WebTrust/ISO 21188 audit include but are not limited to DigiCert's CA business practices disclosure (i.e., this CP/CPS), the service integrity of DigiCert's CA operations and the environmental controls that DigiCert implements to ensure a trustworthy system.

8.5 Actions taken as a result of deficiency

If an audit reports any material noncompliance with applicable law, this CP/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.

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 offers a 30-day refund policy. During a 30-day period (beginning when a certificate is first issued) the Subscriber may request a full refund for their certificate. Under such circumstances, the original certificate may be revoked and a refund provided to the applicant. DigiCert is not obliged to refund a certificate after the 30-day reissue policy period has expired.

9.2 Financial responsibility

9.2.1 Insurance coverage

DigiCert carries at least $1 million in Commercial General Liability insurance coverage.

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 CP/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 CP/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 CP/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 CP/CPS.

The word “DigiCert” is a registered trademark 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 Representations and warranties

9.6.1 CA representations and warranties

Except as expressly stated in this CP/CPS, DigiCert makes no representations or warranties regarding its public service. DigiCert reserves its right to modify such representations as it sees fit, at its sole discretion, or as required by law.

Only to the extent specified in the relevant sections of this CP/CPS, DigiCert promises to:

- Comply with this CP/CPS and its internal or published policies and procedures.
- Comply with applicable laws and regulations.
- Provide infrastructure and certification services, including but not limited to the establishment and operation of the DigiCert Repository and web site for the operation of PKI services.
- Provide trust mechanisms, including a key generation mechanism, key protection, and secret sharing procedures regarding its own infrastructure.
- Provide prompt notice in case of compromise of its private key(s).
- Provide and validate application procedures for the various types of certificates that it may make publicly available.
- Issue digital certificates in accordance with this CP/CPS and fulfill its obligations presented herein.
- Provide support to Subscribers and Relying Parties as described in this CP/CPS.
- Revoke certificates according to this CP/CPS.
- Provide for the expiration and renewal of certificates according to this CP/CPS.
- Make available a copy of this CP/CPS and applicable policies to requesting parties.
- Warrant the accuracy of information published on a Qualified Certificate issued pursuant to the requirements of the European Directive 99/93.
- Warrant that the signatory held the private key at the time of issuance of a certificate issued pursuant to the requirements for Qualified Certificates as in the European Directive 99/93.

The Subscriber also acknowledges that DigiCert has no further obligations under this CP/CPS.

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 CP/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 CP/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

Unless otherwise stated in this CP/CPS or the applicable Subscriber Agreement, Subscribers shall exclusively be responsible:

- To minimize internal risk of private key compromise by ensuring that they and their agents have adequate knowledge and training on PKI.
- To generate a secure private / public key pair to be used in association with the certificate request submitted to DigiCert.
- Ensure that the public key submitted to DigiCert is the correct one and corresponds with the private key used.
- Provide correct and accurate information in communications with DigiCert and alert DigiCert if any information originally submitted has changed since it was submitted to DigiCert.
- Read, understand and agree with all terms and conditions in this CP/CPS and associated policies published in the DigiCert Repository at http://www.digicert.com/ssl-cps-repository.htm.
- Use DigiCert certificates for legal and authorized purposes in accordance with this CP/CPS.
- Cease using the certificate if any information in it becomes misleading, obsolete or invalid.
- Cease using the certificate if it is expired and remove it from any applications and/or devices it has been installed on.
- Make reasonable efforts to prevent the compromise, loss, disclosure, modification, or otherwise unauthorized use of the private key corresponding to the public key published in a DigiCert certificate.
- Request the revocation of a certificate in case of any occurrence that might materially affect the integrity of the certificate.
- For acts and omissions of partners and agents they use to generate, retain, escrow, or destroy their private keys

Without limiting other Subscriber obligations stated in this CP/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

CP/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 CP/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 CP/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 CP/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 CP/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 CP/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 CP/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 CP/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 CP/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 CP/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 CP/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 CP/CPS and without changing the version number of this CP/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 CP/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 CP/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 CP/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 CP/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 CP/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 CP/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 CP/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 CP/CPS are intended for convenience and reference only and shall not be used in interpreting, construing, or enforcing any of the provisions of this CP/CPS.

Appendices and definitions to this CP/CPS are for all purposes an integral and binding part of the CP/CPS. If/when this CP/CPS conflicts with other rules, guidelines, or contracts, this CP/CPS, dated 14 July 2006, shall prevail and bind the Subscriber and other parties. If there is any conflict between the sections of this CP/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 CP/CPS may not assign any of their rights or obligations under this CP/CPS or applicable agreements without the written consent of DigiCert.

