

Certicom Extended Validation (EV) Certificate Practice Statement

Certicom Corp.

Version 1.00

www.Certicom.com

Terms and Acronyms Used in the EV CPS

Acronyms:

CA	Certificate Authority
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CVC	Content Verification Certificate
EPKI	Enterprise Public Key Infrastructure Manager
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
MDC	Multiple Domain Certificate
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (based on X.509 Digital Certificates)
PKCS	Public Key Cryptography Standard
RA	Registration Authority
SGC	Server Gated Cryptography
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

Terms:

Affiliate of Certicom:	A corporation, partnership, joint venture or other entity controlling, controlled by or under common control with Certicom. As used in this definition, “control” (and its correlative meanings, “controlled by” and “under common control with”) means possession, directly or indirectly, of more than fifty percent (50%) of the voting shares of such entity or the power to direct the management and affairs of such entity.
Applicant:	Private Organization, Business Entity, or Government Entity that applies for (or seeks renewal of) an EV Certificate naming it as the Subject.
Applicant Representative:	An individual person employed by the Applicant: (i) who signs and submits, or approves an EV Certificate Request on behalf of an Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of an Applicant.
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 herein. Examples include general partnerships, unincorporated associations, and sole proprietorships.
CA:	See Certification Authority.

Certificate Authority (CA):	An organization agreeing to be bound by these Guidelines that is responsible for the creation, issuance, revocation, and management of EV Certificates. Where the CA is also the Root CA, references to the CA will be synonymous with Root CA.
Certificate Policy (CP):	A set of rules that indicates the applicability of a named certificate to a particular community and/or PKI implementation with common security requirements.
Certificate Revocation List (CRL):	A regularly updated time-stamped list of revoked or invalid EV Certificates that is created and digitally signed by the CA that issued the EV Certificates.
Certification Practice Statement (CPS):	One of several documents providing the framework under which certificates are created, issued, managed and used.
CRL:	See Certificate Revocation List
Demand Deposit Account:	a deposit account held at a bank or other financial institution, the funds deposited in which are payable on demand. The primary purpose of demand accounts is to facilitate cashless payments by means of check, bank draft, direct debit, electronic funds transfer, etc. Usage varies among countries, but a demand deposit account is commonly known as: a checking account, a share draft account, a current account, or a checking account.
Enterprise EV Certificate:	An EV Certificate that an Enterprise RA authorizes the CA to issue at third and higher domain levels that contain the domain that was included in an original Valid EV Certificate issued to the Enterprise RA.
Enterprise RA:	The Subject of a specified Valid EV Certificate that is authorized by the issuing CA to perform the RA function and authorize the CA to issue additional EV Certificates at third and higher domain levels that contain the domain that was included in the original EV Certificate, in accordance with the requirements of these Guidelines.
EV Certificate:	A certificate that contains information specified in these Guidelines and that has been validated in accordance with these Guidelines.
EV Certificate Request:	A request from an Applicant to the CA and requesting that the CA issue an EV Certificate to the Applicant, which request is validly authorized by the Applicant and signed by the Applicant Representative.
EV OID:	an identifying number, called an "object identifier," that is included in the certificatePolicies field of a certificate that: (i) indicates which CA policy statement relates to that certificate, and which, (ii) by pre-agreement with one or more Application Software Vendor, marks the certificate as being an EV Certificate.

Extended Validation Certificate:	See EV Certificate.
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.).
Incorporating 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 a Government Entity, the entity that enacted the law, regulation, or decree establishing the legal existence of the Government Entity.
Jurisdiction of Incorporation:	In the case of a Private Organization, the country and (where applicable) the state or province where the organization's legal existence was established by a filing with (or an act of) an appropriate government agency or entity (e.g., where it was incorporated). In the case of a Government Entity, the country and (where applicable) the state or province where the Entity's legal existence was created by law.
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.
Object Identifier (OID):	A unique alphanumeric/numeric identifier registered under the International Standards Organization's applicable standard for a specific object or object class.
OCSP Responder:	An online software application operated under the authority of the CA and connected to the Repository to process EV Certificate status requests. See also, Online Certificate Status Protocol.
OID:	See Object Identifier
Online Certificate Status Protocol (OCSP):	An online Certificate-checking protocol that enables an OCSP Responder to determine the status of an identified Certificate by contacting the Repository. See also OCSP Responder
Parent Company:	A parent company is defined as a company that wholly owns the Subsidiary Company and this can be verified by referencing a QIIS or from financial statement supplied by a registered Certified Public Accountant / Chartered Professional Accountant (CPA) or equivalent outside of the USA.
Place of Business:	The location of any facility (such as a factory, retail store, warehouse, etc) where the Applicant's business is conducted.

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 Key:	The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.
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) the Incorporating Agency in its Jurisdiction of Incorporation.
Public Key:	The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.
Public Key Infrastructure (PKI):	A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.
Registration Agency:	a Governmental Agency that registers business information in connection with an entity's business formation or authorization to conduct business under a license, charter or other certification. A Registration Agency may include, but is not limited (i) a State Department of Corporations or a Secretary of State; (ii) a licensing agency, such as a State Department of Insurance; or (iii) a chartering agency, such as a state office or department of financial regulation, banking or finance, or a federal agency such as the Comptroller of Currency (OCC) or Office of Thrift Supervision (OTC).
Registered Agent:	An individual or entity that is both: <ul style="list-style-type: none"> a. authorized by the Applicant to receive service of process and business communications on behalf of the Applicant; and b. listed in the official records of the Applicant's Jurisdiction of Incorporation as acting in the role specified in (a) above.
Registered Office:	the official address of a company, as recorded with the Incorporating Agency or Registration Agency, to which official documents are sent and legal notices received.
Registration Number:	The unique number assigned to the Private Organization Applicant or Subject entity by the Incorporating Agency or Registration Agency in such entity's Jurisdiction of Incorporation or Registration.

Regulated Financial Institution:	A financial institution that is regulated, supervised, and examined by governmental, national, state or provincial, or local authorities having regulatory authority over such financial institution based on the governmental, national, state or provincial, or local laws under which such financial institution was organized and/or licensed.
Relying Party:	Any person (individual or entity) that relies on a Valid EV Certificate. An Application Software Vendor is not considered a Relying Party when software distributed by such Vendor merely displays information regarding an EV Certificate.
Repository:	An online database of EV Certificate status information, either in the form of a CRL or an OCSP responder.
Root CA:	The top level certification authority that issues the self-signed Root Certificate under which the CA issues EV Certificates.
Root Certificate:	The self-signed certificate issued by the Root CA to identify itself and to facilitate signing of certificates identifying Subordinate CAs.
Root Key:	The Private Key and its associated Public Key that identifies the Root CA.
Subject:	The organization identified as the Subject in the Subject:organizationName field of an EV Certificate, whose identity is unambiguously bound to a Public Key also specified in the EV Certificate. An Applicant is also a Subject once the EV Certificate it requested is issued.
Subordinate CA:	Certification authority whose certificates are signed by the Root CA, or another Subordinate CA. A Subordinate CA may issue EV Certificates if the appropriate EV OID(s) or the special anyPolicy OID is specified in the certificatePolicies extension.
Subscriber:	The Subscriber is an entity that has been issued a certificate.
Subscriber / Subscribing Organization:	The organization identified as the Subject in the Subject:organizationName field of an EV Certificate issued pursuant to these Guidelines, as qualified by the Jurisdiction of Incorporation information in the EV Certificate.
Subscriber Agreement:	An agreement between Certicom and the Subject named or to be named in an EV Certificate that specifies the right sand responsibilities of the parties, and that complies with the requirements of these Guidelines.
Subsidiary Company:	A subsidiary company is defined as a company that is wholly owned by Applicant as verified by referencing a QIS or from financial statement supplied by a registered Certified Public Accountant / Chartered Professional Accountant (CPA) or equivalent outside of the USA.

Superior Government Entity:	Based on the structure of government in a political subdivision, the Government Entity or Entities that have the ability to manage, direct and control the activities of Applicant.
Technical Representative:	A person authorized by the Applicant or the Applicant Representative to submit EV Certificate Requests on behalf of the Applicant.
Translator:	An individual or Business Entity that Certicom has reason to believe possesses the requisite knowledge and expertise to accurately translate the words of a document written in one language to English.
Trustworthy System:	Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.
Valid:	An EV Certificate that has not expired and has not been revoked.
WebTrust EV Program:	The additional audit procedures specified for CAs that issue EV Certificates by the AICPA/CICA to be used in conjunction with its WebTrust Program for Certification Authorities.
WebTrust Program for CAs:	The then-current version of the AICPA/CICA WebTrust Program for Certification Authorities, available at http://www.webtrust.org/certauth_fin.htm .

1 General

This document is the Certicom Extended Validation Certification Practice Statement (EV CPS) and outlines the legal, commercial and technical principles and practices that Certicom employs in providing certification services that include, but are not limited to, approving, issuing, using and managing of EV Certificates and in maintaining an X.509 Certificate based public key infrastructure (PKI) in accordance with the Certificate Policies determined by Certicom. It also defines the underlying certification processes for Subscribers and describes Certicom's repository operations. The EV CPS is also a means of notification of roles and responsibilities for parties involved in Certificate based practices within the Certicom PKI.

1.1 Certicom

Certicom is a Certification Authority (CA) that issues high quality and highly trusted Extended Validation digital certificates ("EV Certificates") to private organizations, government entities, and other business entities in accordance with this EV CPS. In its role as a CA, Certicom performs functions associated with public key operations that include receiving requests, issuing, revoking and renewing a digital certificate and the maintenance, issuance and publication of Certificate Revocation Lists (CRLs) for users within the Certicom PKI. In delivering its PKI services Certicom complies in all material respects with high-level international standards, including those on Qualified Certificates pursuant to the European Directive 99/93, the relevant law on electronic signatures, the CA/Browser Forum Guidelines for Extended Validation Certificates and all other relevant legislation and regulation.

Certicom may extend, under agreement, membership of its PKI to approved third parties known as Registration Authorities. The international network of Certicom RAs share Certicom's policies, practices, and CA infrastructure to issue Certicom digital certificates, or if appropriate, private labeled digital certificates.

1.2 Certicom EV CPS

The Certicom EV CPS is a public statement of the practices of Certicom and the conditions of issuance, revocation and renewal of an EV Certificate issued under Certicom’s own hierarchy. Pursuant to the division of the tasks of a CA, this EV CPS is largely divided in the following sections: Technical, Organizational, Practices and Legal.

The Certicom Certificate Policy Authority maintains this EV CPS, related agreements and Certificate policies referenced within this document. The Certificate Policy Authority may be contacted at the below address:

Certificate Policy Authority
Certicom Corp.
5520 Explorer Drive, 4th Floor
Mississauga, Ontario L4W 5L1 Canada

This EV CPS, related agreements and Certificate policies referenced within this document are available online in the Certicom Repository.

1.3 EV CPS Suitability, Amendments and Publication

The Certicom Certificate Policy Authority is responsible for determining the suitability of certificate policies described within this EV CPS. The Authority is also responsible for determining the suitability of proposed changes to the EV CPS prior to the publication of an amended edition.

Upon the Certificate Policy Authority accepting such changes deemed by Certicom’s Policy Authority to have significant impact on the users of this EV CPS, an updated edition of the EV CPS will be published at the Certicom Repository with seven (7) days notice given of upcoming changes and suitable incremental version numbering used to identify new editions.

Revisions not denoted “significant” are those deemed by Certicom’s Policy Authority to have minimal or no impact on subscribers and relying parties using certificates and CRLs issued by CA. Such revisions may be made without notice to users of the EV CPS and without changing the version number of this EV CPS.

Controls are in place to reasonably ensure that the Certicom EV CPS is not amended and published without the prior authorization of the Certificate Policy Authority.

1.4 Other Practice Statements & Agreements

The EV CPS is only one of a set of documents relevant to the provision of EV Certification Services by Certicom. The list of documents related to EV Certificates contained in this clause are other documents that Certicom may include in the Repository, and which may or may not apply to EV Certificates. The document name, location of and status, whether public or private, are detailed below. The Certicom Repository can be found at www.Certicom.com/repository.

Document	Status	Location
Certicom Certification Practice Statement	Public	Certicom Repository
Certicom EV Certification Practice Statement	Public	Certicom Repository
EV Subscriber Agreement	Public	Certicom Repository
Relying Party Agreement	Public	Certicom Repository
Relying Party Warranty	Public	Certicom Repository
Reseller Agreement	Confidential	Presented to partners accordingly

Reseller Guide	Confidential	Presented to partners accordingly
----------------	--------------	-----------------------------------

1.5 Liability of Certicom

For legal liability of Certicom under the provisions made in this EV CPS, please refer to Section 5.

1.6 Compliance with applicable standards

The practices specified in this EV CPS have been designed to meet or exceed the requirements of generally accepted and developing industry standards, including the AICPA/CICA WebTrust Program for Certification Authorities; ANS X9.79:2001 PKI Practices and Policy Framework; CA/Browser Forum Guidelines for Extended Validation Certificates (“EV Guidelines”) and other industry standards related to the operation of CAs.

A regular audit is performed by an independent external auditor to assess Certicom’s compliance with the AICPA/CICA WebTrust program for Certification Authorities. Topics covered by the annual audit include, but are not limited to, the following:

- CA business practices disclosure
- Service integrity
- CA environmental controls

Certicom conforms to the current version of the CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Certificates (“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.

1.6.1 Audits

Certicom has successfully complete a point-in-time readiness assessment audit against the WebTrust EV Program, or a point-in-time readiness assessment audit against equivalent audit procedures approved by the CA/Browser Forum.

Certicom strictly control its service quality by performing ongoing self audits against a randomly selected sample of at least three percent of the EV Certificates it has issued in the period beginning immediately after the last sample was taken. For all EV Certificates where the final cross correlation and due diligence requirements of Section 24 of these Guidelines is performed by an RA Certicom strictly control its service quality by performing ongoing self audits against a randomly selected sample of at least six percent of the EV Certificates it has issued in the period beginning immediately after the last sample was taken.

Certicom undergoes an annual (i) WebTrust Program for CAs audit and (ii) WebTrust EV Program audit, or an equivalent for both (i) and (ii) as approved by the CA/Browser Forum. Such audits cover all CA obligations under these Guidelines regardless of whether they are performed directly by Certicom or delegated to an RA or subcontractor.

The audit report are made publicly available.

All audits required under these Guidelines are performed by a Qualified Auditor. A Qualified Auditor:

- (1) is an independent public accounting firm that has proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function and be

currently licensed to perform WebTrust for CA audits and WebTrust EV Program audits, or to perform such alternate equivalent audits approved by the CA/Browser Forum as will be performed; and

- (2) is a member of the American Institute of Certified Public Accountants (AICPA), or a non-US equivalent that requires that audits be completed under defined standards that include the possession of certain skill sets, quality assurance measures such as peer review, competency testing, standards with respect to proper assignment of staff to engagements, and requirements for continuing professional education; and
- (3) maintains Professional Liability/Errors & Omissions insurance, with policy limits of at least \$1 million in coverage.

1.7 Digital Certificate Policy Overview

A digital certificate is formatted data that cryptographically binds an identified subscriber with a public key. A digital certificate allows an entity taking part in an electronic transaction to prove its identity to other participants in such transaction. Digital certificates are used in commercial environments as a digital equivalent of an identification card.

An Extended Validation Certificate (“EV Certificate”) is a certificate that contains information specified in the EV Guidelines and that has been validated in accordance with the EV Guidelines.

1.8 Certicom PKI Hierarchy

Certicom uses the Certicom Extended Validation SSL CA, the Certicom ECC 256 Extended Validation SSL CA, and the Certicom ECC 384 Extended Validation SSL CA for issuing EV Certificates. The following high-level representation of the Certicom PKI is used to illustrate the hierarchy utilized.

