# DigiCert

# Certification Practice Statement for Extended Validation Certificates

**DigiCert, Inc.**
Version 1.0.1
February 21, 2007

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

**TABLE OF CONTENTS**

# 1. INTRODUCTION

## 1.1 Overview

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

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

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

(4) The Private Organization’s Jurisdiction of Incorporation and/or its Place of Business

## 1.5 Policy administration

### 1.5.1 Organization administering the document

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

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

### 1.5.2 Contact person

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

### 1.5.3 Person determining CPS suitability for the policy

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

### 1.5.4 CPS approval procedures

Approval of this CPS and any amendments hereto is by the DCPA. Amendments may be made by updating

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

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

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

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

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

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

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

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

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

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

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

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

(C) Authenti.7(f offe)1.4(r p)-5i.0102de Verificountr12-5.6(pt)-10.6( ph)-4.9(TD.0034 Tific9)]TJl0011 Tc91(o)1.TJ22.16671(r)s c

**Acronyms:**

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

# 2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

## 2.1 Repositories

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

## 2.2 Publication of certification information

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

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

## 2.3 Time or frequency of publication

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

## 2.4 Access controls on repositories

Parties (including Subscribers and Relying Parties) accessing the DigiCert Repository (http://www.digicert.com/ssl-cps-repository.htm) and other DigiCert publication resources are deemed to have agreed with the provisions of this CPS and any other conditions of usage that DigiCert may make available. Parties demonstrate acceptance of the conditions of usage of this CPS by using a DigiCert-issued EV Certificate. Failure to comply with the conditions of usage of the DigiCert Repositories and web site may result in termination of the relationship betw

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 nta i DigiC-9. harmla

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

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

1. **Common Name (cn) - Domain Name**

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

2. **Organization name (o)**

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

3. **City, State and Country**

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

4. **Subject Public Key**

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

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

1. **Confirmation of Correct Legal Name** by the Applicant of the correct Organization Name

EV Certificate Application on behalf of the Applicant; and

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

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

#### 3.2.2.2 EV Guideline Requirements for Authentication of Organizational Identity

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

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

Additionally, the Guidelines require that DigiCert verify the following prior to certificate issuance: actual, current legal existence and identity; physical location; telephone number; and ownership or control of the domain name of the Applicant. The Guidelines also

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

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

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

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

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

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

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

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

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

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

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

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

### 3.2.3 Authentication of individual identity

Not applicable.

### 3.2.4 Non-verified subscriber information

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

### 3.2.5 Validation of authority

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

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

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

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

The request for the EV Authorization Letter is directed to:

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

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

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

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

(b) The business address for such Confirming Person specified in a current Qualified Government Information Source (e.g., an SEC filing), a Qualified Independent Information Source, a Verified Legal Opinion, or a Verified Accountant Letter; or

(c) The address of Applicant's Registered Agent or Registered Office listed in the official records of the Jurisdiction of Incorporation.

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

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

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

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

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

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

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

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

**Step 10:** The Certificate Requester is notified that the Certificate has been created and

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

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

### 4.2.3 Time to process certificate applications

DigiCert makes reasonable efforts to confirm certificate application information and issue an EV Certificate within a reasonable time frame. The time frame is greatly dependent on the Applicant providing the necessary details and documentation in a timely manner. Upon the receipt of the necessary

### 4.4.2 Publication of the certificate by the CA

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

## 4.5 Key pair and certificate usage

### 4.5.1 Subscriber private key and certificate usage

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

### 4.5.2 Relying party public key and certificate usage

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

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

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

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

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

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

DigiCert receives notice or otherwise becomes aware that a Subscriber has breached a material obligation under the Subscriber Agreement;
Either the subscriber’s or DigiCert’s obligations under this CPS are delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's

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

Prior to approving revocation, DigiCert personnel approving the revocation request will create a record in the logging system containing DigiCert's reason for revocation.

A command to revoke the EV Certificate is processed and the CRL is updated. Upon revocation of an EV Certificate, the operational period of that certificate is immediately considered terminated. The serial number of the revoked certificate is placed within the CRL and remains until one additional CRL is published after the end of the certificate's validity period.