9.16.3 Severability

If any provision of this CP/CPS or the application thereof, is for any reason and to any extent found to be invalid or unenforceable, the remainder of this CP/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 CP/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 CP/CPS, no delay or omission by any party to exercise any right, remedy or power it has under this CP/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 CP/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 CP/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 CP/CPS shall be binding upon the successors, executors, heirs, representatives, administrators, and assigns, whether express, implied, or apparent, of the parties that this CP/CPS applies to. The rights and obligations detailed in this CP/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 CP/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

Domain Authorization Letter

(On Your Letterhead)

Dear DigiCert,

I confirm and warrant that:

DigiCert order number _____

Organization enrolling for the certificate is: _____ (Certificate Applicant)

The domain to be included in the certificate is: _____ (Fully Qualified Domain Name)

Registrant of the Domain is: _____ (Owner or Administrator of the domain name)

I am the registrant (and/or employed by the Registrant) and am duly authorized to sign this Domain Release Letter and to deal with all matters related to the registration of the Domain.

DigiCert recently received a request from Certificate Applicant to issue one or more Digital Certificate(s) under Certificate Applicant's name. Certificate Applicant desires to install the Digital Certificate on its web server(s) for the domain and ultimately to enable secure communications with its users.

Registrant acknowledges that it has granted Certificate Applicant the right to use the Domain in connection with its business and as a common name in the Digital Certificate request referenced above and any subsequent and/or additional certificates obtained by the Certificate Applicant during the validity of the above referenced certificate.

Registrant agrees to indemnify DigiCert and its directors, officers, agents, employees, contractors, parents, affiliates, or subsidiaries (collectively, the 'Indemnified Parties') and hold the Indemnified Parties harmless from and against any losses, costs, damages, and fees (including reasonable attorney's fees) incurred by the Indemnified Parties in connection with: (a) Any breach by Registrant of any representation or obligation under this letter or any domain name registration agreement between Registrant and the Registry governing the Domain name registration (collectively, the 'Indemnity Conditions'). Upon appropriate notice, Registrant shall defend, at its expense, any claim brought against one of more of the Indemnified Parties based on or arising out of one or more of the Indemnity Conditions.

Regards,

Full Name: _____

Job Title: _____

Signature: _____ (Must be hand written)

[To be signed by the domain registrant (if an individual person), or an employee of the domain registrant (if an organization)]

[** This document must accompany a personal photo ID of the signer such as a driver’s license or passport. Both should be faxed to 1-866-842-0223]

Appendix B

Certificate Profiles

1. DigiCert's Root Certificates

a. DigiCert Global 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 Global Root CA OU = www.digicert.com O = DigiCert Inc C = US
Validity Period	25 years expressed in UTC format
Subject Distinguished Name	CN = DigiCert Global Root CA OU = www.digicert.com O = DigiCert Inc C = US
Subject Public Key Info	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; 03 de 50 35 56 d1 4c bb 66 f0 a3 e2 1b 1b c3 97 b2 3d d1 55
Subject Key Identifier	c=no; 03 de 50 35 56 d1 4c bb 66 f0 a3 e2 1b 1b c3 97 b2 3d d1 55
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

b. DigiCert Assured ID 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 Assured ID Root CA OU = www.digicert.com O = DigiCert Inc C = US
Validity Period	25 years expressed in UTC format
Subject Distinguished Name	CN = DigiCert Assured ID Root CA OU = www.digicert.com O = DigiCert Inc C = US
Subject Public Key Info	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; 45 eb a2 af f4 92 cb 82 31 2d 51 8b a7 a7 21 9d f3 6d c8 0f
Subject Key Identifier	c=no; 45 eb a2 af f4 92 cb 82 31 2d 51 8b a7 a7 21 9d f3 6d c8 0f
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 Intermediate CA Certificates

a. DigiCert Global CA-1

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 Global Root CA OU = www.digicert.com O = DigiCert Inc C = US
Validity Period	15 years expressed in UTC format
Subject Distinguished Name	CN = DigiCert Global CA-1 OU = www.digicert.com O = DigiCert Inc C = US
Subject Public Key Info	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; 03 de 50 35 56 d1 4c bb 66 f0 a3 e2 1b 1b c3 97 b2 3d d1 55
Subject Key Identifier	c=no; 1e 1c 88 15 aa f2 46 d0 05 da e9 1e dc 22 bd a8 97 de 0f b2
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; {2.16.840.1.114412.1.3.0.3} [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 CP/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 Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://www.digicert.com/CACerts/DigiCertGlobalRootCA.crt
CRL Distribution Points	c = no; CRL HTTP URL =http://crl3.digicert.com/DigiCertGlobalRootCA.crl CRL HTTP URL =http://crl4.digicert.com/DigiCertGlobalRootCA.crl

b. DigiCert Assured ID CA-1

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 Assured ID Root CA OU = www.digicert.com O = DigiCert Inc C = US
Validity Period	15 years expressed in UTC format
Subject Distinguished Name	CN = DigiCert Assured ID CA-1 OU = www.digicert.com O = DigiCert Inc C = US
Subject Public Key Info	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; 45 eb a2 af f4 92 cb 82 31 2d 51 8b a7 a7 21 9d f3 6d c8 0f
Subject Key Identifier	c=no; 15 00 12 2b 13 98 b2 99 07 ed 1e df a2 be 57 0d 2b 67 02 cd
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; {2.16.840.1.114412.1.3.0.4} [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 CP/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 Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.digicert.com/CACerts/DigiCertAssuredIDRootCA.crt
CRL Distribution Points	c = no; CRL HTTP URL =http://crl3.digicert.com/DigiCertAssuredIDRootCA.crl CRL HTTP URL =http://crl4.digicert.com/DigiCertAssuredIDRootCA.crl