1.8.1. EV Certificates

Visible on Browsers on platforms that Trust the “Certicom Certification Authority” root as follows:

Certicom RSA Public Primary CA (*serial number = 44 20 79 44 3F B8 89 FD AD 3B FB BA A5 49 9B 51, expiry = 31 December 2029 23:59:59*)

↳ Certicom RSA Extended Validated SSL CA (*serial number = TBA, expiry = 31 December 2026 23:59:59*)

↳ End Entity EV SSL Certificate (*serial number = x, expiry = 1 month or up to 27 months from issuance*)

Certicom ECC Public Primary CA (*serial number = 45 AC 56 5D 72 EA A2 16 01 90 64 34 0B C1 B3 B2, expiry = 18 January 2038 23:59:59*)

↳ Certicom ECC 256 Extended Validation SSL CA (*serial number = TBA, expiry = 18 January 2035 23:59:59*)

↳ End Entity EV SSL Certificate (*serial number = x, expiry = 1 month or up to 27 months from issuance*)

Certicom ECC Public Primary CA (*serial number = 45 AC 56 5D 72 EA A2 16 01 90 64 34 0B C1 B3 B2, expiry = 18 January 2038 23:59:59*)

↳ Certicom ECC 384 Extended Validation SSL CA (*serial number = TBA, expiry = 18 January 2035 23:59:59*)

- ↳ End Entity EV SSL Certificate (*serial number = x, expiry = 1 month or up to 27 months from issuance*)

1.9 Certicom Certification Authority

In its role as a Certification Authority (CA) Certicom provides certificate services within the Certicom PKI. Certicom will:

- Conform its operations to this EV CPS (or other CA business practices disclosure), as the same may from time to time be modified by amendments published in the Certicom Repository.
- Upon receipt of a valid request to revoke the certificate from a person authorized to request revocation using the revocation methods detailed in this EV CPS, revoke a certificate issued for use within the Certicom PKI.
- Publish CRLs on a regular basis, in accordance with the applicable Certificate Policy and with provisions described in this EV CPS.
- Distribute issued certificates in accordance with the methods detailed in this EV CPS.
- Update CRLs in a timely manner as detailed in this EV CPS.
- Notify subscribers via email of the imminent expiry of their Certicom issued certificate (for a period disclosed in this EV CPS).

1.10 Certicom Registration Authorities

Certicom may delegate the performance of all or any part of a requirement of the EV Guidelines to an Affiliate, a Registration Authority (RA) or subcontractor. This process fulfills all of the requirements of Section 25 of the EV Guidelines. Affiliates and/or RAs comply with the qualification requirements of trustworthiness and competence found in this EV CPS and the EV Guidelines.

Certicom RAs:

- Accept, evaluate, approve, or reject the registration of certificate applications,
- Verify the accuracy and authenticity of application information provided by a subscriber as specified in the Certicom validation guidelines,
- Use official, notarized, or otherwise acceptable documentation to evaluate a subscriber application, and
- Verify the accuracy and authenticity of the information provided by a subscriber at the time of reissue or renewal as specified herein.

A Certicom RA acts within its own geographical or business partnerships with Certicom's approval and authorization and may issue certificates that it has validated. RAs are restricted to operating only within the validation guidelines published by Certicom and must agree to do so prior to or when the RA joins the program. Certificates issued through an RA contain an amended Certificate Profile within the issued certificate to represent to a Relying Party the involvement of the RA in the issuance process.

Certificates issued by RAs that are compliant with and operating under Certicom's practices and procedures have the same warranty as those certificates issued under Certicom's own root as limited by the terms and conditions set forth herein.

1.10.5 Enterprise RAs

Certicom may contractually authorize the Subject of a specified valid EV Certificate to perform the RA function and authorize Certicom to issue additional EV Certificates at third and higher domain levels that contain the domain that was included in the original EV Certificate (also known as "Enterprise EV Certificates"). In such case, the Subject shall be considered an Enterprise RA, and the following shall apply:

- (i) no Enterprise RA may authorize Certicom to issue an Enterprise EV Certificate at the third or higher domain levels to any Subject other than the Enterprise RA or a business that is owned or directly controlled by the Enterprise RA;
- (ii) in all cases, the Subject of an Enterprise EV Certificate must be an organization verified by Certicom in accordance with the EV Guidelines;
- (iii) Certicom will impose these limitations as a contractual requirement with the Enterprise RA and monitor compliance by the Enterprise RA;
- (iv) the Final Cross-Correlation and Due Diligence requirements of Section 4.2.11 of this EV CPS may be performed by a single person representing the Enterprise RA; and
- (v) the audit requirements in Section 35 of the EV Guidelines will not apply to the Enterprise RA if Certicom maintains control over the root key or sub-root key used to issue the enterprise certificates, but the audit must cover the Enterprise RA in all other cases.

1.11 Subscribers

Subscribers of Certicom services are individuals or companies that use PKI in relation with Certicom supported transactions and communications. Subscribers are parties that are identified in an EV Certificate and hold the private key corresponding to the public key listed in the certificate. Prior to verification of identity and issuance of a certificate, a Subscriber is an Applicant for the services of Certicom.

1.12 Relying Parties

Relying parties may use PKI services in relation with Certicom EV Certificates for their intended purposes and may reasonably rely on such certificates and/or digital signatures verifiable with reference to a public key listed in a subscriber' certificate.

To verify the validity of a digital certificate they receive, relying parties must refer to the Certificate Revocation List (CRL) prior to relying on information featured in a certificate to ensure that Certicom has not revoked the certificate. The CRL location is detailed within the certificate.

2 Technology

This section addresses certain technological aspects of the Certicom infrastructure and PKI services.

2.1 Certicom Infrastructure

The Certicom Infrastructure uses trustworthy systems to provide certificate services. A trustworthy system is computer hardware, software and procedures that provide an acceptable resilience against security risks, provide a reasonable level of availability, reliability and correct operation, and enforce a security policy.

2.1.1 Root CA Signing Key Protection & Recovery

The Certicom certificates for signing EV Certificates are shown below in Table 2.1.1. Protection of Certicom Root signing key pairs is ensured with the use of nCipher nShield 500 cryptographic coprocessor devices, which are certified to FIPS 140-1 Level 3, for key generation, storage and use. Certicom Root signing key pairs are 2048 bit and were generated within the nCipher device.

For CA Root key recovery purposes, the Root CA signing keys are encrypted and stored within a secure environment. The decryption key is split across **m** removable media and requires **n** of **m** to reconstruct the decryption key. Custodians in the form of two or more authorized Certicom

officers are required to physically retrieve the removable media from the distributed physically secure locations.

Where CA Root signing keys are backed up to another cryptographic hardware security module, such keys are transferred between devices in encrypted format only.

Table. 2.1.1

CA Number	Description	Usage	Lifetime	Size
6	Certicom RSA Extended Validation SSL CA	Intermediate certificate for RSA Extended Validation SSL certificates	January 18, 2035	RSA 2048
10	Certicom ECC 256 Extended Validation SSL CA	Intermediate certificate for 284-bit Extended Validation SSL certificates	December 31, 2026	ECC 256
12	Certicom ECC 384 Extended Validation SSL CA	Intermediate certificate for 384-bit Extended Validation SSL certificates	January 18, 2035	ECC 384

Certicom protects its Root key pairs in accordance with its AICPA/CICA WebTrust program compliant infrastructure and EV CPS. Details of Certicom’s WebTrust compliance are available at Certicom’s official website (www.Certicom.com).

2.1.2 CA Root Signing Key Generation Process

Certicom securely generates and protects its own private key(s) using a trustworthy system (nCipher nShield 500 accredited to FIPS PUB 140-1 level 3), and takes necessary precautions to prevent the compromise or unauthorized usage of it.

The Certicom Root keys were generated in accordance with the guidelines detailed in the Root Key Generation Ceremony Reference. The activities undergone and the personnel involved in the Root Key Generation Ceremony are recorded for audit purposes. Subsequent Root Key Generation Ceremonies are to follow the documented reference guide also.

2.1.3 CA Root Signing Key Archival

When any CA Root Signing Key pair expires, they will be archived for at least 7 years. The keys will be archived in a secure cryptographic hardware module, as per their secure storage prior to expiration, as detailed in section 2.1.1 of this EV CPS.

2.1.4 Procedures employed for CA Root Signing Key Changeover

The lifetime of Certicom keys is set out in Table 2.1.1. Toward the end of each private key’s lifetime, a new CA signing key pair is commissioned and all subsequently issued certificates and CRLs are signed with the new private signing key. Both keys may be concurrently active. The corresponding new CA public key certificate is provided to subscribers and relying parties through the delivery methods detailed in section 2.1.5 of this EV CPS.

2.1.5 CA Root Public Key Delivery to Subscribers

Certicom makes all its CA Root Certificates available in its online Repository.

Certicom provides the full certificate chain (see section 1.8 of this EV CPS) to the Subscriber upon issuance and delivery of the Subscriber certificate.

2.1.6 Physical CA Operations

2.1.6.1 Access and Facilities

Access to the secure part of Certicom facilities is limited using physical access control and is only accessible to individuals appropriately authorized pursuant to section 3.10 of this EV CPS (referred to herein as Trusted Personnel). Certicom ensures the system used to process and approve EV Certificate Requests requires actions by at least two trusted persons before the EV Certificate is created. Card access systems are in place to control, monitor and log access to all areas of the facility. Access to the Certicom physical machinery within the secure facility is protected with locked cabinets and logical access control. Certicom has made reasonable efforts to ensure its secure facilities are protected from:

- Fire and smoke damage (fire protection is made in compliance with local fire regulations).
- Flood and water damage.

Certicom secure facilities have a primary and secondary power supply and ensure continuous, uninterrupted access to electric power. Heating / air ventilation systems are used to prevent overheating and to maintain a suitable humidity level.

2.1.6.2 Security Program

Certicom implements and maintains a comprehensive Security Program 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 Certicom's possession or control or to which Certicom has access ("EV Data"), and (ii) the keys, software, processes, and procedures by which Certicom verifies EV Data, issues EV Certificates, maintains a Repository, and revokes EV Certificates ("EV Processes");
- (2) Protect against any anticipated threats or hazards to the confidentiality, integrity, and availability of the EV Data and EV Processes;
- (3) Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any EV Data or EV Processes;
- (4) Protect against accidental loss or destruction of, or damage to, any EV Data or EV Processes; and
- (5) Comply with all other security requirements applicable to Certicom by law.

Certicom's Security Program includes regular risk assessments ("Risk Assessments") that:

- (1) Identify reasonably foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any EV Data or EV Processes;
- (2) Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the EV Data and EV Processes; and
- (3) Assess the sufficiency of the policies, procedures, information systems, technology, and other arrangements that Certicom has in place to control such risks.

Based on such Risk Assessment, Certicom implements and maintains a Security Plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to reasonably manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the EV Data and EV Processes, as well as the complexity and scope of the activities of Certicom. Such Security Plan includes administrative, organizational, technical, and physical safeguards appropriate to the size, complexity, nature, and scope of the Certicom's business and the EV Data and EV Processes. Such Security Plan also takes into account the available technology and the cost of implementing the specific measures,

and implements a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

Certicom ensures that the system used to process and approve EV Certificate Requests requires actions by at least two trusted persons before the EV Certificate is created.

2.2 Digital Certificate Management

Certicom certificate management refers to functions that include but are not limited to the following:

- Verification of the identity of an applicant of a certificate.
- Authorizing the issuance of certificates.
- Issuance of certificates.
- Revocation of certificates.
- Listing of certificates.
- Distributing certificates.
- Publishing certificates.
- Storing certificates.
- Retrieving certificates in accordance with their particular intended use.
- Verification of the domain of an applicant of a certificate
- Verification that the entity named in the EV Certificate has authorized the issuance of the EV Certificate.

Certicom conducts the overall certification management within the Certicom PKI; either directly or through a Certicom approved RA. Certicom is not involved in functions associated with the generation, issuance, decommissioning or destruction of a Subscriber key pair.

2.3 Certicom Directories, Repository and Certificate Revocation Lists

Certicom manages and makes publicly available directories of revoked certificates using Certificate Revocation Lists (CRLs) that is available online 24x7. All CRLs issued by Certicom are X.509v2 CRLs, in particular as profiled in RFC3280. Users and relying parties are strongly urged to consult the directories of revoked certificates at all times prior to relying on information featured in a certificate. Certicom updates and publishes a new CRL for end entity certificates every 24 hours or more frequently under special circumstances. The CRL for end entity certificates can be accessed via <http://crl.Certicom.comt/EVSSLCA.crl>

Subordinate CA Certificates issued to entities not controlled by the entity that controls the Root CA CRLs are updated and reissued at least every seven days, and the nextUpdate field value is not be more ten days

For subordinate CA Certificates controlled by the Root CA, CRLs are updated and reissued at least every twelve months, and the nextUpdate field value is not more twelve months.

Certicom ensures that all CRLs for EV Certificate chains can be downloaded in no more than three (3) seconds over an analog telephone line under normal network conditions. Certicom also operates its CRL with sufficient resources to provide a commercially-reasonable response time for the number of queries generated by all of the EV Certificates issued by Certicom. Revocation entries are not removed until after the expiration date of the revoked EV Certificate.

Certicom also publishes legal notices regarding its PKI services, including this EV CPS, agreements and notices, references within this EV CPS as well as any other information it considers essential to its services in its Repository.

2.4 Types of Certicom Certificates

Certicom may update or extend its list of products, including the types of certificates it issues, as it sees fit. The publication or updating of the list of Certicom products creates no claims by any third party. Upon the inclusion of a new certificate product in the Certicom hierarchy, an amended version of this EV CPS will be made public on the official Certicom websites at least seven (7) days prior to the offering such new product.

Suspended or revoked certificates are appropriately referenced in CRLs and published in Certicom directories. Certicom does not perform escrow of subscriber private keys.

Pricing and subscriber fees for the EV certificates are made available on the relevant official Certicom website. The maximum warranty associated with EV certificates is set forth in detail in section 5.31.

As the suggested usage for a digital certificate differs on a per application basis, Subscribers are urged to appropriately study their requirements for their specific application before applying for a specific certificate.

2.4.1 Certicom EV Certificates

Certicom makes available Secure Server Certificates that in combination with a Secure Socket Layer (SSL) web server attest the public server's identity, providing full authentication and enabling secure communication with customers and business partners.

Certicom EV Certificates are professional level Secure Server Certificates from Certicom intended for use in establishing web-based data communication conduits via TLS/SSL protocols. Their intended usage is for websites conducting high value e-commerce or transferring data and within internal networks.

EV Certificates are validated by Certicom in accordance with section 4.2 (Validation Practices) of this EV CPS, and are issued to Private Organizations and Government Entities only.

EV Certificates may be available from the following channels: Certicom Website, Reseller Network, Web Host Network, PoweredSSL Network, and EPKI Manager.

2.5 Extensions and Naming

2.5.1 Digital Certificate Extensions

Certicom uses the standard X.509, version 3 to construct digital certificates for use within the Certicom PKI. X.509v3 allows a CA to add certain certificate extensions to the basic certificate structure. Certicom uses a number of certificate extensions for the purposes intended by X.509v3 as per Amendment 1 to ISO/IEC 9594-8, 1995. X.509v3 is the standard of the International Telecommunications Union for digital certificates.

2.5.2 Incorporation by Reference for Extensions and Enhanced Naming

Enhanced naming is the usage of an extended organization field in an X.509v3 certificate. Information contained in the organizational unit field is also included in the Certificate Policy extension that Certicom may use.

2.6 Subscriber Private Key Generation and Certificate Request Process

2.6.1 Key Generation

The Subscriber is solely responsible for the generation of the private key used in the certificate request. Certicom does not provide key generation, escrow, recovery or backup facilities for EV Certificates.

Upon making a certificate application, the Subscriber is solely responsible for the generation of an RSA or ECC key pair appropriate to the certificate type being applied for. During application, the Subscriber will be required to submit a public key and other personal / corporate details in the form of a Certificate Signing Request (CSR).

2.6.2 Documentation Requirements

Prior to the issuance of an EV Certificate, Certicom must obtain from the Applicant the following documentation, in compliance with the requirements of The EV Guidelines:

- a) EV Certificate Request
- b) Subscriber Agreement
- c) Such additional documentation as Certicom requires from the Applicant to satisfy its obligations under The EV Guidelines

2.6.3 Role Requirements

The following Applicant roles are required for the issuance of an EV Certificate

- a) **Certificate Requester** – The EV Certificate Request must be submitted by an authorized 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.
- b) **Certificate Approver** – The EV Certificate Request must be approved by an authorized 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 Requester, and (ii) to approve EV Certificate Requests submitted by other Certificate Requesters.
- c) **Contract Signer** – A Subscriber Agreement applicable to the requested EV Certificate MUST be signed by an authorized Contract Signer. A Contract Signer is a natural person who is either Applicant, employed by Applicant, or an authorized agent who has express authority to represent Applicant, and who has authority on behalf of Applicant to sign Subscriber Agreements.

One person may be authorized by the Applicant to fill one, two, or all three of these roles, provided that in all cases the Certificate Approver and Contract Signer must be an employee of Applicant. An Applicant may also authorize more than one person to fill each of these roles.