Revocation logs are maintained in accordance with the logging procedures covered in Section 5.5.1.2 of this CPS.

### 4.9.4 Revocation request grace period

There is no revocation grace period.

### 4.9.5 Time within which CA must process the revocation request

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

### 4.9.6 Revocation checking requirement for relying parties

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

### 4.9.7 CRL issuance frequency

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

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

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

### 4.9.8 Maximum latency for CRLs

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

### 4.9.9 On-line revocation/status checking availability

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

### 4.9.10 On-line revocation checking requirements

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

### 4.9.11 Other forms of revocation advertisements available

None.

### 4.9.12 Special requirements re key compromise

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

### 4.9.13 Circumstances for suspension

DigiCert does not utilize certificate suspension.

### 4.9.14 Who can request suspension

Not applicable.

### 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

discussion of actions or investigation results with the employee, he or she may be reassigned to a non-trusted role or dismissed from employment as appropriate.

### 5.3.7 Independent contractor requirements

Independent contractors who are assigned to perform trusted roles are subject to the duties and requirements specified for such roles in this Section 5.3 and are subject to sanctions stated above in Section 5.3.6.

### 5.3.8 Documentation supplied to personnel

Personnel in trusted roles are provided with the documentation necessary to perform the role to which they are assigned, including a copy of this CPS and all technical and operational documentation needed to maintain the integrity of DigiCert's CA operations. The information also includes internal system and security documentation, identity vetting policies and procedures, discipline-specific books, treatises and periodicals, and other information developed by DigiCert, provided to DigiCert by third parties or available over the Internet.

## 5.4 Audit logging procedures

### 5.4.1 Types of events recorded

All systems require identification and authentication at system logon with unique user name and

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

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

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

#### 5.5.1.2 Certificate Revocation

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

#### 5.5.1.3 Other Information

DigiCert also archives the following information concerning its CA operations:

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

### 5.5.2 Retention period for archive

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

### 5.5.3 Protection of archive

Archive records are stored at a secure off-site location and are maintained in a manner that prevents unauthorized modification, substitution or destruction.

### 5.5.4 Archive backup procedures

No stipul.1(ta)-5e227a(.1(t)7.2(d)7C7(th32 0 10.98 90 197.0401 Tm.0008 5c.0)-6.6(structi-4.5(lia )]m032m-4.5(rIam002 Tc.0024 Tw

# 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

## 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 tam1 T(e)-4.1(evn)1.9( dy)12.4(nt envel)1.9( ope/TT4 1 -156.0001 Tc.0725 Tw[(9)-10.1-4.1)-5(a)-4 , at le

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

### 6.2.9 Method of deactivating private key

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

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

### 6.2.10 Method of destroying private key

Initially, the CA private key can be destroyed by deleting it from all known storage partitions. However, the Luna SA device and associated PCMCIA backup tokens are also zeroized by performing ten (10) consecutive failed login attempts. This reinitializes the device and overwrites all of the data on it with binary zeros. In cases when this zeroization or re-initialization procedure fails, DigiCert will crush, shred and/or incinerate the device in a manner that destroys the ability to extract any private key.

### 6.2.11 Cryptographic Module Rating

See Section 6.2.1.

## 6.3 Other aspects of key pair management

### 6.3.1 Public key archival

DigiCert retains copies of all Public Keys for archival in accordance with Section 5.5.

### 6.3.2 Certificate operational periods and key pair usage periods

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

| | |
|---|---|
| Root CA | 25 years |
| Sub CA | 15 years |
| Subscriber | 1 year |

Pursuant to Section 5.6, DigiCert voluntarily retires its CA Private Keys from signing subordinate certificates before the periods listed above to accommodate the ke

### 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.

No stAppepis p7.6(o)-4.7(r)-1.2TJp9(e)-4.oto aDid bre insoto7(o)-11ures-23.56 oor tob(ss (3( )-5.6(o1ol. 7(h)-4.6(ich D)-(e)

## 6.5 Computer security controls

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

(1) Protect the confidentiality, integrity, and availability of: (i) all EV Certificate Requests and data related thereto (whether obtained from the Applicant or otherwise) in its possession or control or to which DigiCert has access (“EV Data”), and (ii)

are purchased or developed in the same manner as the original equipment or software and are installed and tested by trusted and trained personnel.