3. DigiCert End Entity Certificates

a. DigiCert Global CA-1 End Entity

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 Global CA-1 OU = www.digicert.com O = DigiCert Inc C = US
Validity Period	1, 2 or 3 years expressed in UTC format
Subject Distinguished Name	cn = <DNS Name of Website> ou = <Organizational Unit of Subscriber> o = <Full Legal Name of Subscriber> l = <Locality of Subscriber> s = <State of Subscriber> c = <country of Subscriber>
Subject Public Key Info	1024/2048-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; 1e 1c 88 15 aa f2 46 d0 05 da e9 1e dc 22 bd a8 97 de 0f b2
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	c=no; Certificate Policies c=no; {2.16.840.1.114412.1.3.0.3} [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 CP/CPS and the Relying Party Agreement which limit liability and are incorporated herein by reference.
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 Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://www.digicert.com/CACerts/DigiCertGlobalCA-1.crt
CRL Distribution Points	c = no; CRL HTTP URL = http://crl3.digicert.com/DigiCertGlobalCA-1.crl CRL HTTP URL = http://crl4.digicert.com/DigiCertGlobalCA-1.crl

b. DigiCert Assured ID CA-1 End Entity

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 Assured ID CA-1 OU = www.digicert.com O = DigiCert Inc C = US
Validity Period	1, 2 or 3 years expressed in UTC format
Subject Distinguished Name	cn = <DNS Name of Website> ou = <Organizational Unit of Subscriber> o = <Full Legal Name of Subscriber> l = <Locality of Subscriber> s = <State of Subscriber> c = <country of Subscriber>
Subject Public Key Info	1024/2048-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; 15 00 12 2b 13 98 b2 99 07 ed 1e df a2 be 57 0d 2b 67 02 cd
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	c=no; Certificate Policies c=no; {2.16.840.1.114412.1.3.0.4} [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 CP/CPS and the Relying Party Agreement which limit liability and are incorporated herein by reference.
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 Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://www.digicert.com/CACerts/DigiCertAssuredIDCA-1.crt
CRL Distribution Points	c = no; CRL HTTP URL = http://crl3.digicert.com/DigiCertAssuredIDCA-1.crl CRL HTTP URL = http://crl4.digicert.com/DigiCertAssuredIDCA-1.crl

4. DigiCert's Entrust-issued Intermediate CA Certificate

a. DigiCert Global 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 = Entrust.net Secure Server Certification Authority OU = (c) 1999 Entrust.net Limited OU = www.entrust.net/Certificate Policy incorp. by ref. (limits liab.) O = Entrust.net C = US
Validity Period	8 years expressed in UTC format
Subject Distinguished Name	CN = DigiCert Global CA OU = www.digicert.com O = DigiCert Inc C = US
Subject Public Key Info	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; a7 c7 13 a0 7a 01 3c 9d ef 82 48 82 48 d5 73 51 b6 12 56 2a
Key Usage	c=yes; Certificate Signing , Off-line CRL Signing , CRL Signing (06)
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) Secure Email (1.3.6.1.5.5.7.3.4) OCSP Signing (1.3.6.1.5.5.7.3.9)
Certificate Policies	Policy Identifier=1.2.840.113533.7.75.2
Basic Constraints	c=yes; cA=True; path length constraint = 0
Authority Information Access	None
CRL Distribution Points	http://crl.entrust.net/server1.crl

b. DigiCert Global CA End Entity

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 Global CA OU = www.digicert.com O = DigiCert Inc C = US
Validity Period	1, 2 or 3 years expressed in UTC format
Subject Distinguished Name	cn = <DNS Name of Website> ou = <Organizational Unit of Subscriber> o = <Full Legal Name of Subscriber> l = <Locality of Subscriber> s = <State of Subscriber> c = <country of Subscriber>
Subject Public Key Info	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; a7 c7 13 a0 7a 01 3c 9d ef 82 48 82 48 d5 73 51 b6 12 56 2a
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	c=no; Certificate Policies; {2.16.840.1.114412.1.3.0.1} [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 CP/CPS and the Relying Party Agreement which limit liability and are incorporated herein by reference.
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 Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://www.digicert.com/CACerts/DigiCertGlobalCA.crt
CRL Distribution Points	c = no; CRL HTTP URL = http://crl3.digicert.com/DigiCertGlobalCA.crl CRL HTTP URL = http://crl4.digicert.com/DigiCertGlobalCA.crl