2.6.4 EV Certificate Request Requirements

- (a) **General.** Prior to the issuance of the EV Certificate, Certicom must obtain Applicant's agreement to a legally enforceable Subscriber Agreement with Certicom for the express benefit of Relying Parties and Application Software Vendors. The Subscriber Agreement must be signed by an authorized Contract Signer acting on behalf of Applicant in accordance with Section 20 of the EV Guidelines, and must apply to the EV Certificate to be issued pursuant to the EV Certificate Request. A separate Subscriber Agreement may be used for each EV Certificate Request, or a single Subscriber Agreement may be used to cover multiple future EV Certificate Requests and resulting EV Certificates, so long as each EV Certificate that the CA issues to Applicant is clearly covered by a

Subscriber Agreement signed by an authorized Contract Signer acting on behalf of Applicant.

(b) Request and Certification. The EV Certificate Request must contain a request from or on behalf of the Applicant for the issuance of an EV Certificate, and a certification by or on behalf of the Applicant that all of the information contained therein is true and correct.

(b) Information Requirements. The EV Certificate Request may include all factual information about the Applicant to be included in the EV Certificate, and such additional information as is necessary for Certicom to obtain from the Applicant in order to comply with the EV Guidelines and Certicom's own policies. In cases where the EV Certificate Request does not contain all necessary information about the Applicant, Certicom will obtain the remaining information from either the Certificate Approver or Contract Signer.

Applicant information shall include, but not be limited to, the information specified in section 4.3 of this EV CPS.

2.7 Subscriber Private Key Protection and Backup

The Subscriber is solely responsible for protection of its private keys. Certicom maintains no involvement in the generation, protection or distribution of such keys.

Certicom strongly urges Subscribers to use a password or equivalent authentication method to prevent unauthorized access and usage of the Subscriber private key.

2.8 Subscriber Public Key Delivery to Certicom

Secure Server Certificate requests are generated using the Subscriber's webserver software and the request is submitted to Certicom in the form of a PKCS #10 Certificate Signing Request (CSR). Submission is made electronically via the Certicom website or through a Certicom approved RA.

2.9 Delivery of Issued Subscriber Certificate to Subscriber

Secure server certificates are delivered via email to the Subscriber using the administrator contact email address provided during the application process.

2.10 Delivery of Issued Subscriber Certificate to Partners

Issued Subscriber Secure Server Certificates applied for through a Partner Account are emailed to the administrator contact of the account.

2.11 Reserved

2.12 Certicom Certificates Profile

A Certificate profile contains fields as specified below.

2.12.1 Content of the EV Certificate as it relates to the identity of Certicom and the Subject of the EV Certificate

These are the minimum requirements for the content of the EV Certificate.

(a) Subject Organization Information. Subject to the requirements of the EV Guidelines, the EV Certificate and certificates issued to subordinate CAs that are not controlled by the same entity as the Root CA MUST include the following information about the Subject organization in the fields listed ("Subject Organization Information"):

(1) Organization name:

Certificate Field: subject:organizationName (OID 2.5.4.10)

Required/Optional: Required

Contents: This field contains the Subject's full legal organization name as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration or as otherwise verified by Certicom as provided herein. Certicom may abbreviate the organization prefixes or suffixes in the Organization name, e.g., if the QGIS shows "*Company Name* Incorporated" Certicom may include "*Company Name*, Inc." Certicom will use common abbreviations that are generally accepted in the Jurisdiction of Incorporation or Registration.

In addition, an assumed name, "trading as," or d/b/a name used by the Subject may be included at the beginning of this field, provided that it is followed by the full legal organization name in parenthesis. If the combination of the full legal organization name and the assumed, trading as, or d/b/a name exceeds 64 characters, as defined by RFC 3280, Certicom will use only the full legal organization name in the certificate.

If the Organization name by itself exceeds 64 characters, Certicom abbreviate parts of organization name, and/or omit non-material words in the organization name in such a way that the name in the certificate does not exceed the 64-character limit, provided that a Relying Party will not be misled into thinking they are dealing with a different Organization. In cases where this is not possible, the Certicom will not issue the EV certificate.

(2) Domain name:

Certificate Field: subject:commonName (OID 2.5.4.3) or SubjectAlternativeName:dNSName

Required/Optional: Required

Contents: This field contains one or more host domain name(s) owned or controlled by the Subject and to be associated with Subject's publicly accessible server. 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.

(3) Business Category:

Certificate Field: subject:businessCategory (OID 2.5.4.15)

Required/Optional: Required

Contents: This field contains information about the qualification of the Applicant for an EV certificate and will contain one of the following strings in UTF-8 English: 'V1.0, Clause 5.(b)', 'V1.0, Clause 5.(c)' or 'V1.0, Clause 5.(d)'.

(4) Jurisdiction of Incorporation or Registration:

Certificate Fields:

City or town (if any):

subject:jurisdictionOfIncorporationLocalityName
(1.3.6.1.4.1.311.60.2.1.1)

ASN.1 - X520LocalityName as specified in RFC 3280

State or province (if any):

subject:jurisdictionOfIncorporationStateOrProvinceName
(1.3.6.1.4.1.311.60.2.1.2)

ASN.1 - X520StateOrProvinceName as specified in RFC 3280

Country:

subject:jurisdictionOfIncorporationCountryName
(1.3.6.1.4.1.311.60.2.1.3)

ASN.1 - X520countryName as specified in RFC 3280

Required/Optional: Required

Contents: These fields contain information only to the level of the Incorporating Agency or Registration Authority – e.g., the Jurisdiction of Incorporation for an Incorporating Agency or Jurisdiction of Registration for a Registering Authority at the country level would include country information but would not include state or province or city or town information; the Jurisdiction of Incorporation for an Incorporating Agency or Jurisdiction of Registration for a Registering Authority at the state or province level would include both country and state or province information, but would not include city or town information; and so forth. Country information will be specified using the applicable ISO country code. State or province information, and city or town information (where applicable) for the Subject's Jurisdiction of Incorporation or Registration will be specified using the full name of the applicable jurisdiction.

Compliance with European Union Qualified Certificates Standard: In addition, Certicom may include a qcStatements extension per RFC 3739. The OID for qcStatements:qcStatement:statementId is 1.3.6.1.4.1.311.60.2.1.

(4) Registration Number:

Certificate Field: Subject:serialNumber (OID 2.5.4.5)

Required/Optional: Required

Contents: This field contains the unique registration number assigned to the Subject by the Incorporating or Registration Agency in its Jurisdiction of Incorporation or by the Registration Agency in its Jurisdiction of Registration, as appropriate.

If the Jurisdiction of Incorporation or Registration does not provide a Registration Number, then the field will contain the date of Incorporation or Registration instead of a registration number and will be in any one of the common date formats. For other Business Entities, the field will contain the registration number that was received by the Business Entity upon government registration.

For those Business Entities that register with an Incorporating Agency or Registration Agency in a jurisdiction that does not issue numbers pursuant to government registration, the field will contain the date of the registration in any one of the common date formats.

For Government Entities that do not have a Registration Number or readily verifiable date of creation, the field will contain appropriate language to indicate that the Subject is a Government Entity.

(5) Physical Address of Place of Business:

Certificate Fields:

Number & street (optional)
City or town

subject:streetAddress (OID 2.5.4.9)
subject:localityName (OID 2.5.4.7)

State or province (if any)	subject:stateOrProvinceName (OID 2.5.4.8)
Country	subject:countryName (OID 2.5.4.6)
Postal code (optional)	subject:postalCode (2.5.4.17)

Required/Optional: City, state, and country – Required; Street and postal code – Optional

Contents: This field contains the address of the physical location of the Subject's Place of Business.

2.12.2 Key Usage extension field

In order to use and rely on a Certicom certificate a relying party must use X.509v3 compliant software. Certicom certificates include key usage extension fields to specify the purposes for which the certificate may be used and to technically limit the functionality of the certificate when Fused with X.509v3 compliant software. Reliance on key usage extension fields is dependent on correct software implementations of the X.509v3 standard and is outside the control of Certicom.

The Extension Criticality field denotes two separate uses for the Key Usage field. If the extension is noted as critical, then the key in the certificate is only to be applied to the stated uses. To use the key for another purpose in this case would break the issuer's policy. If the extension is not noted as critical, the Key Usage field is simply there as an aid to help applications find the proper key for a particular use.

The Basic Constraints extension specifies whether the subject of the certificate may act as a CA or only as an end-entity. Reliance on basic constraints extension field is dependent on correct software implementations of the X.509v3 standard and is outside of the control of Certicom.

The EV Certificates certificate extensions are as follows:

Root CA Certificate

Root certificates generated are X.509 v3 compliant.

(a) basicConstraints

This extension appears as a critical extension in all Certicom certificates that contain Public Keys used to validate digital signatures on certificates. The CA field is set true. The pathLenConstraint field will not be present.

(b) keyUsage

This extension will be present and will be marked critical. Bit positions for CertSign and cRLSign will be set. All other bit positions will not be set.

All other fields and extensions set in accordance to RFC 3280.

Subordinate CA Certificate

(a) certificatePolicies:

will be present and will not be marked critical. The set of policy identifiers includes the identifier for Certicom's EV Policy if the certificate is issued to a subordinate CA that is not controlled by the Root CA.

certificatePolicies:policyIdentifier (Required)

- anyPolicy if subordinate CA is controlled by Root CA
- explicit EV policy OID(s) if subordinate CA is not controlled by Root CA

The following fields will be present if the Subordinate CA is not controlled by the same entity that controls the Root CA.

certificatePolicies:policyQualifiers:policyQualifierId
- id-qt 2 [RFC 3280]

certificatePolicies:policyQualifiers:qualifier
- URI to the Certificate Practice Statement

(b) cRLDistributionPoint

will be present and will not be marked critical. If present, it will contain the HTTP URL of Certicom's CRL service.

(c) authorityInformationAccess

will be present and will not be marked critical. It will contain the HTTP URL of Certicom's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1). An HTTP accessMethod

It may be included for Certicom's certificate (accessMethod = 1.3.6.1.5.5.7.48.2).

(d) basicConstraints

This extension will appear as a critical extension in all CA certificates that contain Public Keys used to validate digital signatures on certificates. Certicom field will be set true. The pathLenConstraint field may be present.

(e) keyUsage

This extension will be present and will be marked critical. Bit positions for CertSign and cRLSign will be set. All other bit positions will not be set.

All other fields and extensions set in accordance to RFC 3280.

Subscriber Certificate

(a) certificate Policies

will be present and will not be marked critical. The set of policyIdentifiers will include the identifier for Certicom's EV policy.

certificatePolicies:policyIdentifier (Required)
- EV policy OID

certificatePolicies:policyQualifiers:policyQualifierId (Required)
- id-qt 2 [RFC 3280]

certificatePolicies:policyQualifiers:qualifier (Required)
- URI to the Certificate Practice Statement

(b) cRLDistributionPoint

will be present and will not be marked critical. If present, it will contain the HTTP URL of Certicom's CRL service. This extension will be present if the certificate does not specify OCSP responder locations in an authorityInformationAccess extension.

(c) authorityInformationAccess

will be present and will not be marked critical. It will contain the HTTP URL of Certicom's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1). An HTTP accessMethod may be included for Certicom's certificate (accessMethod = 1.3.6.1.5.5.7.48.2). This extension will be present if the certificate does not contain a cRLDistributionPoint extension.

(d) basicConstraints (optional)

If present, the Certicom field will be set false.

(e) keyUsage (optional)

If present, bit positions for CertSign and cRLSign will not be set.

All other fields and extensions set in accordance to RFC 3280.

2.123 Certificate Policy (CP)

Certificate Policy (CP) is a statement of the issuer that corresponds to the prescribed usage of a digital certificate within an issuance context. A policy identifier is a number unique within a specific domain that allows for the unambiguous identification of a policy, including a certificate policy.

The content of the EV Subscriber and non-Root CA Certificates as they relate to the identification of EV certificate policy is as follows:

- (a) EV Subscriber Certificates.** Each EV Certificate issued by Certicom to a Subscriber contains an OID defined by Certicom in the certificate's certificatePolicies extension that: (i) indicates which CA policy statement relates to that certificate, (ii) asserts Certicom's adherence to and compliance with the EV Guidelines, and which (iii), by pre-agreement with the Application Software Vendor, marks the certificate as being an EV Certificate.
- (b) EV Subordinate CA Certificates.**
 - (1) Certificates issued to Subordinate CAs that are not controlled by the same entity as the Root CA contain one or more OID defined by Certicom that explicitly defines the EV Policies the Subordinate CA supports;
 - (2) Certificates issued to Subordinate CAs that are controlled by the same entity as the Root CA may contain the special anyPolicy OID (2.5.29.32.0).
- (c) Root CA Certificates.** Root CA Certificates will not contain the certificatePolicies or extendedKeyUsage fields.

The Application Software Vendor identifies Root CAs that can issue EV Certificates by storing EV OIDs in metadata associated with Root CA Certificates.

2.12.5 Minimum Cryptographic Algorithm and Key Sizes

1. Root CA Certificates

	Certificate issued on or before 31 Dec 2010	Certificate issued after 31 Dec 2010
Digest algorithm	MD5 (NOT RECOMMENDED),	SHA-1*, SHA-256, SHA-384 or SHA-512

	SHA-1	
RSA	2048**	2048
ECC	NIST P-256 or 384	NIST P-256 or 384

2. Subordinate CA Certificates

	Certificate issued on or before 31 Dec 2010	Certificate issued after 31 Dec 2010
Digest algorithm	SHA-1	SHA-1*, SHA-256, SHA-384 or SHA-512
RSA	1024	2048
ECC	NIST P-256 or 384	NIST P-256 or 384

3. Subscriber Certificates

	Certificate issued on or before 31 Dec 2010	Certificate issued after 31 Dec 2010
Digest algorithm	SHA-1	SHA1*, SHA-256, SHA-384 or SHA-512
RSA	1024 or 2048 (Note: subscriber certificates containing a 1024 bit RSA key MUST expire on or before 31 Dec 2010)	2048
ECC	NIST P-256 or 384	NIST P-256 or 384

*SHA-1 should be used only until SHA-256 is supported widely by browsers used by a majority of relying parties worldwide.