### 6.6.2 Security management controls

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

### 6.6.3 Life cycle security controls

No stipulation.

## 6.7 Network security controls

DigiCert's CA system is connected to one internal network and is protected by firewalls, a Demilitarized Zone (DMZ) and Network Address Translation for all internal IP addresses (e.g., 192.168.x.x). DigiCert's customer support and vetting workstations are also protected by firewall(s) and only use internal IP addresses. Root Keys are kept offline and brought online only when necessary to sign certificate-issuing subordinate CAs or periodic CRLs. Firewalls and boundary control devices are configured to allow access only by the addresses, ports, protocols and commands required for the trustworthy provision of PKI services by such systems. It is DigiCert's security policy to block all ports and protocols and open only necessary ports to enable CA functions. All CA equipment is configured with a minimum number of services and all unused network ports and services are disabled. All firewall configurations and changes thereto are documented, authorized, tested and implemented in accordance with change management policies and procedures. DigiCert's network configuration is available for review on-site by its auditors and consultants under an appropriate non-disclosure agreement

## 6.8 Time-stamping

See Section 5.5.5.

# 7. CERTIFICATE, CRL, AND OCSP PROFILES

Information for interpreting the following Certificate and CRL Profiles may be found in IETF's RFC 2459 (http://www.ietf.org/rfc/rfc2459.txt). DigiCert uses the ITU X.509, version 3 standard to construct digital certificates for use within the DigiCert PKI. X.509v3 allows a CA to add certain certificate extensions to the basic certificate structure. DigiCert use a number of certificate extensions for the purposes intended by X.509v3 as per Amendment 1 to ISO/IEC 9594-8, 1995.

## 7.1 Certificate profile

### 7.1.1 Version number(s)

All certificates are X.509 version 3 certificates.

### 7.1.2 Certificate extensions

*See* Appendix A.

### 7.1.3 Algorithm object identifiers

*See* Appendix A.

### 7.1.4 Name forms

*See* Appendix A and

## 8.2 Identity/qualifications of assessor

(1) Qualifications and experience. Auditing must be the individual's or group's primary business function. The individual or at least one member of the audit group must be qualified as a Certified Information Systems Auditor (CISA), an AICPA Certified Information Technology Professional (CPA.CITP), a Certified Internal Auditor (CIA), or have another recognized information security auditing credential.
(2) Expertise: The individual or group must be trained and skilled in the auditing of secure information systems and be familiar with public key infrastructures, certification systems, and the like, as well as Internet security issues (such as management of a security perimeter), operations of secure data centers, personnel controls, and operational risk management.
(3) Rules and standards: The individual or group must conform to applicable standards, rules, and best practices promulgated by the American Institute of Certified Public Accountants (AICPA), the Canadian Institute of Chartered Accountants (CICA), the Institute of Chartered Accountants of England & Wales (ICAEW), the International Accounting Standards adopted by the European Commission (IAS), Information Systems Audit and Control Association (ISACA), the Institute of Internal Auditors (IIA), or another qualified auditing standards body.
(4) Reputation: The firm must have a reputation for conducting its auditing business competently and correctly.
(5) Disinterest: The firm must have no financial interest, business relationship, or course of dealing that could foreseeably create a significant bias for or against DigiCert.

## 8.3 Assessor's relationship to assessed entity

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

## 8.4 Topics covered by assessment

Topics covered by the annual WebTrust EV Program for CAs audit include but are not limited to DigiCert's CA business practices disclosure (i.e., this CPS), the service integrity of DigiCert's CA operations, the environmental controls that DigiCert implements to ensure a trustworthy system and DigiCert's compliance with the EV Guidelines.

