DigiCert

Certification Practice Statement for Extended Validation Certificates

DigiCert, Inc.
Version 1.0.3
April 2,2008

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

1. INTRODUCTION

1.1 Overview

This document is the DigiCert, Inc. (hereafter referred to as “DigiCert” where applicable) Certification Practice Statement (CPS) for Extended Validation Certificates and serves as a statement of the practices that DigiCert employs in providing certification services that meet the "Guidelines for the Issuance and Management of Extended Validation Certificates," version 1.0 (6/7/2007) (the "Guidelines") of the Certification Authority / Browser Forum ("CA/Browser Forum"). This CPS constitutes DigiCert's Statement of "EV Policies" as that term is used in the Guidelines. DigiCert conforms to the current version of the CA/Browser Forum Guidelines published at http://www.cabforum.org. In the event of any inconsistency between this document and those Guidelines, those Guidelines take precedence over this document.

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

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

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

This CPS also defines the underlying certification processes for Subscribers of EV Certificates and describes DigiCert’s Certification Authority (CA) and certificate repository operations. It is also a public statement of the practices of DigiCert, Inc. and serves to notify Subscribers and Relying Parties of their roles and responsibilities concerning Extended Validation ("EV") Certificates. Pursuant to the IETF

1.2 Document name and identification

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

Date	Changes	Version
11-20-2006	New Version	1.0
3-19-2007	Modified refund policy, warranty statement and limitation of liability language in Section 9 and added Certificate Profile for Root CA cross-certified by Entrust.	1.0.1
8-9-2007	Made changes to conform to final approved version EV Guidelines (including issuance to other types of entities).	1.0.2
4-2-2008	Updated address, and made changes to conform to Code Signing standards	1,0,3

As detailed in this CPS, DigiCert's EV certificate type is identified by the following object identifier

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

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

(1) The Private Organization MUST be a legally recognized entity whose existence was

To verify the validity of an EV Certificate they receive, relying parties must refer to the CRL or perform an Online Certificate Status Protocol check (http://ocsp.digicert.com) prior to relying on information featured in a certificate to ensure that DigiCert has not revoked the certificate. The location of the CRL distribution point is detailed within the EV Certificate.

1.4 Certificate usage

1.4.1. Appropriate certificate uses

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

1.4.2 Prohibited certificate uses

Certificates issued under the provisions of this CPS may not be used for: (i) any application requiring fail-safe performance such as: (a) the operation of nuclear power facilities, (b) air traffic control systems, (c) aircraft navigation systems, (d) weapons control systems, or (e) any other system whose failure could lead to injury, death or environmental damage; or (ii) transactions where applicable law prohibits the use of encryption or digital certificates for such transactions or where otherwise prohibited by law.

1.5 Policy administration

1.6 Definitions and acronyms

Applicant: The Applicant is a Private Organization, Government Entity or Business Entity applying for a Certificate.

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

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

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

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

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

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

Government Agency: In the case of a Private Organization, the government agency in the Jurisdiction of Incorporation under whose authority the legal existence of the Private Organization was established (e.g., the government agency that issued the Certificate of Incorporation). In the case of Business Entities, the government agency in the jurisdiction of operation that registers business entities. In the case of a Government Entity, the entity that enacted the law, regulation, or decree establishing the legal existence of the Government Entity.

Government Entity: A government-operated legal entity, agency, department, ministry, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).

Individual: A natural person.

Jurisdiction of Registration: In the case of a Business Entity, the state, province, locality where the organization has registered its business presence by filings by a Principal Individual involved in the business to verify its existence.

Legal Existence: A Private Organization, Government Entity or Business Entity has Legal Existence if it has been validly formed and not otherwise terminated, dissolved, or abandoned.

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

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

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

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

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

(1) data that will be relied upon has been independently verified by other independent information sources;

(2) the database distinguishes between self-reported data and data reported by independent information sources;

X.509 The ITU-T standard for Certificates and their corresponding authentication framework