** An end-entity certificate may, in addition, chain to an EV-enabled 1024-bit RSA root CA certificate key.

The specific Certicom EV Certificate profile is as per the table below:

Suite B 256 Extended Validation (EV) SSL Server Certificates

Field	Content
Version	v3
Serial Number	<a 16-byte integer>
Signature Algorithm	ecdsa-with-SHA256
Issuer	CN=Certicom ECC 256 Extended Validation SSL CA OU=Certicom Certification Authority OU=Terms and Conditions of use: http://www.certicom.com/repository O=Certicom Corp. C=US
Validity Period	1 or 2 years
Subject	(Required) CN=<Fully-Qualified Domain Name> (Optional) OU=<Product Name> (Optional) OU=<Organizational Unit Name> (Required) O=<Organization Name> (Required) Street=<Street Address 1> (Optional) Street=<Street Address 2> (Optional) Street=<Street Address 3> (Required) L=<Locality Name> (Required) ST=<State or Province Name> (Required) PostalCode=<Postal Code> (Required) C=<Country Name> (Required) businessCategory=V1.0, Clause 5.(<a b c d e>) (Optional) joiLocalityName=<Jurisdiction of Incorporation Locality Name> (Optional) joiStateOrProvinceName=<J. of I. State or Province Name> (Required) joiCountryName=<J. of I. Country Name> (Required) serialNumber=<Company Reg. Number or Date of Inc./Reg.>
Public Key:	
Algorithm Identifier	id-ecPublicKey
ECPParameters (namedCurve)	secp256r1
ECPoint	<Supplied by customer>
Extensions:	
Authority Key Identifier (non-critical)	Key ID: B8FE15D654A3A5A3EA503E5FBD72CEC3C6380D01
Subject Key Identifier (non-critical)	<SHA-1 hash of customer-supplied ECC Public Key>
Key Usage (critical)	Digital Signature
Basic Constraints (critical)	Subject Type=End-entity
Extended Key Usage (non-critical)	Server Authentication, Client Authentication, Microsoft SGC, Netscape SGC
Certificate Policies (non-critical)	OID: 1.3.132.11.1 CPS URL: http://www.certicom.com/repository/ev_cps
CRL Distribution Points (non-critical)	URI: http://crl.certicom.com/CerticomECC256ExtendedValidationSSLCA.crl
Authority Info Access (non-critical)	CA Issuer: http://crt.certicom.com/CerticomECC256ExtendedValidationSSLCA.crt OCSP: http://ocsp.certicom.com
Subject Alternative Name (non-critical)	DNS Name: <Fully-Qualified Domain Name>

Suite B 384 Extended Validation (EV) SSL Server Certificates

Field	Content
Version	v3
Serial Number	<a 16-byte integer>
Signature Algorithm	ecdsa-with-SHA384
Issuer	CN=Certicom ECC 384 Extended Validation SSL CA OU=Certicom Certification Authority OU=Terms and Conditions of use: http://www.certicom.com/repository O=Certicom Corp. C=US
Validity Period	1 or 2 years
Subject	(Required) CN=<Fully-Qualified Domain Name> (Optional) OU=<Product Name> (Optional) OU=<Organizational Unit Name> (Required) O=<Organization Name> (Required) Street=<Street Address 1> (Optional) Street=<Street Address 2> (Optional) Street=<Street Address 3> (Required) L=<Locality Name> (Required) ST=<State or Province Name> (Required) PostalCode=<Postal Code> (Required) C=<Country Name> (Required) businessCategory=V1.0, Clause 5.<a b c d e> (Optional) joiLocalityName=<Jurisdiction of Incorporation Locality Name> (Optional) joiStateOrProvinceName=<J. of I. State or Province Name> (Required) joiCountryName=<J. of I. Country Name> (Required) serialNumber=<Company Reg. Number or Date of Inc./Reg.>
Public Key:	
Algorithm Identifier	id-ecPublicKey
ECPParameters (namedCurve)	secp384r1
ECPPoint	<Supplied by customer>
Extensions:	
Authority Key Identifier (non-critical)	Key ID: 1F6162645CDC054E4AFA8622AAB4EB7848B80090
Subject Key Identifier (non-critical)	<SHA-1 hash of customer-supplied ECC Public Key>
Key Usage (critical)	Digital Signature
Basic Constraints (critical)	Subject Type=End-entity
Extended Key Usage (non-critical)	Server Authentication, Client Authentication, Microsoft SGC, Netscape SGC
Certificate Policies (non-critical)	OID: 1.3.132.11.1 CPS URL: http://www.certicom.com/repository/ev_cps
CRL Distribution Points (non-critical)	URI: http://crl.certicom.com/CerticomECC384ExtendedValidationSSLCA.crl
Authority Info Access (non-critical)	CA Issuer: http://crt.certicom.com/CerticomECC384ExtendedValidationSSLCA.crt OCSP: http://ocsp.certicom.com
Subject Alternative Name (non-critical)	DNS Name: <Fully-Qualified Domain Name>

2.13 Certicom Certificate Revocation List Profile

The profile of the Certicom EV Certificate Revocation List is as per the table below:

Field	Content
Version	v2
Signature Algorithm	<Same Signature Algorithm used to sign certificates>
Issuer	<Same Issuer name included in certificates>
Validity Period	96 hours, but refreshed every 24 hours
Extensions:	
Authority Key Identifier (non-critical)	<Same Authority Key Identifier included in certificates>
CRL Number (non-critical)	<A monotonically increasing integer>
For each Revoked Certificate:	
Serial Number	<Copied from the revoked certificate>
Revocation Date	<Date/time at which this certificate was revoked>

2.13 Certicom OCSP Responses

The profile of the Certicom EV Certificate Online Certificate Status Protocol responses is as per the table below:

Field	Content
Version	v1
Responder ID	byKey: <SHA-1 Hash of the Issuing CA's Public Key> (OCSP Responses are always signed directly by the Issuing CA, rather than by a delegated OCSP Responder Certificate)
Produced At	<Date/Time that this OCSP Response was produced>
There is always precisely 1 "SingleResponse" in each OCSP Response:	
Hash Algorithm	<Same Hash algorithm used in the certificate's signature>
Issuer Name Hash	<Hash of the Issuing CA's Name>
Issuer Key Hash	<Hash of the Issuing CA's Public Key>
Serial Number	<Copied from the certificate>
Certificate Status	"good" when the certificate is unrevoked "revoked" when the certificate is revoked "unknown" when the OCSP Request contained an invalid Serial Number
Validity Period	96 hours, but refreshed every 24 hours
Revocation Time	<Date/Time when the certificate was revoked, if applicable>

3 Organization

Certicom operates within the United Kingdom, Canada, and the United States, with separate operations, research & development and server operation sites. All sites operate under a security policy designed to, within reason, detect, deter and prevent unauthorized logical or physical access to CA related facilities. This section of the EV CPS outlines the security policy, physical and logical access control mechanisms, service levels and personnel policy in use to provide trustworthy and reliable CA operations.

3.1 Conformance to this EV CPS

Certicom conforms to this EV CPS and other obligations it undertakes through adjacent contracts when it provides its services.

3.2 Termination of CA Operations

In case of termination of CA operations for any reason whatsoever, Certicom will provide timely notice and transfer of responsibilities to succeeding entities, maintenance of records, and remedies. Before terminating its own CA activities, Certicom will take the following steps, where possible:

- Providing subscribers of valid EV certificates with ninety (90) days notice of its intention to cease acting as a CA.
- Revoking all certificates that are still un-revoked or un-expired at the end of the ninety (90) day notice period without seeking subscriber's consent.
- Giving timely notice of revocation to each affected subscriber.
- Making reasonable arrangements to preserve its records according to this EV CPS.
- Reserving its right to provide succession arrangements for the re-issuance of certificates by a successor CA that has all relevant permissions to do so and complies with all necessary rules, while its operation is at least as secure as Certicom's.

The requirements of this article may be varied by contract, to the extent that such modifications affect only the contracting parties.

3.3 Form of Records

Certicom retains records in electronic or in paper-based format for a period detailed in section 3.4 of this EV CPS. Certicom may require subscribers to submit appropriate documentation in support of a certificate application.

Certicom Registration Authorities are required to submit appropriate documentation as detailed in any applicable agreements, and prior to being validated and successfully accepted as an approved Certicom Registration Authority. In their role as a Certicom Registration Authority, RAs may require documentation from subscribers to support certificate applications. In such circumstances, RAs are obliged to retain such records in line with the practices of record retention and protection as used by Certicom and as stated in this EV CPS.

3.4 Records Retention Period

Certicom retains all documentation relating to all EV Certificate Requests and verification thereof, and all EV Certificates and revocation thereof, for at least seven (7) years after any EV Certificate based on that documentation ceases to be valid. In connection therewith, Certicom maintains current an internal database of all previously revoked EV Certificates and previously rejected EV Certificate Requests due to suspected phishing or other fraudulent usage or concerns. Such

information may be used to flag suspicious EV Certificate Requests. Such records may be retained in electronic, in paper-based format or any other format that Certicom may see fit.

Audit logs are available to independent auditors upon request. Audit logs are retained for at least seven (7) years

All such records are archived at a secure off-site location and are maintained in a form that prevents unauthorized modification, substitution or destruction.

Certicom retains all documentation relating to all EV Certificate Requests and verification thereof, and all EV Certificates and revocation thereof, for at least seven years after any EV Certificate based on that documentation ceases to be valid. In connection therewith Certicom maintains current an internal database of all previously revoked EV Certificates and previously rejected EV Certificate Requests due to suspected phishing or other fraudulent usage or concerns. Such information is used to flag suspicious EV Certificate Requests.

3.5 Logs for Core Functions

For audit purposes, and for compliance with the EV Guidelines, Certicom, its RAs, and its subcontractors maintain electronic or manual logs of every action taken to process an EV Certificate Request and to issue an EV Certificate, including all information generated or received in connection with an EV Certificate Request, and every action taken to process the Request, including time, date, and personnel involved in the action. All logs are backed up on removable media and the media held at a secure off-site location on a daily basis. These media are only removed by Certicom staff on a visit to the data centre, and when not in the data centre are held either in a safe in a locked office within the development site, or off-site in a secure storage facility.

An audit log is maintained of each movement of the removable media. Logs are archived by the system administrator on a weekly basis and event journals reviewed on a weekly basis by CA management. Both current and archived logs are maintained in a form that prevents unauthorized modification, substitution or destruction. When the removable media reaches the end of its life it is wiped by a third party secure data destruction facility and the certificates of destruction are archived.

The foregoing record requirements include, but are not limited to, an obligation to record the following events:

- a) CA key lifecycle management events, including:
 - a. Key generation, backup, storage, recovery, archival, and destruction; and
 - b. Cryptographic device lifecycle management events
- b) CA and Subscriber EV Certificate lifecycle management events, including:
 - a. EV Certificate Requests, renewal and re-key requests, and revocation;
 - b. All verification activities required by The EV Guidelines
 - c. Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
 - d. Acceptance and rejection of EV Certificate Requests;
 - e. Issuance of EV Certificates; and
 - f. Generation of EV Certificate revocation lists (CRLs); and OCSP entries
- c) Security events, including:
 - a. Successful and unsuccessful PKI system access attempts;
 - b. PKI and security system actions performed;
 - c. Security profile changes;
 - d. System crashes, hardware failures, and other anomalies;
 - e. Firewall and router activities; and

- f. Entries to and exits from CA facility
- d) Log entries MUST include the following elements:
 - a. Date and time of entry;
 - b. Identity of the persona and entity making the journal entry; and
 - c. Description of entry

3.6 Business Continuity Plans and Disaster Recovery

To maintain the integrity of its services Certicom implements, documents and periodically tests appropriate contingency and disaster recovery plans and procedures. Such plans are revised and updated as may be required at least once a year.

- a) Certicom operates a fully redundant CA system. The backup CA is readily available in the event that the primary CA should cease operation. All of our critical computer equipment is housed in a co-location facility run by a commercial data-centre, and all of the critical computer equipment is duplicated within the facility. Incoming power and connectivity feeds are duplicated. The duplicate equipment is ready to take over the role of providing the implementation of Certicom, and allows us to specify a maximum system outage time (in case of critical systems failure) of 1 hour.
- b) Backup of critical CA software is performed weekly and is stored offsite.
- c) Backup of critical business information is performed daily and is stored offsite.
- d) Certicom operations are distributed across several sites world wide. All sites offer facilities to manage the lifecycle of a certificate, including but not limited to the application, issuance, revocation and renewal of such certificates.

As well as a fully redundant CA system, Certicom maintains provisions for the activation of a backup CA and a secondary site should the primary site suffer a total loss of systems. This disaster recovery plan states that Certicom will endeavor to minimize interruptions to its CA operations.

3.7 Availability of Revocation Data

Certicom publishes Certificate Revocation Lists (CRLs) to allow relying parties to verify a digital signature made using a Certicom issued digital certificate. Each CRL contains entries for all revoked un-expired certificates issued and is valid for 24 hours. Certicom issues a new CRL every 24 hours and includes a monotonically increasing sequence number for each CRL issued. Under special circumstances, Certicom may publish new CRLs prior to the expiry of the current CRL. All expired CRLs are archived (as described in section 3.4 of this EV CPS) for a period of 7 years or longer if applicable.

3.8 Publication of Critical Information

Certicom publishes this EV CPS, certificate terms and conditions, the relying party agreement and copies of all subscriber agreements in the official Certicom Repository. The Certicom Certificate Policy Authority maintains the Certicom Repository. All updates, amendments and legal promotions are logged in accordance with the logging procedures referenced in section 3.5 of this EV CPS.

3.9 Confidential Information

Certicom observes applicable rules on the protection of personal data deemed by law or the Certicom privacy policy (see section 3.11 of this EV CPS) to be confidential.

3.9.1 Types of Information deemed as Confidential

Certicom keeps the following types of information confidential and maintains reasonable controls to prevent the exposure of such records to non-trusted personnel.

- Subscriber agreements.
- Certificate application records and documentation submitted in support of certificate applications whether successful or rejected.
- Transaction records and financial audit records.
- External or internal audit trail records and reports, except for WebTrust audit reports that may be published at the discretion of Certicom.
- Contingency plans and disaster recovery plans.
- Internal tracks and records on the operations of Certicom infrastructure, certificate management and enrolment services and data.

3.9.2 Revocation Information not deemed as Confidential

Subscribers acknowledge that revocation data of all certificates issued by the Certicom is public information is published every 24 hours.

3.9.3 Access to Confidential Information

All Trusted Personnel handle all information in strict confidence. Personnel of RA/LRAs especially must comply with the requirements of the English law on the protection of personal data.

3.9.4 Release of Confidential Information

Certicom is not required to release any confidential information, unless as otherwise required by law, without an authenticated, reasonably specific request by an authorized party specifying:

- The party to whom Certicom owes a duty to keep information confidential.
- The party requesting such information.
- A court order, if any.

3.10 Personnel Management and Practices

Consistent with this EV CPS Certicom follows personnel and management practices that provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties.

3.10.1 Trusted roles

Trusted roles relate to access to the Certicom account management system, with functional permissions applied on an individual basis. Senior members of the management team decide permissions, with signed authorizations being archived.

3.10.2 Personnel controls

Trusted Personnel must identify and authenticate themselves to the system before access is granted. Identification is via a username, with authentication requiring a password and digital certificate.

All Trusted Personnel have background checks before access is granted to Certicom's systems. These checks include, but are not limited to, credit history, employment history for references and a Companies House cross-reference to disqualified directors. Training of personnel is undertaken via a mentoring process involving senior members of the team to which they are attached.

Prior to the commencement of employment of any person by Certicom for engagement in the EV Certificate process, whether as an employee, agent, or an independent contractor, of Certicom, Certicom will:

- (1) Verify the identity of such person. Verification of identity may be performed through:
 - (A) The personal (physical) presence of such person before trusted persons who perform human resource or security functions, and
 - (B) The verification of well-recognized forms of government-issued photo identification (e.g., passports and/or driver's licenses); and
- (2) Verify the trustworthiness of such person. Verification of trustworthiness shall include background checks which address at least the following (or their equivalent):
 - (A) Confirmation of previous employment,
 - (B) Check of professional references;
 - (C) Confirmation of the highest or most relevant educational degree obtained,
 - (D) Search of criminal records (local, state or provincial, and national) where allowed by the jurisdiction where the person will be employed; and
- (3) In the case of employees of Certicom at the time of the adoption of the EV Guidelines whose identity and background has not previously been verified as set forth above, Certicom shall conduct such verification within three (3) months of the date of adoption of the EV Guidelines.

3.10.3 Training and Skills Level

- (1) Certicom 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 EV Guidelines.
- (2) Certicom maintains 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.
- (3) Validation Specialists engaged in EV Certificate issuance maintain adequate skill levels in order to have issuance privilege, consistent with Certicom's training and performance programs.
- (4) Certicom ensures that its Validation Specialists qualify for each skill level required by the corresponding validation task before granting privilege to perform said task.
- (5) Certicom requires all Validation Specialists to pass an internal examination on the EV Certificate validation criteria outlined in The EV Guidelines.

3.10.4 Separation of Duties

Certicom enforces rigorous control procedures for the separation of validation duties to ensure that no one person can single-handedly validate and authorize the issuance of an EV Certificate. The final due diligence steps as outlined in Section 4.2.11 may be performed by one of the persons. For example, one Validation Specialist reviews and verifies all Applicant information and a second Validation Specialist approves issuance of the EV Certificate. All such separation controls are auditable.

3.11 Privacy Policy

Certicom has implemented a privacy policy that complies with this EV CPS which governs the collection, use, retention, and disclosure of non-public information including information and trade secret laws and regulations and the information that is part of the EV Certificate vetting process. The Certicom privacy policy is published in the Certicom Repository.

3.12 Publication of information

The Certicom certificate services and the Certicom repository are accessible through several means of communication:

- On the web: www.certicom.com
- By email from: CAservice@certicom.com
- and by mail from:

Certicom Corp.
Attn: Certicom Certificate Service
5520 Explorer Drive, 4th Floor
Mississauga, Ontario Canada L4W 5L1

4 Practices and Procedures

This section describes the certificate application process, including the information required to make and support a successful application.

4.1 Certificate Application Requirements

Prior to issuance of an EV Certificate, Certicom will obtain from Applicant 1) an EV Certificate Request, 2) a Subscriber Agreement, and 3) additional documentation required to satisfy the EV Certificate Guidelines.