## 8.5 Actions taken as a result of deficiency

If an audit reports any material noncompliance with applicable law, this CPS, or any other contractual obligations related to the CA services described herein, DigiCert shall develop a plan to cure such noncompliance, subject to the approval of the DigiCert Policy Authority and any third party to whom DigiCert is legally obligated to satisfy. In the event DigiCert fails to take appropriate action in response to the report, then the DigiCert Policy Authority may instruct DigiCert's Operations Manager to revoke the certificates affected by such non-compliance.

## 8.6 Communication of results

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

## 8.7 Self-Audits

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

# 9. OTHER BUSINESS AND LEGAL MATTERS

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

## 9.1 Fees

### 9.1.1 Certificate issuance or renewal fees

DigiCert charges Subscriber fees for certificate issuance and renewal. Such fees are detailed on its web site (http://www.digicert.com

All private keys
Any activation data used to access private keys or gain access to the CA system
Any business continuity, incident response, contingency, and disaster recovery plans
Any other security practices, measures, mechanisms, plans, or procedures used to protect the confidentiality, integrity or availability of information
Any information held by DigiCert as private information in accordance with Section 9.4
Any transactional, audit log and archive record identified in Section 5.4 or 5.5, including certificate application records and documentation submitted in support of certificate applications whether successful or rejected.
Transaction records, financial audit records and external or internal audit trail records and any audit reports (with the exception of an auditor's letter confirming the effectiveness of the controls set forth in this CPS)

### 9.3.2 Information not within the scope of confidential information

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

### 9.3.3 Responsibility to protect confidential information

### 9.4.7 Other information disclosure circumstances

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

## 9.5 Intellectual property rights

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

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

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

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

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

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

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

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

Transactions effectuated using the private key corresponding to the public key included in the certificate are the acts of the Subscriber and that the certificate has been accepted and is properly operational at that time and until further notice to DigiCert.

The Subscriber retains control of the Subscriber's private key, uses a tr, u6v he.5(,214.6 se)1.6(y6)14(v.9(m, (o)-13ha d -52. th

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

### 9.6.5 Representations and Warranties of Other Participants

Not applicable.

## 9.7 Disclaimers of warranties

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

Any indirect, incidental or consequential damages.
Any costs, expenses, or loss of profits.
Any death or personal injury.
Any loss of data.
Any other indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, performance or non-performance of certificates or digital signatures.
Any other transactions or services offered within the framework of this CPS.
Any other damages except for those due to reliance, on the information featured on a certificate, or on the verified information in a certificate.
Any liability incurred in this case or any other case if the fault in this verified

## 9.10 Term and termination

### 9.10.1 Term

This CPS and any amendments hereto shall become effective upon publication in the Repository and shall remain in effect perpetually

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

### 9.16.5 Force Majeure

DIGICERT INCURS NO LIABILITY IF IT IS

# Appendix A

## Certificate Profiles

### 1. DigiCert's High Assurance EV Root CA

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

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

| Field | Value |
|---|---|
| Version | V3 (2) |
| Serial Number | Unique number |
| Issuer Signature Algorithm | sha-1WithRSAEncryption {1 2 840 113549 1 1 5} |
| Issuer Distinguished Name | Unique X.500 CA DN.<br>CN = DigiCert High Assurance EV Root CA<br>OU = www.digicert.com<br>O = DigiCert Inc<br>C = US |
| Validity Period | 15 years expressed in UTC format |
| Subject Distinguished Name | CN = DigiCert High Assurance EV CA-1<br>OU = www.digicert.com<br>O = DigiCert Inc<br>C = US |

## 3. DigiCert End Entity EV Certificates

| Field | Value | Comments |
|---|---|---|
| Version | V3 (2) | |
| Serial Number | Unique number | |

| | | |
|---|---|---|
| Incorporation | tateOrProvinceName (1.3.6.1.4.1.311.60.2.1.2) | X520StateOrProvinceName as specified in RFC 3280<br>Full name of Jurisdiction of Incorporation for an Incorporating Agency at the state or province level, including country information as follows, but not city or town |

Client Authentication