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

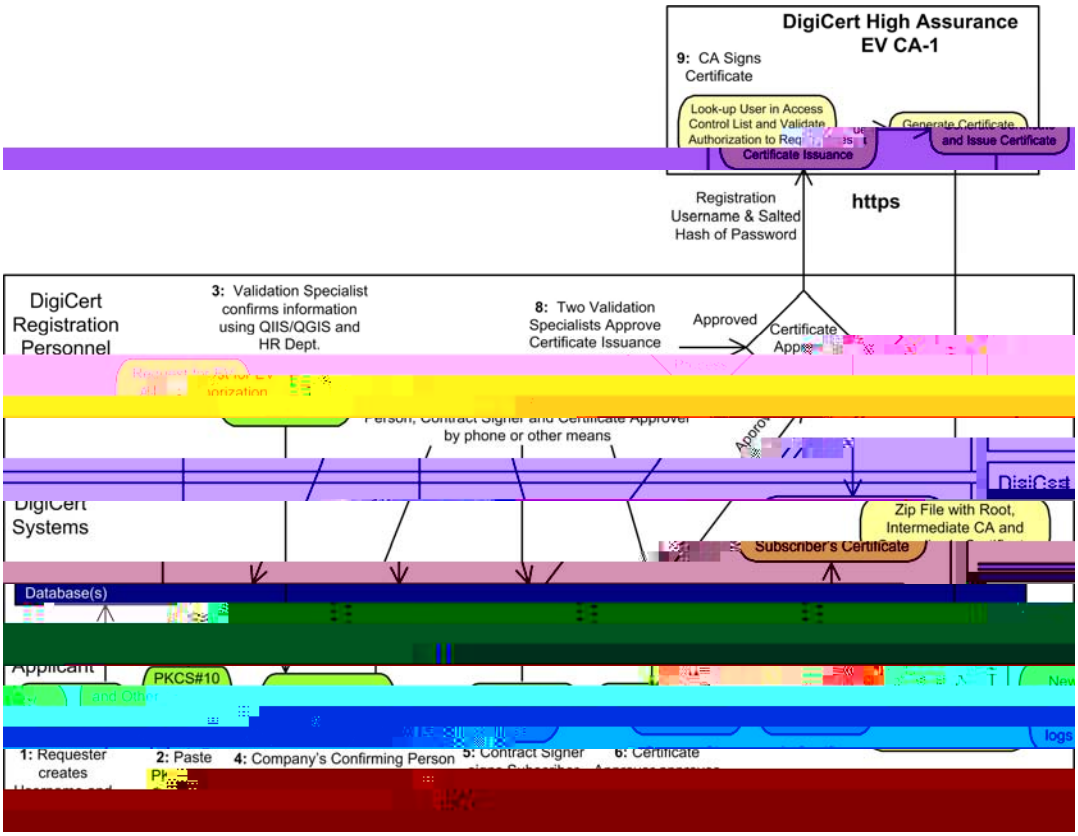

Figure 1.

3.2.1 Method to prove possession of private key

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

3.2.2 Authentication of organization identity

3.2.2.1 Data Elements Collected

The elements listed in this section are collected and utilized by DigiCert during the certificate issuance process to authenticate identity as discussed above. Elements that are already in the public domain (e.g., available via WHOIS, etc.) are not treated as confidential for purposes of the privacy and protection of data provisions outlined in Section 9.3 and Section 9.4 of this CPS.

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

1. Common Name (cn) - Domain Name

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

2. Organization name (o)

The Applicant's formal legal organization name to be included in EV Certificate, as recorded with the Government Agency in Applicant's Jurisdiction of Incorporation or Registration (for Private Organizations), or as specified in the law of Applicant's Jurisdiction of Incorporation or charter (for Government Entities). The "o=" MUST match the Applicant's full legal name and MAY include the Applicant's assumed name (e.g., d/b/a name) to be included in the EV

Certificate, as recorded in the Applicant's legal jurisdiction. However, if an assumed name is used, the "o=" MUST be in the format of "Assumed Name (Full Legal Name)."

3. City, State and Country

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

4. Subject Public Key

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

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

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

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

Verified Legal Opinion or Account Letter: DigiCert also accepts and relies on Verified Legal Opinions and Verified Accountant Letters to establish that th

(a) Face-to-face validation: The face-to-face validation MUST be conducted before either an employee of DigiCert, a Latin Notary, a Notary (or equivalent in Applicant's jurisdiction), a Lawyer, or Accountant ("Third-Party Validator"). The Principal Individual(s) MUST present the following documentation ("Vetting Documents") directly to the Third-Party Validator:

(i) A Personal Statement that includes the following information:

1. Full name or names by which a person is, or has been, known (including all other names used);
2. Residential Address at which he/she can be located;
3. Date of birth;
4. An affirmation that all of the information contained in the Certificate Request is true and correct.