Certicom may issue EV Certificates to Private Organizations that satisfy the following requirements:

- a) The Private Organization is a legally recognized entity whose existence was created by a filing with (or an act of) the Incorporating Agency in its Jurisdiction of Incorporation or Registration (e.g., by issuance of a certificate of incorporation) or is an entity that is chartered by a state or federal regulatory agency or national government;
- b) The Private Organization has designated with the Incorporating Agency, a Registered Agent, Registered Office (as required under the laws of the Jurisdiction of Incorporation) or equivalent facility;
- c) The Private Organization is not designated on the records of the Incorporating Agency by labels such as “inactive,” “invalid,” “not current,” or the equivalent;
- d) The Private Organization’s Jurisdiction of Incorporation, Registration, Charter, or License, and/or its Place of Business is not in any country where Certicom is prohibited from doing business or issuing a certificate by the laws of Certicom’s jurisdiction; and
- e) The Private Organization is not listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of Certicom’s jurisdiction.

Certicom may issue EV Certificates to Government Entities that satisfy the following requirements:

- a) The legal existence of the Government Entity is established by the political subdivision in which such Government Entity operates;
- b) The Government Entity is not in any country where Certicom is prohibited from doing business or issuing a certificate by the laws of Certicom’s jurisdiction; and
- c) The Government Entity is not listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of Certicom’s jurisdiction.

Certicom may issue EV Certificates to Business Entities who do not qualify above but do satisfy the following requirements:

- a) The Business Entity is a legally recognized entity whose formation included the filing of certain forms with the Registration Agency in its Jurisdiction, the issuance or approval by such Registration Agency of a charter, certificate, or license, and whose existence can be verified with that Registration Agency;
- b) The Business Entity has a verifiable physical existence and business presence;
- c) At least one Principal Individual associated with the Business Entity is identified and validated;
- d) The identified Principal Individual attests to the representations made in the Subscriber Agreement;
- e) Where the Business Entity represents itself under an assumed name, the Business Entity’s use of the assumed name can be verified;

- f) The Business Entity and the identified Principal Individual associated with the Business Entity are not located or residing in any country where Certicom is prohibited from doing business or issuing a certificate by the laws of Certicom's jurisdiction; and
- g) The Business Entity is not listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of Certicom's jurisdiction.

All qualifying EV Certificate applicants must complete the enrolment process, which may include:

- Generate a RSA/ECC key pair and demonstrate to Certicom ownership of the private key half of the key pair through the submission of a valid PKCS#10 Certificate Signing Request (CSR) (or SPKAC request for certain Certicom TF certificates)
- Make all reasonable efforts to protect the integrity the private key half of the key pair
- Submit to Certicom a certificate application request, including application information as detailed in this EV CPS, a public key half of a key pair, and agree to the terms of the relevant subscriber agreement
- Provide proof of identity through the submission of official documentation as requested by Certicom during the enrolment process

Certificate applications are submitted to either Certicom or a Certicom approved RA.

4.1.1 Reserved

4.1.2 Reserved

4.1.3 Methods of application

Generally, applicants will complete the online forms made available by Certicom or by approved RAs at the respective official websites. Under special circumstances, the applicant may submit an application via email; however, this process is available at the discretion of Certicom or its RAs.

4.1.4 Certificate Request

A properly completed and signed EV Certificate request form must be submitted via an authorized certificate requestor to Certicom prior to obtaining an EV Certificate. One EV Certificate Request may suffice for multiple EV Certificates to be issued to the same Applicant at the same time. Any information required to issue an EV Certificate that is missing from an EV Certificate Request will be obtained by Certicom from the Certificate Approver or Contract Signor (as defined in the EV Guidelines), or, after having obtained the information from a reliable source, will confirm the information with the Certificate Approver or Contract Signor.

4.2. Certicom EV Certificates Validation Process

Before issuing an EV Certificate, Certicom ensures that all Subject organization information in the EV Certificate conforms to the requirements of, and has been verified in accordance with, the EV Guidelines and matches the information confirmed and documented by Certicom pursuant to its verification processes.

As a general rule, Certicom is responsible for taking all verification steps reasonably necessary to satisfy each of the Verification Requirements set forth below. The Acceptable Methods of Verification set forth in each of Sections 4.2.1 through 4.2.11 below (which usually include alternatives) are considered to be acceptable methods of verification that may be employed by Certicom. In all cases, however, Certicom will take any additional verification steps that may be reasonably necessary under the circumstances to satisfy the applicable Verification Requirement.

4.2.1. Verification of Applicant's Legal Existence and Identity

(a) Verification Requirements. To verify Applicant's legal existence and identity, Certicom will do the following:

(1) Private Organizations:

- a. **Legal Existence:** Verify that the Applicant is a legally recognized entity, in existence and validly formed (e.g., incorporated) with the Incorporating or Registration Agency in Applicant's Jurisdiction of Incorporation or Registration, and not designated on the records of the Incorporating Agency by labels such as "inactive," "invalid," "not current," or the equivalent.
- b. **Organization Name:** Verify that the Applicant's formal legal name as recorded with the Incorporating or Registration Agency in Applicant's Jurisdiction of Incorporation or Registration matches Applicant's name in the EV Certificate Request.
- c. **Registration Number:** Obtain the specific unique Registration Number assigned to Applicant by the Incorporating or Registration Agency in the Applicant's Jurisdiction of Incorporation or Registration. Where the Incorporating or Registration Agency does not assign a Registration Number Certicom will obtain Applicant's date of Incorporation or Registration.
- d. **Registered Agent:** Obtain the identity and address of the Applicant's Registered Agent or Registered Office (as applicable) in the Applicant's Jurisdiction of Incorporation or Registration.

(2) Government Entity:

- a. **Legal Existence:** Verify that Applicant is a legally recognized Government Entity, in existence in the political subdivision in which such Government Entity operates.
- b. **Entity Name:** Verify that Applicant's formal legal name matches Applicant's name in the EV Certificate Request.
- c. **Registration Number:** Obtain Applicant's date of incorporation, registration, or formation, or the identifier for the legislative act that created the Government Entity. In circumstances where this information is not available, Certicom will enter appropriate language to indicate that the Subject is a Government Entity

(3) Business Entities:

- a. **Legal Existence:** Verify that Applicant is engaged in business under the name submitted by Applicant in the Application.
- b. **Organization Name:** Verify that Applicant's formal legal name as recognized by the Registration Authority in Applicant's Jurisdiction of Registration matches Applicant's name in the EV Certificate Request.
- c. **Registration Number:** Obtain the specific unique Registration Number assigned to Applicant by the Registration Agency in Applicant's Jurisdiction of Registration. Where the Registration Agency does not assign a Registration Number, Certicom will obtain Applicant's date of Registration.
- d. **Principal Individual:** Verify the identity of the identified Principal Individual.

(b) Acceptable Method of Verification.

- (1) Private Organizations. All of the foregoing will be verified directly with or obtained directly from the Incorporating or Registration Agency in the Applicant's Jurisdiction

of Incorporation or Registration. Such verification may be through use of a Qualified Government Information Source operated by or on behalf of the Incorporating Agency, or by direct contact with the Incorporating Agency in person or via mail, e-mail, web address, or telephone using an address or phone number obtained from a Qualified Independent Information Source.

- (2) Government Entities: All of the foregoing will be verified directly with, or obtained directly from, one of the following: (i) a QGIS in the political subdivision in which such Government Entity operates; (ii) a superior governing Government Entity in the same political subdivision as Applicant (e.g. a Secretary of State may verify the legal existence of a specific State Department), or (iii) from a judge that is an active member of the federal, state or local judiciary within that political subdivision, or (iv) an attorney representing the Government Entity.

Any communication from a judge SHALL be verified in the same manner as is used for verifying factual assertions that are asserted by an Attorney as set forth below.

Such verification may be by direct contact with the appropriate Government Entity in person or via mail, e-mail, Web address, or telephone, using an address or phone number obtained from a Qualified Independent Information Source.

- (3) Business Entities: All of the foregoing items will be verified directly with, or obtained directly from, the Registration Agency in Applicant's Jurisdiction of Registration. Such verification may be through use of a Qualified Government Information Source, a Qualified Governmental Tax Information Source, or by direct contact with the Registration Agency in person or via mail, e-mail, web address, or telephone, using an address or phone number obtained from a Qualified Independent Information Source. In addition, Certicom will validate a Principal Individual associated with the Business Entity pursuant to the requirements below.
- (4) Principal Individual: A Principal Individual associated with the Business Entity will be validated in a face-to-face setting. Certicom may rely upon a face-to-face validation of the Principal Individual performed by the Registration Agency, provided that the Certicom has evaluated the validation procedure and concluded that it satisfies the requirements of the Guidelines for face-to-face validation procedures. Where no face-to-face validation was conducted by the Registration Agency, or the Registration Agency's face-to-face validation procedure does not satisfy the requirements of the Guidelines, Certicom will perform face-to-face validation.
- (i) Face-to-face validation: The face-to-face validation will be conducted before either an employee of Certicom, 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:
- a. 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.
 - b. A current signed government-issued identification document that includes a photo of the Individual and is signed by the Individual such as: A passport;
 1. A drivers license;
 2. A personal identification card;

3. A concealed weapons permit;
 4. A military ID.
- b. 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.

Acceptable financial institution documents include:

1. A major credit card, provided that it contains an expiration date and it has not expired.
2. A debit card from a regulated financial institution, provided that it contains an expiration date and it has not expired.
3. A mortgage statement from a recognizable lender that is less than six months old.
4. 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 will:

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.
- ii. Cross-checking of Information. Certicom will obtain the original signed and attested Personal Statement together with the attested copy of the current signed government-issued photo identification document. Certicom will review the documentation to determine that the information is consistent, matches the information in the application and identifies the Individual.
- iii. Verification of Third-party Validator. Certicom will 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.

4.2.2 Verification of Applicant's Legal Existence and Identity – Assumed Name

- (a) **Verification Requirements.** If, in addition to the Applicant's formal legal name as recorded with the Incorporating or Registration Agency in Applicant's Jurisdiction of Incorporation or Registration, Applicant's identity as asserted in the EV Certificate is to contain any assumed name (also known as "doing business as", "DBA", or "d/b/a" in the US and "trading as" in the UK) under which Applicant conducts business, Certicom will

verify that: (i) the Applicant has registered its use of the assumed name with the appropriate government agency for such filings in the jurisdiction of its Place of Business (as verified in accordance with The EV Guidelines), and (ii) that such filing continues to be valid.

(b) Acceptable Method of Verification. To verify any assumed name under which Applicant conducts business:

- (1) Certicom may verify the assumed name through use of a Qualified Government Information Source operated by or on behalf of an appropriate government agency in the jurisdiction of the Applicant's Place of Business, or by direct contact with such government agency in person or via mail, e-mail, web address, or telephone;
- (2) Certicom may verify the assumed name through use of a Qualified Independent Information Source provided that the QIIS has verified the assumed name with the appropriate government agency; or
- (3) Certicom may rely on a Verified Legal Opinion or Verified Accountant Letter that indicates the assumed name under which Applicant conducts business, the government agency such assumed name is registered with, and that such filing continues to be valid.

4.2.3 Verification of Applicant's Physical Existence

(a) Address of Applicant's Place of Business

- (1) Verification Requirements. To verify Applicant's physical existence and business presence, Certicom will verify that the physical address provided by Applicant is an address where Applicant conducts business operations (e.g., not a mail drop or P.O. Box), and is the address of Applicant's Place of Business.
- (2) Acceptable Methods of Verification. To verify the address of Applicant's Place of Business:
 - (A) For Applicants whose Place of Business is in the same country as the Applicant's Jurisdiction of Incorporation or Registration:
 - (1) For Applicants listed at the same Place of Business address in the current version of at least one (1) Qualified Independent Information Source or a Qualified Governmental Tax Information Source, Certicom will confirm that the Applicant's address as listed in the EV Certificate Request is a valid business address for Applicant by reference to such Qualified Independent Information Sources, and may rely on Applicant's representation that such address is its Place of Business;
 - (2) For Applicants who are not listed at the same Place of Business address in the current version of at least one (1) Qualified Independent Information Source or a Qualified Governmental Tax Information Source, Certicom will confirm that the address provided by the Applicant in the EV Certificate Request is in fact Applicant's business address by obtaining documentation of a site visit to the business address which will be performed by a reliable individual or firm. The documentation of the site visit will:
 - (a) Verify that the Applicant's business is located at the exact address stated in the EV Certificate Request (e.g., via permanent signage, employee confirmation, etc.);

- (b) Identify the type of facility (e.g., office in a commercial building, private residence, storefront, etc.) and whether it appears to be a permanent business location;
 - (c) Indicate whether there is a permanent sign (that cannot be moved) that identifies the Applicant
 - (d) Indicate whether there is evidence that Applicant is conducting ongoing business activities at the site (e.g., that it is not just a mail drop, P.O. box, etc.), and
 - (e) Include one or more photos of (i) the exterior of the site (showing signage indicating the Applicant's name, if present, and showing the street address if possible), and (ii) the interior reception area or workspace.
- (3) For all Applicants, Certicom may alternatively rely on a Verified Legal Opinion or a Verified Accountant Letter that indicates the address of Applicant's Place of Business and that business operations are conducted there.
 - (4) For Government Entity Applicants, Certicom may rely on the address contained in the records of the QGIS in Applicant's Jurisdiction.
- (B) For Applicants whose Place of Business is not in the same country as the Applicant's Jurisdiction of Incorporation, Certicom will rely on a Verified Legal Opinion that indicates the address of Applicant's Place of Business and that business operations are conducted there.

(b) Telephone Number for Applicant's Place of Business

- (1) Verification Requirements. To further verify Applicant's physical existence and business presence, as well as to assist in confirming other verification requirements, Certicom will verify that the telephone number provided by Applicant is a main phone number for Applicant's Place of Business.
- (2) Acceptable Methods of Verification. To verify Applicant's telephone number, Certicom will perform A and one of B, C, or D as listed below:
 - (A) Confirm Applicant's telephone number by calling it and obtaining an affirmative response sufficient to enable a reasonable person to conclude that the Applicant is reachable by telephone at the number dialed; *and*
 - (B) Confirm that the telephone number provided by Applicant is listed as Applicant's or Parent/Subsidiary Company's telephone number for the verified address of its Place of Business in records provided by the applicable phone company, or, alternatively, in either at least one (1) a Qualified Independent Information Source or a Qualified Governmental Tax Information Source; *or* (C) During a site visit, the person who is conducting the site visit will confirm the Applicant's main telephone number by calling it and obtaining an affirmative response sufficient to enable a reasonable person to conclude that the Applicant is reachable by telephone at the number dialed. Certicom will also confirm that the Applicant's main telephone number is not a mobile phone; *or*
 - (D) Rely on a Verified Legal Opinion or a Verified Accountant Letter to the effect that the Applicant's telephone number provided is a main phone number for Applicant's Place of Business;
 - (E) For Government Entity Applicants, Certicom may rely on the telephone number contained in the records of the QGIS in Applicant's Jurisdiction.

4.2.4 Verification of Applicant's Operational Existence

- (a) **Verification Requirements.** If the Applicant has been in existence for less than three (3) years, as indicated by the records of the Incorporating or Registration Agency, **and** is not listed in the current version of one (1) Qualified Independent Information Source or a Qualified Governmental Tax Information Source, Certicom will verify that the Applicant has the ability to engage in business.
- (b) **Acceptable Methods of Verification.** To verify the Applicant's operational existence, Certicom will perform one of the following:
 - (1) Verify the Applicant has an active current Demand Deposit Account with a Regulated Financial Institution. Certicom will receive authenticated documentation directly from a Regulated Financial Institution verifying that the Applicant has an active current Demand Deposit Account with the institution; or
 - (2) Rely on a Verified Legal Opinion or a Verified Accountant Letter to the effect that the Applicant has an active current Demand Deposit Account with a Regulated Financial Institution;

4.2.5 Verification of Applicant's Domain Name

- (a) **Verification Requirements.** To verify Applicant's registration or exclusive control of the domain name(s) to be listed in the EV Certificate, Certicom will verify that each such domain name satisfies the following requirements:
 - (1) The domain name is registered with an Internet Corporation for Assigned Names and Numbers (ICANN)-approved registrar or a registry listed by the Internet Assigned Numbers Authority (IANA);
 - (2) Domain registration information in the WHOIS database should be public and should show the name, physical address, and administrative contact information for the organization.

