DigiCert

Certificate Policy and Certification Practice Statement

DigiCert, Inc.
Version 3.03
February 14, 2007

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

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

Date	Changes	Version
	added l = locality and s = state of Subscriber fields to subject	

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

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.

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 tererith cff.5(b) (2iti)7.2(ons) (o7(r))13.9(i.pEt)1.2(ilure to comply)11.7(ories)6.6

-

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

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:

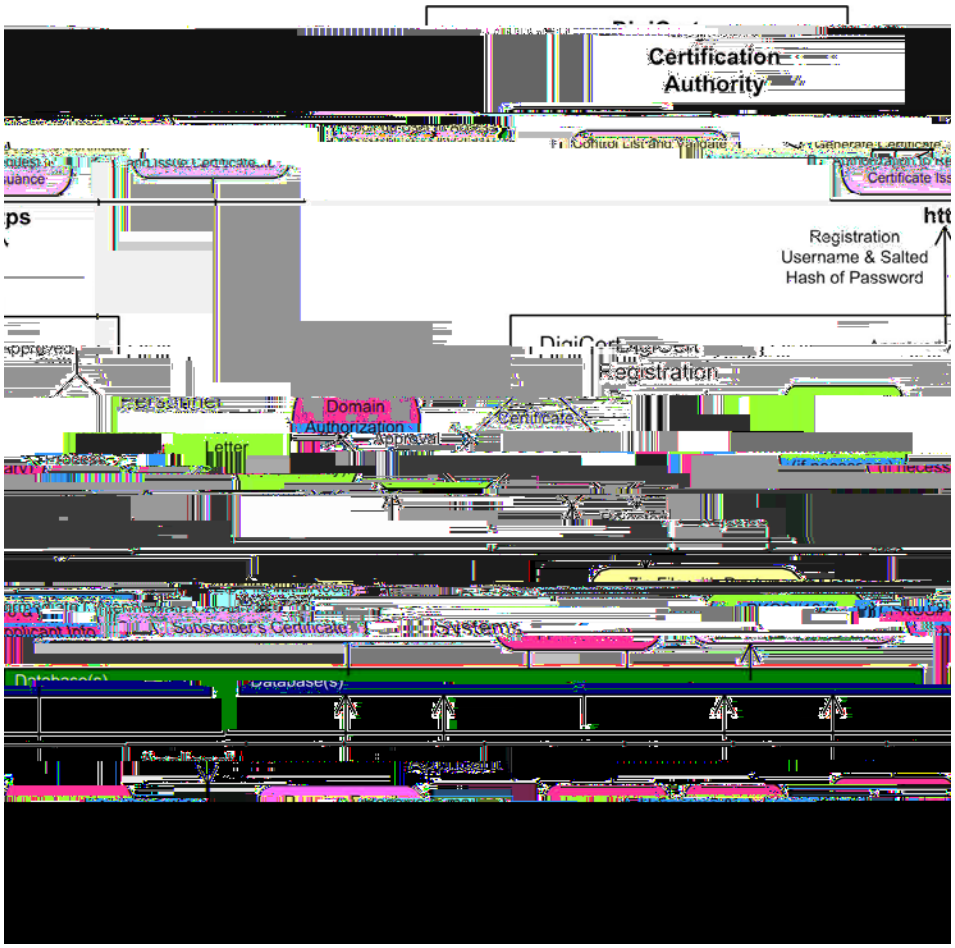

Figure 1.

In **Step 4** of the enrollment process, the Applicant pastes and submits the PKCS#10 CSR into a web

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 p

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

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

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

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

Auditable Event	CA System	Vetting Interface

Auditable Event	CA System

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

- 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).

6.2.7 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

6.4 Activation data

6.4.1 Activation data generation and installation

DigiCert uses its PIN-protected PED Keys and PED dev

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

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 WebTrusttA/ItASOtA 21188"),tA and other industry standards related to thetA operatAiontA oftA 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.

9.3.3 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 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.
-

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-

DigiCert-issued certificate.

-

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 co

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.

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 PREVENT(po)-47 TcNT(bD(Tc-.0022 T-R)-10.5(orc)iRBIDDEN OR)-2.2(io)7.3(n)7/AY

Appendix A

Domain Authorization Letter

(On Your Letterhead)

Dear DigiCert,

I confirm and warrant that:

DigiCert order number _____

Organization enrolling for the certificate is: _

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

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

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>

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>

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}

c. DigiCert Global CA End Entity Unified Communications Certificates

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
Netscape Certificate Type	c=no; SSL Client Authentication, SSL Server Authentication (c0)

Authority Information Access	c=no; Access Method= - Id-ad-ocsp (On-line Certificate Status Protocol - 1.3.6.1.5.5.7.48.1); URL =https://ocsp.digicert.com
CRL Distribution Points	c = no; CRL HTTP URL = http://crl3.digicert.com/DigiCertGlobalCA.crl CRL HTTP URL = http://crl4.digicert.com/DigiCertGlobalCA.crl