(ii) A current signed government-issued identification document that includes a photo of the Individual and is signed by the Individual such as:

1. A passport;
2. A drivers license;
3. A personal identification card;
4. A concealed weapons permit;
5. A military ID.

(iii) At least two secondary documentary evidences to establish his/her identity that include the name of the Individual, one of which MUST be from a financial institution.

1. Acceptable financial institution documents include:
    a. A major credit card, provided that it contains an expiration date and it has not expired.
    b. A debit card from a regulated financial institution, provided that it contains an expiration date and it has not expired.
    c. A mortgage statement from a recognizable lender that is less than six months old.
    d. A bank statement from a regulated financial institution that is less than six months old.

Acceptable non-financial documents include:

1. Recent original utility bills or certificates from a utility company confirming the arrangement to pay for the services at a fixed address (not a mobile/cellular telephone bill).
2. A copy of a statement for a payment of a lease provided the statement is dated within the past six months.
3. A certified copy of a birth certificate.
4. A local authority tax bill for the current year.
5. A certified copy of a court order, such as a divorce certificate, annulment papers, or adoption papers.

The Third-Party Validator performing the face-to-face validation MUST:

1. Attest to the signing of the Personal Statement and the identity of the signer; and
2. Identify the original Vetting Documents used to perform the identification. In addition, the Third-Party Validator MUST attest on a copy of the current signed government-issued photo identification document that it is a full, true, and accurate reproduction of the original.

(b) Cross-checking of Information. DigiCert MUST obtain the original signed and attested Personal Statement together with the attested copy of the current signed government-issued photo identification document. DigiCert reviews the documentation to determine that the information is consistent, matches the information in the application and identifies the Individual.

(c) Verification of Third-party validator. DigiCert MUST independently verify that the Third-Party Validator is a legally-qualified Latin Notary or Notary (or legal equivalent in Applicant's jurisdiction),

Lawyer, or Accountant in the jurisdiction of the Individual's residency, and that the Third-Party Validator actually did perform the services and did attest to the signature of the Individual.

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, registered Principal Individual, or Registered Office in the Jurisdiction of Incorporation or Registration as listed in the official records of the Government Agency, with instructions that it be forwarded to an appropriate Confirming Person; or

(c) A named individual verified to be in the direct line of management above the Contract Signer or Certificate Approver by contacting Applicant's Human Resources Department by phone or mail (at the phone number or address for Applicant's Place of Business, verified in accordance with the EV Guidelines).

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 or Registration.

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

If the request for the EV Authorization Letter is made by telephone call, then the Confirming Person is

Common Name (CN=XYZ.com) contained in the PKCS#10 CSR. The Requester is required to verify that the full legal name of the organization (and if applicable, any assumed name) in the application is correct and that all records match. If the common name does not match, the Requester must make the necessary corrections and generate and re-submit a new PKCS#10 to proceed. (If other information does not match, a new PKCS#10 may or may not be required, depending on the server platform.) DigiCert registration personnel compare the information submitted by the Requester to ensure that it is consistent with the information in the WHOIS record before allowing the application process to continue.

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

4.2 Certificate application processing

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

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

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

Step 3:

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

Final Cross-Correlation and Due Diligence

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

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

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

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

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

(e) In the case where some or all of the documentation used to support the application is in a language other than English, a DigiCert employee skilled in such language having the appropriate training, experience, and judgment in confirming organizational identification and authorization performs the requirements of this Final Cross-Correlation and Due Diligence. When DigiCert employees do not possess the necessary language skills, DigiCert relies on language translations of the relevant portions of the documentation provided by a qualified Translator.

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

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

If the information in the certificate application cannot be confirmed, then DigiCert will reject the certificate application. DigiCert reserves the right to reject an application for an EV Certificate if, in its own assessment, the good and trusted name of DigiCert might be tarnished or diminished and may do so without incurring any liability or responsibility for any loss or expenses arising out of such refusal. DigiCert reserves the right not to disclose reasons for such a refusal.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Upon determining that all required steps have been completed, DigiCert registration personnel approve the issuance of the EV Certificate. As illustrated in Figure 1, when an EV Certificate is approved, a unique request string is sent to the CA via https. The request string contains the relevant parameters for the EV Certificate to be signed (e.g. PKCS #10 CSR, validity period, etc.) and authentication information for the DigiCert employee who is the Requester. The Requester's password is stored in the CA's access control database as a salted SHA-1 hash. Certificate access rights of DigiCert registration personnel (e.g. issue, revoke, retrieve) are managed by the CA system's access control database. The access control database determines whether the Requester has authorization to request certificate issuance from the specified CA key pair. If so, the CA system verifies the applicant's signature on the PKCS#10 CSR and extracts the