For Government Entity Applicants, Certicom may rely on the domain name listed for that entity in the records of the QGIS in Applicant's Jurisdiction to verify Domain Name.
 - (3) Applicant:
 - (A) is the registered holder of the domain name; or
 - (B) has been granted the exclusive right to use the domain name by the registered holder of the domain name;
 - (4) The Applicant is aware of its registration or exclusive control of the domain name;

(b) Acceptable Methods of Verification

- (1) **Applicant as Registered Holder.** Acceptable methods by which Certicom may verify that the Applicant is the registered holder of the domain name includes the following:
 - (A) Performing a WHOIS inquiry on the Internet for the domain name supplied by the Applicant, and obtaining a response indicating that the Applicant is the entity registered to the domain name;
 - (B) Communicating with the contact listed on the WHOIS record to confirm that Applicant is the registered holder of the domain name and having the contact update the WHOIS records to reflect the proper domain name registration. Confirmation that the registered owner of the domain name is a

Parent/Subsidiary Company of Applicant, or a registered trading name of Applicant, is sufficient to establish that Applicant is the registered owner of the domain name.;

- (C) In cases where domain registration information is private, Certicom may contact the applicant through the domain registrar by e-mail or paper mail if the domain registrar offers services to forward such communication to the registered domain holder.
- (2) Applicant's Exclusive Right to Use. In cases where Applicant is not the registered holder of the domain name, Certicom will verify the Applicant's exclusive right to use a domain name.

- (A) In cases where the registered domain holder can be contacted using information obtained from WHOIS, or through the domain registrar, Certicom will obtain positive confirmation from the registered domain holder by paper mail, e-mail, telephone, or facsimile that the applicant has been granted the exclusive right to use the requested Fully Qualified Domain Name (FQDN).

If the Top-Level Domain is a generic top-level domain (gTLD) such as .com, .net, or .org in accordance to RFC 1591, Certicom will obtain positive confirmation with the second level domain registration holder unless explicitly delegated by the holder. For example, if the requested FQDN is www1.www.example.com, Certicom will obtain positive confirmation from the domain holder of example.com.

If the Top-Level Domain is a 2 letter Country Code Top-Level Domain (ccTLD), Certicom will obtain positive confirmation with the domain holder at the domain level appropriate based on the rules of the ccTLD. For example, if the requested FQDN is www.mysite.users.internet.co.uk, Certicom will obtain positive confirmation from the domain holder of internet.co.uk.

In addition, Certicom will also verify the Applicant's exclusive right to use the domain name using one of the following methods:

- (1) Relying on a Verified Legal Opinion to the effect that the Applicant has the exclusive right to use the specified domain name in identifying itself on the Internet; or
 - (2) Relying on a representation from the Contract Signer, or the Certificate Approver, if expressly so authorized in a mutually-agreed-upon contract.
- (B) In cases where the registered domain holder cannot be contacted, Certicom will:
- (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;
- (3) Knowledge. Acceptable methods by which Certicom may verify the Applicant is aware that it has exclusive control of the domain name include the following:
- (A) Relying on a Verified Legal Opinion to the effect that the Applicant is aware that it has exclusive control of the domain name; or

- (B) Obtaining a confirmation from the Contract Signer or Certificate Approver verifying that the Applicant is aware that it has exclusive control of the domain name.
- (4) Mixed Character Set Domain Names. EV Certificates may include domain names containing mixed character sets only in compliance with the rules set forth by the domain registrar. Certicom will visually compare any domain names with mixed character set with known high risk domains. If similarity is found then the EV Certificate Request will be flagged as High Risk. Certicom must perform reasonably appropriate additional authentication and verification to be certain beyond reasonable doubt that the Applicant and the target in question are the same organization.

4.2.6 Verification of Name, Title, and Authority of Contract Signer and Certificate Approver

(a) Verification Requirements. For both the Contract Signer and the Certificate Approver, Certicom will verify the following:

- (1) Name, Title and Agency. Certicom will verify the name and title of the Contract Signer and the Certificate Approver, as applicable. Certicom will also verify that the Contract Signer and the Certificate Approver are agents representing the Applicant.
- (2) Authorization of Contract Signer. Certicom will verify, through a source other than the Contract Signer, that the Contract Signer is expressly authorized by the Applicant to enter into the Subscriber Agreement (and any other relevant contractual obligations) on behalf of the Applicant, including a contract that designates one or more Certificate Approvers on behalf of Applicant (“Signing Authority”).
- (3) Authorization of Certificate Approver. Certicom will verify, through a source other than the Certificate Approver, that the Certificate Approver is expressly authorized by the Applicant to do the following, as of the date of the EV Certificate Request (“EV Authority”):
 - (a) Submit, and if applicable authorize a Certificate Requester to submit, the EV Certificate Request on behalf of the Applicant; and
 - (b) Provide, and if applicable authorize a Certificate Requester to provide, the information requested from the Applicant by Certicom for issuance of the EV Certificate; and
 - (c) Approve EV Certificate Requests submitted by a Certificate Requester

(b) Acceptable Methods of Verification – Name, Title and Agency. Acceptable methods of verification of the name, title, and agency status of the Contract Signer and the Certificate Approver include:

- (1) Name and Title:** Certicom may verify the name and title of the Contract Signer and the Certificate Approver by any appropriate method designed to provide reasonable assurance that a person claiming to act in such role is in fact the named person designated to act in such role.
- (2) Agency:** Certicom may verify agency of the Contract Signer and the Certificate Approver by:
 - (A) 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 EV Guidelines) and obtaining confirmation that the Contract Signer and/or the Certificate Approver, as applicable, is an employee; or

- (B) Obtaining an Independent Confirmation From Applicant, or a Verified Legal Opinion (as described in Section 4.2.9(a)), or a Verified Accountant Letter (as described in Section 4.2.9(b)) verifying that the Contract Signer and/or the Certificate Approver, as applicable, is either an employee or has been otherwise been appointed as an agent of Applicant

Certicom may also verify the agency of the Certificate Approver via a certification from the Contract Signer (including in a contract between Certicom and the Applicant signed by the Contract Signer), provided that the employment or agency status and Signing Authority of the Contract Signer has been verified.

(c) Acceptable Methods of Verification - Authorization. Acceptable methods of verification of the Signing Authority of the Contract Signer, and the EV Authority of the Certificate Approver, as applicable, include:

- (1) Legal Opinion:** The Signing Authority of the Contract Signer, and/or the EV Authority of the Certificate Approver, may be verified by reliance on a Verified Legal Opinion (as described in Section 4.2.9(a));
- (2) Accountant Letter:** The Signing Authority of the Contract Signer, and/or the EV Authority of the Certificate Approver, may be verified by reliance on a Verified Accountant Letter (as described in Section 4.2.9 (b));
- (3) Corporate Resolution:** The Signing Authority of the Contract Signer, and/or the EV Authority of the Certificate Approver, may be verified by reliance on a properly authenticated corporate resolution that confirms that the person has been granted such Signing Authority, provided that such resolution is (1) certified by the appropriate corporate officer (e.g., secretary), and (2) Certicom reliably verify that the certification was validly signed by such person, and that such person does have the requisite authority to provide such certification.
- (4) Independent Confirmation from Applicant:** The Signing Authority of the Contract Signer, and/or the EV Authority of the Certificate Approver, may be verified by obtaining an Independent Confirmation From Applicant.
- (5) Contract between CA and Applicant:** The EV Authority of the Certificate Approver may be verified by reliance on a contract between Certicom and the Applicant that designates the Certificate Approver with such EV Authority, provided the contract is signed by the Contract Signer and provided that the agency and Signing Authority of the Contract Signer has been verified.

(d) Pre-Authorized Certificate Approver. Where Certicom and the Applicant contemplate the submission of multiple future EV Certificate Requests, then, after Certicom:

- (1) Has verified the name and title of the Contract Signer and that he/she is an employee or agent of the Applicant, and
- (2) Has verified the Signing Authority of such Contract Signer in accordance with one of the procedures in the preceding Subsection (c) above,

Certicom and the Applicant may enter into a written agreement, signed by the Contract Signer on behalf of the Applicant, whereby, for a specified term, the Applicant expressly authorizes one or more Certificate Approver(s) designated in such agreement to exercise EV Authority with respect to each future EV Certificate Application submitted on behalf of the Applicant (provided that such Applications are properly authenticated as originating with, or otherwise being approved by, such Certificate Approver(s)).

Such an agreement will provide that the Applicant shall be obligated under the Subscriber Agreement for all EV Certificates issued at the request of, or approved by, such Certificate Approver(s) until such EV Authority is revoked, and will include mutually

agreed-upon provisions for (i) authenticating the Certificate Approver when EV Certificate Requests are approved, (ii) periodic re-confirmation of the EV Authority of the Certificate Approver, (iii) secure procedure by which the Applicant can notify Certicom that the EV Authority of any such Certificate Approver is revoked, and (iv) such other appropriate precautions as are reasonably necessary.

4.2.7 Verification of Signature on Subscriber Agreement and EV Certificate Requests.

Both the Subscriber Agreement and each EV Certificate Request must be signed. The Subscriber Agreement must be signed by an authorized Contract Signer. The EV Certificate Request will be signed by the Certificate Requester submitting the document. If the Certificate Requester is not also an authorized Certificate Approver, an authorized Certificate Approver must independently approve the EV Certificate Request. In all cases, the signature must be a legally valid and enforceable seal or handwritten signature (for a paper Subscriber Agreement and/or EV Certificate Request), or a legally valid and enforceable electronic signature (for an electronic Subscriber Agreement and/or EV Certificate Request), that binds the Applicant to the terms of each respective document.

(a) Verification Requirements.

- (1) Signature. Certicom will authenticate the signature of the Contract Signer on the Subscriber Agreement and the signature of the Certificate Requester on each EV Certificate Request in a manner that makes it reasonably certain that the person named as the signer in the applicable document is, in fact, the person who signed the document on behalf of the Applicant.
- (2) Approval Alternative: In cases where an EV Certificate Request is signed and submitted by a Certificate Requester who does not also function as a Certificate Approver, approval and adoption of the EV Certificate Request by a Certificate Approver in accordance with the requirements of Section 4.2.6 can substitute for authentication of the signature of the Certificate Requester on such EV Certificate Request.

(b) Acceptable Methods of Signature Verification. Acceptable methods of authenticating the signature of the Certificate Requester or Contract Signer include:

- (1) A phone call to the Applicant's or Agent's phone number, as verified in accordance with the EV Guidelines, asking to speak to the Certificate Requester or Contract Signer, as applicable, followed by a response from someone who identifies themselves as such person confirming that he/she did sign the applicable document on behalf of the Applicant;
- (2) A letter mailed to the Applicant's or Agent's address, as verified through independent means in accordance with the EV Guidelines, c/o of the Certificate Requester or Contract Signer, as applicable, followed by a phone or mail response from someone who identifies themselves as such person confirming that he/she did sign the applicable document on behalf of the Applicant;
- (3) Use of a signature process that establishes the name and title of the signer in a secure manner, such as through use of an appropriately secure login process that identifies the signer before signing, or through use of a digital signature made with reference to an appropriately verified certificate; or
- (4) Notarization by a notary, provided that Certicom independently verifies that such notary is a legally qualified notary in the jurisdiction of the Certificate Requester or Contract Signer;

4.2.8 Verification of Approval of EV Certificate Request

- (a) **Verification Requirements.** In cases where an EV Certificate Request is submitted by a Certificate Requester, before Certicom may issue the requested EV Certificate, Certicom will verify that an authorized Certificate Approver reviewed and approved the EV Certificate Request.
- (b) **Acceptable Methods of Verification.** Acceptable methods of verifying the Certificate Approver's approval of an EV Certificate Request include:
- (1) Contacting the Certificate Approver by phone or mail at a verified phone number or address for the applicant and obtaining oral or written confirmation that the Certificate Approver has reviewed and approved the EV Certificate Request;
 - (2) Notifying the Certificate Approver that one or more new EV Certificate Requests are available for review and approval at a designated access-controlled and secure website, followed by a login by and an indication of approval from the Certificate Approver in the manner required by the website; or
 - (3) Verifying the signature of the Certificate Requestor on the EV Certificate Request in accordance with Section 4.2.7.

4.2.9 Verification of Certain Information Sources

(a) **Verified Legal Opinion.**

- (1) Verification Requirements. Before relying on any legal opinion submitted to Certicom, Certicom will verify that such legal opinion meets the following requirements ("Verified Legal Opinion"):
 - (A) Status of Author. Certicom will verify that the legal opinion is authored by an independent legal practitioner retained by and representing the Applicant (or an in-house legal practitioner employed by the Applicant) (Legal Practitioner) who is either:
 - (i) A lawyer (or solicitor, barrister, advocate, or equivalent) licensed to practice law in the country of the Applicant's Jurisdiction of Incorporation or Registration 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 Registration 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. Certicom will verify 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) Authenticity. Certicom will confirm the authenticity of the Verified Legal Opinion.
- (2) Acceptable Methods of Verification. Acceptable methods of establishing the foregoing requirements for a Verified Legal Opinion include:
 - (A) Status of Author. Certicom will verify the professional status of the author of the legal opinion by directly contacting, or querying the online licensing database of, the authority responsible for registering or licensing such Legal Practitioner(s) in the applicable jurisdiction.

- (B) Basis of Opinion. The text of the legal opinion will make it clear that the Legal Practitioner is acting on behalf of Applicant and that the conclusions of the legal opinion are based on the Legal Practitioner's stated familiarity with the relevant facts and the exercise of the practitioner's professional judgment and expertise. The legal opinion may also include disclaimers and other limitations customary in the Legal Practitioner's jurisdiction, provided that the scope of the disclaimed responsibility is not so great as to eliminate any substantial risk (financial, professional, and/or reputational) to the Legal Practitioner, should the legal opinion prove to be erroneous.
- (C) Authenticity. To confirm the authenticity of the legal opinion, Certicom will call or send a copy of the legal opinion back to the Legal Practitioner at the address, phone number, facsimile, or (if available) e-mail address for the Legal Practitioner listed with the authority responsible for registering or licensing such Legal Practitioner and obtain confirmation from the Legal Practitioner or the Legal Practitioner's assistant that the legal opinion is authentic. If a phone number is not available from the licensing authority, Certicom may use the number listed for the Legal Practitioner in records provided by the applicable phone company, a QGIS, or a QIIS.

In circumstances where the opinion is digitally signed, in a manner that confirms the authenticity of the document and the identity of the signer, as verified by Certicom in Section 4.2.9(A), no further verification of authenticity is required.

(b) Verified Accountant Letter.

- (1) Verification Requirements. Before relying on any accountant letter submitted to Certicom, Certicom will verify that such accountant letter meets the following requirements ("Verified Accountant Letter"):
 - (A) Status of Author. Certicom will verify that the accountant letter is authored by an independent professional accountant retained by and representing the Applicant (or an in-house professional accountant employed by the Applicant) (Accounting Practitioner) who is a certified public accountant, chartered accountant, or equivalent licensed by a full member of the International Federation of Accountants (IFAC) to practice accounting in the country of the Applicant's Jurisdiction of Incorporation or any jurisdiction where the Applicant maintains an office or physical facility; or
 - (B) Basis of Opinion. Certicom will verify that the Accounting Practitioner is acting on behalf of the Applicant and that the conclusions of the Verified Accountant Letter are based on the Accounting Practitioner's stated familiarity with the relevant facts and the exercise of the Accounting Practitioner's professional judgment and expertise.
 - (C) Authenticity. Certicom will confirm the authenticity of the Verified Accountant Letter.
- (2) Acceptable Methods of Verification. Acceptable methods of establishing the foregoing requirements for a Verified Accountant Letter are:
 - (A) Status of Author. Certicom will verify the professional status of the author of the accountant letter by directly contacting, or querying the online licensing database of, the authority responsible for registering or licensing such Accounting Practitioner (s) in the applicable jurisdiction.
 - (B) Basis of Opinion. The text of the accountant letter will make clear that the Accounting Practitioner is acting on behalf of the Applicant and that the information in the accountant letter is based on the Accounting Practitioner's stated familiarity with the relevant facts and the exercise of the practitioner's

professional judgment and expertise. The accountant letter may also include disclaimers and other limitations customary in the Accounting Practitioner's jurisdiction, provided that the scope of the disclaimed responsibility is not so great as to eliminate any substantial risk (financial, professional, and/or reputational) to the Accounting Practitioner should the accountant letter prove to be erroneous.

- (C) **Authenticity.** To confirm the authenticity of the accountant's opinion, Certicom will call or send a copy of the accountant letter back to the Accounting Practitioner at the address, phone number, facsimile, or (if available) e-mail address for the Accounting Practitioner listed with the authority responsible for registering or licensing such Accounting Practitioner and obtain confirmation from the Accounting Practitioner or the Accounting Practitioner's assistant that the accountant letter is authentic. If a phone number is not available from the licensing authority, Certicom may use the number listed for the Accountant in records provided by the applicable phone company, a QGIS, or a QIIS.

In circumstances where the opinion is digitally signed, in a manner that confirms the authenticity of the document and the identity of the signer, as verified by the CA in Section 4.2.9(A), no further verification of authenticity is required.

(c) Face-to-face Validation.

- (1) **Verification Requirements.** Before relying on any face-to-face vetting documents submitted to Certicom, Certicom will verify that the Third-Party Validator meets the following requirements:
- (A) **Qualification of Third-Party Validator.** Certicom will 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;
 - (B) **Document chain of custody.** Certicom will verify that the Third-Party Validator viewed the Vetting Documents in a face-to-face meeting with the individual being validated
 - (C) **Verification of Attestation.** If the Third-Party Validator is not a Latin Notary, then Certicom will confirm the authenticity of the attestation and vetting documents.
- (2) **Acceptable Methods of Verification.** Acceptable methods of establishing the foregoing requirements for vetting documents are:
- (A) **Qualification of Third-Party Validator.** Certicom will verify the professional status of the Third-Party Validator by directly contacting the authority responsible for registering or licensing such Third-Party Validators in the applicable jurisdiction.
 - (B) **Document Chain of Custody.** The Third-Party Validator MUST submit a statement to Certicom which attests that they obtained the Vetting Documents submitted to Certicom for the individual during a face-to-face meeting with the individual.
 - (C) **Verification of Attestation.** If the Third-Party Validator is not a Latin Notary, then Certicom will confirm the authenticity of the vetting documents received from the Third-Party Validator. Certicom will make a telephone call to the Third-Party Validator and obtain confirmation from them or their assistant that they performed the face-to-face validation. Certicom may rely upon self-reported information obtained from the Third-Party Validator for the sole purpose of performing this verification process. In circumstances where the attestation is digitally signed, in a manner that confirms the authenticity of the documents, and the identity of the signer as verified by Certicom, no further verification of authenticity is required.

(d) Independent Confirmation From Applicant. An “Independent Confirmation From Applicant” is a confirmation of a particular fact (e.g., knowledge of its exclusive control of a domain name, confirmation of the employee or agency status of a Contract Signer or Certificate Approver, confirmation of the EV Authority of a Certificate Approver, etc.) that:

- (i) Received by Certicom from a person employed by the Applicant (other than the person who is the subject of the inquiry) who has the appropriate authority to confirm such a fact (“Confirming Person”), and who represents that he/she has confirmed such fact;
- (ii) Received by Certicom in a manner that authenticates and verifies the source of the confirmation; and
- (iii) Binding on the Applicant.

An Independent Confirmation From Applicant may be obtained via the following procedure:

- (1) Confirmation Request: Certicom will initiate an appropriate out-of-band communication requesting verification or confirmation of the particular fact in issue (“Confirmation Request”) as follows:
 - (A) Addressee: The Confirmation Request will be directed to:
 - (i) A position within Applicant’s organization that qualifies as a Confirming Person (e.g., Secretary, President, CEO, CFO, COO, CIO, CSO, Director, etc.) and is identified by name and title in a current Qualified Government Information Source (e.g., an SEC filing), a Qualified Independent Information Source, a Qualified Government Tax Information Source, a Verified Legal Opinion, a Verified Accountant Letter, or 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); or
 - (ii) 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.
 - (iii) A named individual verified to be in the direct line of management above the Contract Signer or Certificate Approver by contacting Applicant’s Human Resources Department by phone or mail (at the phone number or address for Applicant’s Place of Business, verified in accordance with the EV Guidelines).
 - (B) Means of Communication: The Confirmation Request will be directed to the Confirming Person in a manner reasonably likely to reach such person. The following options are acceptable:
 - (i) By paper mail, addressed to the Confirming Person at:
 - (a) The address of Applicant’s Place of Business as verified by Certicom in accordance with the EV Guidelines; or
 - (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 Qualified Government Tax 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

- (ii) By e-mail addressed to the Confirming Person at the business e-mail address for such person listed in a current Qualified Government Information Source, a Qualified Government Tax Information Source, a Qualified Independent Information Source, a Verified Legal Opinion, or a Verified Accountant Letter; or
 - (iii) By telephone call to the Confirming Person, where such person is contacted by calling the main phone number of Applicant's Place of Business (verified in accordance with the EV Guidelines) and asking to speak to such person, and a person taking the call identifies himself as such person; or
 - (iv) By facsimile to the Confirming Person at the Place of Business. The facsimile number must be listed in a current Qualified Government Information Source, a Qualified Independent Information Source, a Qualified Government Tax Information Source, a Verified Legal Opinion, or a Verified Accountant Letter. The cover page must be clearly addressed to the Confirming Person.
- (2) Confirmation Response: Certicom will receive a response to the Confirmation Request from a Confirming Person that confirms the particular fact in issue. Such response may be provided to Certicom by telephone, by e-mail, or by paper mail, so long as Certicom reliably verify that it was provided by a Confirming Person in response to the Confirmation Request.

(e) Qualified Independent Information Sources (QIIS). A regularly-updated and current online publicly available database designed for the purpose of accurately providing the information for which it is consulted, and which is generally recognized as a dependable source of such information. A Commercial database is QIIS if the following are true:

- (1) data it contains 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.

Databases in which Certicom or its owners or affiliated companies maintain a controlling interest, or in which any registration agents (RAs) or subcontractors to whom Certicom has outsourced any portion of the vetting process (or their owners or affiliated companies) maintain any ownership or beneficial interest do not qualify as a QIIS. Certicom may check the accuracy of the database and ensure its data is acceptable.

(f) Qualified Government Information Source (QGIS). A regularly-updated and current publicly available database designed for the purpose of accurately providing the information for which it is consulted, and which is generally recognized as a dependable source of such information provided they are that it is maintained by a Government Entity, the reporting or recording of data is required by law and false or misleading reporting or recording is punishable with criminal or civil penalties. Nothing in these Guidelines shall prohibit the use of third-party vendors to obtain the information from the Government Entity provided that the third party obtains the information directly from the Government Entity.

- (g) Qualified Government Tax Information Source (QGTIS).** 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).

4.2.10 Other Verification Requirements

(a) High Risk Status

- (1) Verification Requirements. Certicom will seek to identify Applicants likely to be at a high risk of being targeted for fraudulent attacks (“High Risk Applicants”), and conduct such additional verification activity and take such additional precautions as are reasonably necessary to ensure that such Applicants are properly verified under the EV Guidelines.
- (2) Acceptable Methods of Verification. Certicom may identify High Risk Applicants by checking appropriate lists of organization names that are most commonly targeted in phishing and other fraudulent schemes, and automatically flagging EV Certificate Requests from Applicants named on these lists for further scrutiny before issuance. Examples of such lists include:
 - (A) Lists of phishing targets published by the Anti-Phishing Work Group (APWG); and
 - (B) Internal databases maintained by Certicom that include previously revoked EV Certificates and previously rejected EV Certificate Requests due to suspected phishing or other fraudulent usage;

The information should then be used to flag suspicious new EV Certificate Requests. If an Applicant is flagged as a High Risk Applicant, Certicom will perform reasonably appropriate additional authentication and verification to be certain beyond reasonable doubt that the Applicant and the target in question are the same organization.

(b) Denied Lists and Other Legal Black Lists

- (1) Verification Requirements. Certicom will verify that if the Applicant, the Contract Signer or Certificate Approver, or if the Applicant’s Jurisdiction of Incorporation or Registration or Place of Business:
 - (a) Is identified on any government denied list, list of prohibited persons, or other list that prohibits doing business with such organization or person under the laws of the country of Certicom’s jurisdiction(s) of operation; and
 - (b) Has its Jurisdiction of Incorporation, Registration, or Place of Business in any country with which the laws of Certicom’s jurisdiction prohibit doing business

Certicom will not issue any EV Certificate to the Applicant if either the Applicant, the Contract Signer, or Certificate Approver or if the Applicant’s Jurisdiction of Incorporation or Registration or Place of Business is on any such list.

- (2) Acceptable Methods of Verification. Certicom will take reasonable steps to verify with the following lists and regulations:

If Certicom has operations in the U.S., Certicom will take reasonable steps to verify with the following US Government Denied lists and regulations:

- (A) BIS Denied Persons List - <http://www.bis.doc.gov/dpl/thedeniallist.asp>
- (B) BIS Denied Entities List - <http://www.bis.doc.gov/Entities/Default.htm>

- (C) US Treasury Department List of Specially Designated Nationals and Blocked Persons - <http://www.treas.gov/ofac/t11sdn.pdf>
 - (D) US Government export regulations
- (3) If Certicom has operations in any other country, Certicom will take reasonable steps to verify with all equivalent denied lists and export regulations (if any) in such other country.

4.2.11 Final Cross-Correlation and Due Diligence

Except for EV Subscriber Certificates approved by an Enterprise RA:

- (a) The results of the verification processes and procedures outlined in this EV CPS and the EV Guidelines are intended to be viewed both individually and as a group. Thus, after all of the verification processes and procedures are completed, Certicom will have a person who is not responsible for the collection of information review all of the information and documentation assembled in support of the EV Certificate application and look for discrepancies or other details requiring further explanation.
- (b) Certicom will obtain and document 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) Certicom will refrain from issuing 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 Certicom 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, Certicom may decline the EV Certificate Request and notify the Applicant accordingly.
- (d) In the case where some or all of the documentation used to support the application is in a language other than English, Certicom or an affiliate of Certicom will perform the requirements of this Final Cross-Correlation and Due Diligence section using employees under its control and having appropriate training, experience, and judgment in confirming organizational identification and authorization and fulfilling all qualification requirements contained in Section 29 of the EV Guidelines. When employees under the control of Certicom do not possess the language skills necessary to perform the Final Cross-Correlation and Due Diligence Certicom may:
 - (i) Rely on language translations of the relevant portions of the documentation, provided that the translations are received from a Translator; or
 - (ii) When Certicom has utilized the services of a RA, Certicom may rely on the language skills of the RA to perform the Final Cross-Correlation and Due Diligence, provided the RA complies with a, b, and c above. Notwithstanding the foregoing, prior to issuing the EV Certificate, Certicom MUST review the work completed by the RA and determine that all requirements have been met; or
 - (iii) When Certicom has utilized the services of a RA, Certicom may rely on the RA to perform the Final Cross-Correlation and Due Diligence, provided that the RA complies with this section and is subjected to the Audit Requirements of Sections 35 (b) and (c) of the EV Guidelines.

Furthermore, in the case of Enterprise EV Certificates to be issued in compliance with the requirements of Section 30 of the EV Guidelines, the Enterprise RA may perform the requirements of this Final Cross-Correlation and Due Diligence section.

4.3 Validation Information for Certificate Applications

Applications for Certicom certificates are supported by appropriate documentation to establish the identity of an applicant.

From time to time, Certicom may modify the requirements related to application information for individuals, to respond to Certicom's requirements, the business context of the usage of a digital certificate, or as prescribed by law.

4.3.1 Application Information for Organizational Applicants

The EV Certificate Request may include all factual information about the Applicant to be included in the EV Certificate, and such additional information as is necessary for Certicom to obtain from Applicant in order to comply with the EV Guidelines and Certicom's own policies. In cases where the EV Certificate Request does not contain all necessary information about Applicant, Certicom will obtain the remaining information from either the Certificate Approver or Contract Signer or, having obtained it from a reliable source, confirm it with the Certificate Approver or Contract Signer.

Application information shall include, but not be limited to, the following information:

- a) Organization Name: Applicant's formal legal organization name to be included in the EV Certificate, as recorded with the Incorporating or Registration Agency in Applicant's Jurisdiction of Incorporation or Registration (for Private Organizations), or as specified in the law of the political subdivision in which the Government Entity operates (for Government Entities), or as registered with the government business Registration Agency (for Business Entities);
- b) Assumed Name (Optional): Applicant's assumed name (e.g., d/b/a name) to be included in the EV Certificate, as recorded in the jurisdiction of Applicant's Place of Business, if requested by Applicant;
- c) Domain Name: Applicant's domain name(s) to be included in the EV Certificate;
- d) Jurisdiction of Incorporation or Registration: Applicant's Jurisdiction of Incorporation or Registration to be included in the EV Certificate, and consisting of:
 - i. City or town (if any),
 - ii. State or province (if any), and
 - iii. Country.
- e) Incorporating or Registration Agency: The name of the Applicant's Incorporating or Registration Agency;
- f) Registration Number: The Registration Number assigned to Applicant by the Incorporating or Registration Agency in Applicant's Jurisdiction of Incorporation or Registration and to be included in the EV Certificate. If the Incorporating or Registration Agency does not issue Registration numbers, then the date of Incorporation or Registration must be included instead.
- g) Applicant Address: The address of Applicant's Place of Business, including –
 - i. Building number and street,
 - ii. City or town,
 - iii. State or province (if any),
 - iv. Country,
 - v. Postal code (zip code), and
 - vi. Main telephone number.

- h) Certificate Approver: Name and contact information of the Certificate Approver submitting and signing, or that has authorized the Certificate Requester to submit and sign, the EV Certificate Application on behalf of the Applicant; and
- i) Certificate Requester: Name and contact information of the Certificate Requester submitting the EV Certificate Request on behalf of the Applicant, if other than the Certificate Approver.

4.3.2 Validity Period for Validated Data

The maximum validity period for validated data that can be used to support issuance of an EV Certificate (before revalidation is required) is as follows:

- a) Legal existence and identity – one (1) year;
- b) Assumed name – one (1) year;
- c) Address of Place of Business – one (1) year, but thereafter data may be refreshed by checking a Qualified Independent Information Source, even where a site visit was originally required;
- d) Telephone number for Place of Business – one (1) year;
- e) Bank account verification – one (1) years;
- f) Domain name – one (1) year;
- g) Identity and authority of Certificate Approver – one (1) year, unless a contract is in place between Certicom and the Applicant that specifies a different term, in which case, the term specified in such contract will control. For example, the contract may use terms that allow the assignment of roles that are perpetual until revoked, or until the contract expires or is terminated.

4.3.3 Reuse and Updating Information and Documentation

Certicom may issue multiple EV Certificates listing the same Subject and based on a single EV Certificate Request, subject to the aging and updating requirement in (b) below.

- a) Each EV Certificate issued by Certicom will be supported by a valid current EV Certificate Request and a Subscriber Agreement signed by the Applicant Representative on behalf of the Applicant.
- b) The age of information used by Certicom to verify such an EV Certificate Request will not exceed the Maximum Validity Period for such information set forth in the EV Guidelines in Section 4.8, based on the earlier of the date the information was obtained (e.g., the date of a confirmation phone call) or the date the information was last updated by the source (e.g., if an online database was accessed by Certicom on July 1, but contained data last updated by the vendor on February 1, then the date of information would be considered to be February 1).
- c) In the case of outdated information, Certicom will repeat the verification processes required in this EV CPS.

4.4 Validation Requirements for Certificate Applications

Before issuing an EV Certificate, Certicom ensures that all Subject organization information in the EV Certificate conforms to the requirements of, and has been verified in accordance with, the EV Guidelines and matches the information confirmed and documented Certicom pursuant to its verification processes. Certicom confirms the following information:

- (1) Applicant's existence and identity, including;
 - a. Applicant's legal existence and identity (as established with an Incorporating Agency);

- b. Applicant's physical existence (business presence at a physical address); and
- c. Applicant's operational existence (business activity)
- (2) Applicant is a registered holder or has exclusive control of the domain name to be included in the EV Certificate; and
- (3) Applicant's authorization for the EV Certificate, including:
 - a. the name, title, and authority of the Contract Signer, Certificate Approver, and Certificate Requester;
 - b. that Contract Signer signed the Subscriber Agreement; and
 - c. that a Certificate Approver has signed or otherwise approved the EV Certificate Request

For all Certicom EV certificates, the subscriber has a continuous obligation to monitor the accuracy of the submitted information and notify Certicom of any changes that would affect the validity of the certificate. Failure to comply with the obligations as set out in the subscriber agreement will result in the revocation of the Subscriber's Digital Certificate without further notice to the Subscriber and the Subscriber shall pay any Charges payable but that have not yet been paid under the Agreement.

4.4.1 Serial Number Assignment

Certicom assigns certificate serial numbers that appear in Certicom certificates. Assigned serial numbers are unique.

4.5 Time to Confirm Submitted Data

Certicom makes reasonable efforts to confirm certificate application information and issue a digital certificate within reasonable time frames.

4.6 Approval and Rejection of Certificate Applications

Following successful completion of all required validations of a certificate application Certicom may approve an application for a digital certificate.