use the same PKCS#10 CSR as was used for the previous certificate. Otherwise, a new PKCS#10 CSR must be submitted and a new certificate is issued, provided that the subscriber meets the application validation and issuance requirements detailed for new customers, or otherwise qualifies for certificate renewal, above, or certificate modification/re-issue, below. Other aspects of certificate re-key (e.g., who may request re-key, notification of issuance, conduct constituting acceptance, and publication of the certificate) are the same as they are for initial certificate issuance. *See* Sections 3.3.1, 4.1, 4.2, 4.3 and 4.4.

4.8 Certificate modification

DigiCert does not allow modification of certificate details during the lifetime of the certificate. If any information on the certificate changes, the Subscriber must request revocation of the original certificate and request that a new certificate be issued. DigiCert may, at its discretion, credit a portion of the cost of the new certificate to the Subscriber's account. *See* Sections 4.1, 4.2, 4.3 and 4.4.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

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

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

For a party who is not the Subscriber, the filing of a "Certificate Problem Report" is the first step in

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.

CRLs for end-user Subscriber Certificates are issued at least once per day. CRLs for CA Certificates are issued twice annually, but also whenever a CA Certificate is revoked.

If a Certificate listed in a CRL expires, it may be removed from later-issued CRLs after the Certificate's expiration.

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

CRLsCRLs are posted to our online repository within a commercially reasonable time after generation. This is generally done automatically within one minute of generation.

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 rID /3ru0(yPrements re ke4)-5(y b)-5(e)2( )7(o42ft)7(o42 kevo610(o)2(o)]TJ-0.0017 Tc 0.0039 TJEM

person before a trusted person whose responsibility it is verify identity. The trusted person must verify the required forms of government-issued photo identification (e.g., passports and/or driver's licenses reviewed pursuant to U.S. Citizenship and Immigration Services Form I-9, Employment Eligibility Verification). Pre-employment checks include confirmation of previous employment, a check of professional references and confirmation of highest degree obtained. A criminal background check is performed on all trusted personnel before access is granted to DigiCert's certificate management system. These checks include, but are not limited to, verification of social security number, previous residences, driving records and criminal background.

5.3.3 Training requirements

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

io4(logs7Mo0.00771(.y)1w)2(i-5(m7t dn7il21(iqn7iuem7t dn7is8(a)e)7tro4(nas7Mme)7tdd7(ands7M1v6-8(o.0188567 d)

time, (ii) type of event, (iii) success or failure, and (iv) the user the initiating action, for the auditable events listed in the chart below.

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

Auditable Event	CA System	Vetting Interface

Auditable Event

vulnerability assessments. A written summary of the monthly review and vulnerability assessment is prepared that contains findings and recommendations for consideration by DigiCert's Operations Manager. These written reviews are also made available to DigiCert's auditor.

5.4.3 Retention period for audit log

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

5.4.4 Protection of audit log

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

5.4.5 Audit log backup procedures

No stipulation.

5.4.6 Audit collection system (internal vs. external)

No stipulation.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessments

See Section 5.4.2.

5.5 Records archival

5.5.1 Types of records archived

5.5.1.1 Certificate Issuance

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

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

- the subscriber's PKCS#10 CSR;
- Documentation of organizational existence for organizational applicants as listed in Section 3.2.2;
- Documentation of individual identity for individual applicants as listed in Section 3.2.3;
- Verification of organizational existence and status received from third party databases and government entities (including screen shots of web sites reporting such information);
- Screen shot of WHOIS record for domain name to be listed in the certificate;
- Mailing address validation (if different than those identified through the resources listed above);
-

- 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

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 failover in the event of a disaster (Disaster Recovery / Mirror Site). The DRBCP and supporting procedures are reviewed and tested periodically (at least on an annual basis) and are revised and updated as needed.

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

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

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

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

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

5.7.3 Entity private key compromise procedures

In the event that a DigiCert CA private key has been or is suspected to have been compromised, DigiCert's Operations Manager will immediately convene an emergency Incident Response Team to assess the situation to determine the degree and scope of the incident and take appropriate action, including implementation of DigiCert's Incident Response Plan, outlined as follows:

- Collect all information related to the incident (and if the event is ongoing, ensure that all data are being captured and recorded);
- Begin investigating incident and determine degree and scope;

- Incident Response Team determines the course of action or strategy that should be taken, (and in the case of Key Compromise, determining the scophat s(of Ke)-4hce ⁄c(r)lJSe

6.1.3 Public key delivery to certificate issuer

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

6.1.4 CA public key delivery to relying parties

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

6.1.5 c Kesite oblicicicicicicicicicic(0.8c)-5(b)]TJ0ricEa54ec8(om Digi)-6DTJEMCl-m10 09 Tc 0 Tw 1

PED Keys and PCMCIA devices under multi-person control as when performing other sensitive CA private key operations. The separation-of-duties/multi-party control provided by the PED and PED keys prevents a single individual from gaining access to the CA private key.

6.2.3 Private key escrow

DigiCert does not escrow private keys.

6.2.4 Private key backup

DigiCert's CA Private Keys are generated and stored inside the Luna SA module, which has been evaluated to at least FIPS 140 Level 3 and EAL 4+. Where such keys must be transferred to other media for backup and disaster recovery purposes, they are transferred a

(4) Protect against accidental loss or destruction of, or damage to, any EV Data or EV Processes; and
(5) Comply with all other security requirements applicable to DigiCert by law.

6.5.1 Specific computer security technical requirements

DigiCert's CA computer systems are equipped with Intel 64-bit processors/Intel chip sets. DigiCert's CA servers and support-and-vetting workstations run on Windows 2003, Windows XP Professional, and Linux operating systems. DigiCert's computer systems are configured and hardened using industry best practices. All operating systems require individual identification and authentication for authenticated logins and provide discretionary access control, access control restrictions to services based on authenticated identity, security audit capability and a protected audit record for shared resources, self-protection EMC BTpw 18.s Tc 0.0539 Tw2 0.347 0 Td6(d pro

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.

9.1.5 Refund policy

DigiCert charges the credit card submitted with Applicant's request for an EV Certificate. Applicants agree that the applicable certificate issuance fee includes a non-refundable application processing fee of $99. If Applicant's request is canceled or rejected, DigiCert will refund the certificate issuance fee minus

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

9.6 DigiCert Representations and Warranties

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

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

(B) Identity: DigiCert has confirmed that, as of the date the EV Certificate was issued, the legal name of the Subject named in the EV Certificate matches the name on the official government records of so3fgencor en[(co Td[(

the certificate.

- The certificate is used exclusively for authorized and legal purposes, consistent with this CPS, and that the Subscriber will use the certificate only in conjunction with the entity named in the organization field of the certificate
- The Subscriber agrees with the terms and conditions of this CPS and other agreements and policy statements of DigiCert.
-

- Any other indirect, consequential or punitive damages arising from or in connection with the

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

9.10 Term and termination

9.10.1 Term

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

9.10.2 Termination

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

9.10.3 Effect of termination and survival

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

9.11 Individual notices and communications with participants

DigiCert accepts notices related to this CPS by means of digitally signed messages or in paper form addressed to the locations specified in Section 2.2 of this CPS. Upon receipt of a valid, digitally signed acknowledgment of receipt from DigiCert, the sender of the notice shall deem their communication effective. The sender must receive such acknowledgment within five (5) days, or else written notice must then be sent in paper form through

expert's advice, co-operation monitoring and normal expert's advice) the parties agree to notify DigiCert of the dispute with a view to seek dispute resolution.

9.14 Governing law

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

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

9.15 Compliance with applicable law

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

9.16 Miscellaneous provisions

9.16.1 Entire agreement

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

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

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

9.16.2 Assignment

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

9.16.3 Severability

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

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

9.16.4 Enforcement (attorneys' fees and waiver of rights)

DigiCert reserves the right to seek indemnification and attorneys' fees from any party related to that party's conduct described in Section 9.9

Appendix A

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

Field	Value
Version	V3 (2)
Serial Number	Unique number
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Issuer Distinguished Name	CN = Entrust.net Secure Server Certification Authority OU = (c) 1999 Entrust.net Limited OU = www.entrust.net/CPS incorp. by ref. (limits liab.) O = Entrust.net C = US
Validity Period	September 30, 2006 (inclusive) [illegible]

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

Field	Value
Subject Public Key Information	RSA (2048 Bits)

3. DigiCert End Entity EV Certificates

		by the Subject or another entity (e.g., a hosting service). Wildcard certificates are not allowed for EV certificates.
City or Town of Incorporation or Registration		

Subject Key Identifier	c=no; Octet String – Same as calculated by CA from PKCS#10	