If the validation of a certificate application fails, Certicom rejects the certificate application. Certicom reserves its right to reject applications to issue a certificate to applicants if, on its own assessment, by issuing a certificate to such parties the good and trusted name of Certicom might get tarnished, diminished or have its value reduced and under such circumstances may do so without incurring any liability or responsibility for any loss or expenses arising as a result of such refusal.

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

4.7 Certificate Issuance and Subscriber Consent

Certicom issues a certificate upon approval of a certificate application. A digital certificate is deemed to be valid at the moment a subscriber accepts it (refer to section 4.9 of this EV CPS). Issuing a digital certificate means that Certicom accepts a certificate application.

4.8 Certificate Validity

Certificates are valid upon issuance by Certicom and acceptance by the subscriber. The validity period for an EV Certificate will not exceed twenty seven (27) months. Generally, the Certicom EV Certificate standard validity period will be 1 year, however, Certicom reserves the right to offer validity periods outside this standard validity period.

4.9 Certificate Acceptance by Subscribers

An issued certificate is either delivered via email or installed on a subscriber's computer / hardware security module through an online collection method. A subscriber is deemed to have accepted a certificate when:

- the subscriber uses the certificate, or
- 30 days pass from the date of the issuance of a certificate

4.10 Verification of Digital Signatures

Verification of a digital signature is used to determine that:

- the private key corresponding to the public key listed in the signer's certificate created the digital signature, and
- the signed data associated with this digital signature has not been altered since the digital signature was created.

4.11 Reliance on Digital Signatures

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

- the digital signature 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 Certificate Revocation Lists 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 suggested in the EV CPS and named as Object Identifiers in the certificate profile; and
- the digital certificate applied for is appropriate for the application it is used in,

Reliance is accepted as reasonable under the provisions made for the relying party under this EV CPS and within the relying party agreement. If the circumstances of reliance exceed the assurances delivered by Certicom under the provisions made in this EV CPS, the relying party must obtain additional assurances.

Warranties are only valid if the steps detailed above have been carried out.

4.12 Certificate Suspension

Certicom does not utilize certificate suspension.

4.13 Certificate Revocation and Compromise

Revocation of a certificate is to permanently end the operational period of the certificate prior to reaching the end of its stated validity period. Certicom maintains a 24x7 ability to accept and respond to revocation requests and related inquiries. Certicom may revoke an EV Certificate it has issued in the event that Certicom has reasonable grounds to believe that any of the following events has occurred:

- a) Either the Subscriber's or Certicom's obligations under this EV CPS or the relevant Subscriber Agreement are delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's reasonable control, and as a result another person's information is materially threatened or compromised;

- b) The certificate was issued to persons or entities identified as publishers of malicious software or that impersonated other persons or entities;
- c) The certificate was issued as a result of fraud or negligence; or
- d) The certificate, if not revoked, will compromise the trust status of Certicom.
- e) Subscriber requests revocation of its EV Certificate;
- f) Subscriber indicates that the original EV Certificate Request was not authorized and does not retroactively grant authorization;
- g) Certicom obtains reasonable evidence that the Subscriber's Private Key (corresponding to the Public Key in the EV Certificate) has been compromised, or that the EV Certificate has otherwise been misused, or that a personal identification number, Private Key or password has, or is likely to become known to someone not authorized to use it, or is being or is likely to be used in an unauthorized way;
- h) Certicom receives notice or otherwise become aware that a Subscriber violates any of its material obligations under the Subscriber Agreement or this EV CPS;
- i) Subscriber has used the Subscription Service contrary to law, rule or regulation or Certicom reasonably believes that the Subscriber is using the certificate, directly or indirectly, to engage in illegal or fraudulent activity;
- j) Certicom receives notice or otherwise becomes aware that a court or arbitrator has revoked Subscriber's right to use the domain name listed in the EV Certificate, or that Subscriber has failed to renew its domain name;
- k) Certicom receives notice or otherwise becomes aware of a material change in the information contained in the EV Certificate;
- l) a determination, in Certicom's sole discretion, that the EV Certificate was not issued in accordance with the terms and conditions of the EV Guidelines or Certicom's EV Policies, including Certicom's CPS;
- m) Certicom determines that any of the information appearing in the EV Certificate is not accurate;
- n) Certicom ceases operations for any reason and has not arranged for another certificate authority to provide revocation support for the EV Certificate;
- o) Certicom's right to issue EV Certificates under the EV Guidelines expires or is revoked or terminated [unless Certicom makes arrangements to continue maintaining the CRL/OCSP Repository];
- p) Certicom's Private Key for Subscriber's EV Certificate has been or is suspected to be compromised;
- q) there has been, there is, or there is likely to be a violation of, loss of control over, or unauthorized disclosure of Confidential Information relating to the Subscription Service;
- r) the Subscriber has used the Subscription Service with third party software not authorized by Certicom for use with the Subscription Service;
- s) such additional revocation events as Certicom publishes in its EV Policies; or
- t) Certicom receives notice or otherwise becomes aware that Subscriber has been added as a denied party or prohibited person to a blacklist, or is operating from a prohibited destination under the laws of Certicom's jurisdiction of operation as described in Section 4.2.10 of the EV Guidelines.

4.13.1 Request for Revocation

The subscriber or other appropriately authorized parties such as RAs can request revocation of a certificate. Prior to the revocation of a certificate Certicom will verify that the revocation request has been:

- Made by the organization entity that has made the certificate application.
- Made by the RA on behalf of the organization entity that used the RA to make the certificate application Certicom employs the following procedure for authenticating a revocation request:
 - The revocation request must be sent by the Administrator contact associated with the certificate application. Certicom may if necessary also request that the revocation

request be made by the organizational contact and billing contact.

- Upon receipt of the revocation request Certicom will request confirmation from the known administrator out of bands contact details, either by telephone or by fax.
- Certicom validation personnel will then command the revocation of the certificate and logging of the identity of validation personnel and reason for revocation will be maintained in accordance with the logging procedures covered in this EV CPS.

4.13.2 Effect of Revocation

Upon revocation of a certificate, the operational period of that certificate is immediately considered terminated. The serial number of the revoked certificate will be placed within the Certificate Revocation List (CRL) and remains on the CRL until some time after the end of the certificate's validity period. An updated CRL is published on the Certicom website every 24 hours; however, under special circumstances the CRL may be published more frequently. Revoked Certificate information will also be added to Certicom's database for use by Certicom's OCSF Responder.

4.13.3 EV Certificate Problem Reporting and Response Capability

- (a) In addition to EV Certificate revocation, Certicom provides Subscribers, Relying Parties, Application Software Vendors, and other third parties with clear instructions for reporting complaints or suspected Private Key compromise, EV Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to EV Certificates ("Certificate Problem Reports"), and a 24x7 capability to accept and acknowledge such Reports.
- (b) Certicom begins investigation of all Certificate Problem Reports within twenty-four (24) hours and decides whether revocation or other appropriate action is warranted based on at least the following criteria:
 - (i) The nature of the alleged problem;
 - (ii) Number of Certificate Problem Reports received about a particular EV Certificate or website;
 - (iii) The identity of the complainants (for example, complaints from a law enforcement official that a web site is engaged in illegal activities have more weight than a complaint from a consumer alleging they never received the goods they ordered); and
 - (iv) Relevant legislation.
- (c) Certicom also maintains a continuous 24/7 ability to internally respond to any high priority 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.

4.14 Renewal

Before renewing an EV Certificate, Certicom must perform all authentication and verification tasks required by the EV Guidelines to ensure that the renewal request is properly authorized by the Applicant and that the information in the EV Certificate is still accurate and valid.

Renewal fees are detailed on the official Certicom websites and within communications sent to subscribers approaching the certificate expiration date.

Renewal application requirements and procedures are the same as those employed for the application validation and issuance requirements detailed for new customers.

4.15 Notice Prior to Expiration

Certicom shall make reasonable efforts to notify subscribers via e-mail of the imminent expiration of a digital certificate. Notice shall ordinarily be provided within a 60-day period prior to the expiry of the certificate.

5 Legal Conditions of Issuance

This part describes the legal representations, warranties and limitations associated with Certicom digital certificates.

5.1 Certicom Representations

Certicom makes to all subscribers and relying parties certain representations regarding its public service, as described below. Certicom reserves its right to modify such representations as it sees fit or required by law.

5.2 Information Incorporated by Reference into a Certicom Digital Certificate

Certicom incorporates by reference the following information in every digital certificate it issues:

- Terms and conditions of the digital certificate.
- Any other applicable certificate policy as may be stated on an issued Certicom certificate, including the location of this EV CPS.
- The mandatory elements of the standard X.509v3.
- Any non-mandatory but customized elements of the standard X.509v3.
- Content of extensions and enhanced naming that are not fully expressed within a certificate.
- Any other information that is indicated to be so in a field of a certificate.

5.3 Displaying Liability Limitations, and Warranty Disclaimers

Certicom certificates may include a brief statement describing limitations of liability, limitations in the value of transactions to be accomplished, validation period, and intended purpose of the certificate and disclaimers of warranty that may apply. Subscribers must agree to Certicom Terms & Conditions before signing-up for a certificate. To communicate information Certicom may use:

- An organizational unit attribute.
- A Certicom standard resource qualifier to a certificate policy.
- Proprietary or other vendors' registered extensions.

5.4 Publication of Certificate Revocation Data

Certicom reserves its right to publish a CRL (Certificate Revocation List) as may be indicated and may publish information as part of its OCSP responder operations.

5.5 Duty to Monitor the Accuracy of Submitted Information

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

5.6 Publication of Information

Published critical information may be updated from time to time as prescribed in this EV CPS. Such updates shall be indicated through appropriate version numbering and publication date on any new version.

5.7 Interference with Certicom Implementation

Subscribers, relying parties and any other parties shall not interfere with, or reverse engineer the technical implementation of Certicom PKI services including the key generation process, the public web site and the Certicom repositories except as explicitly permitted by this EV CPS or upon prior written approval of Certicom. Failure to comply with this as a subscriber will result in

the revocation of the Subscriber's Digital Certificate without further notice to the Subscriber and the Subscriber shall pay any Charges payable but that have not yet been paid under this Agreement. Failure to comply with this as a relying party will result in the termination of the agreement with the relying party, the removal of permission to use or access the Certicom repository and any Digital Certificate or Service provided by Certicom.

5.8 Standards

Certicom assumes that user software that is claimed to be compliant with X.509v3 and other applicable standards enforces the requirements set out in this EV CPS. Certicom cannot warrant that such user software will support and enforce controls required by Certicom, while the user should seek appropriate advice.

5.9 Certicom Partnerships Limitations

Partners of the Certicom network shall not undertake any actions that might imperil, put in doubt or reduce the trust associated with the Certicom products and services. Certicom partners shall specifically refrain from seeking partnerships with other root authorities or apply procedures originating from such authorities. Failure to comply with this will result in the termination of the agreement with the relying party, the removal of permission to use or access the Certicom repository and any Digital Certificate or Service provided by Certicom.

5.10 Certicom Limitation of Liability for a Certicom Partner

As the Certicom network includes RAs that operate under Certicom practices and procedures Certicom warrants the integrity of any certificate issued under its own root within the limits of the Certicom insurance policy and in accordance with this EV CPS.

5.11 Choice of Cryptographic Methods

Parties are solely responsible for having exercised independent judgment and employed adequate training in choosing security software, hardware, and encryption/digital signature algorithms, including their respective parameters, procedures, and techniques as well as PKI as a solution to their security requirements.

5.12 Reliance on Unverified Digital Signatures

Parties relying on a digital certificate must verify a digital signature at all times by checking the validity of a digital certificate against the relevant CRL published by Certicom. Relying parties are alerted that an unverified digital signature cannot be assigned as a valid signature of the subscriber.

Relying on an unverifiable digital signature may result in risks that the relying party, and not Certicom, assumes in whole.

By means of this EV CPS, Certicom has adequately informed relying parties on the usage and validation of digital signatures through this EV CPS and other documentation published in its public Repository or by contacting via out of bands means via the contact address as specified in the Document Control section of this EV CPS.

5.13 Rejected Certificate Applications

The private key associated with a public key, which has been submitted as part of a rejected certificate application, may not under any circumstances be used to create a digital signature if the effect of the signature is to create conditions of reliance upon the rejected certificate. The private key may also not be resubmitted as part of any other certificate application.

5.14 Refusal to Issue a Certificate

Certicom reserves its right to refuse to issue a certificate to any party as it sees fit, without incurring any liability or responsibility for any loss or expenses arising out of such refusal. Certicom reserves the right not to disclose reasons for such a refusal.

5.15 Subscriber Obligations

Unless otherwise stated in this EV CPS, subscribers shall exclusively be responsible:

- a) To minimize internal risk of private key compromise by ensuring adequate knowledge and training on PKI is provided internally.
- b) To generate their own private / public key pair to be used in association with the certificate request submitted to Certicom or a Certicom RA.
- c) Ensure that the public key submitted to Certicom or a Certicom RA corresponds with the private key used.
- d) Ensure that the public key submitted to Certicom or a Certicom RA is the correct one.
- e) Provide correct and accurate information in its communications with Certicom or a Certicom RA.
- f) Alert Certicom or a Certicom RA if at any stage while the certificate is valid, any information originally submitted has changed since it had been submitted to Certicom.
- g) Generate a new, secure key pair to be used in association with a certificate that it requests from Certicom or a Certicom RA.
- h) Read, understand and agree with all terms and conditions in this Certicom EV CPS and associated policies published in the Certicom Repository.
- i) Refrain from tampering with a Certicom certificate.
- j) Use Certicom certificates for legal and authorized purposes in accordance with the suggested usages and practices in this EV CPS.
- k) Cease using a Certicom certificate if any information in it becomes misleading, obsolete or invalid.
- l) Cease using a Certicom certificate if such certificate is expired and remove it from any applications and/or devices it has been installed on.
- m) Refrain from using the subscriber's private key corresponding to the public key in a Certicom issued certificate to issue end-entity digital certificates or subordinate CAs.
- n) Make reasonable efforts to prevent the compromise, loss, disclosure, modification, or otherwise unauthorized use of the private key corresponding to the public key published in a Certicom certificate.
- o) Request the revocation of a certificate in case of an occurrence that materially affects the integrity of a Certicom certificate.
- p) For acts and omissions of partners and agents, they use to generate, retain, escrow, or destroy their private keys.
- q) use or access the Subscription Service only in conjunction with the Software or other software that may be provided by Certicom from time to time or specified by Certicom to be appropriate for use in conjunction with the Subscription Service;
- r) install the Digital Certificate only on the server accessible at the domain name listed on the Digital Certificate, and use the Digital Certificate solely in compliance with all applicable laws, solely for authorized company business, and solely in accordance with the terms and conditions of this Agreement;
- s) be responsible, at its own expense, for access to the Internet and all other communications networks (if any) required in order to use the Subscription Service and Digital Certificate, and for the provision of all computer and

- telecommunications equipment and software required to use the Subscription Service, except where expressly provided otherwise herein;
- t) obtain and keep in force any authorization, permission or license necessary for the Subscriber to use the Subscription Service, except where Certicom expressly agrees to obtain the same under the terms of this Agreement;
 - u) bind each and every Relying Party using the Subscriber's Certicom Certificate(s) to substantially the following terms: "By relying upon a Certicom digital certificate, the user agrees to be bound by the Certicom Relying Party Agreement, which is incorporated herein in its entirety, and which can be found at https://www.Certicom.com/repository/relying_party.html";
 - v) be responsible for the generation of any Private Key belonging to the Subscriber, and take all reasonable measures, either by itself or through a subcontractor (e.g. hosting provider), to maintain sole control of, keep confidential, properly protect at all times, and ensure the proper use of the Private Key that corresponds to the Public Key to be included in the requested Digital Certificate, personal identification numbers, passwords and other access information or devices used in connection with the Subscription Service, and immediately inform Certicom if there is any reason to believe that any of the foregoing has or is likely to become known to someone not authorized to use it, or is being, or is likely to be used in an unauthorized way;
 - w) provide accurate and complete information to Certicom at all times, both upon requesting a Digital Certificate and thereafter as requested by Certicom in connection with the issuance of the Digital Certificate, and immediately inform Certicom if any of the Subscriber Data or information provided by the Subscriber to Certicom ceases to remain valid or correct or otherwise changes;
 - x) promptly cease all use of the Subscriber's Digital Certificate and its associated Private Key, and promptly request Certicom to revoke the Digital Certificate, in the event that any information in the Digital Certificate is or becomes incorrect or inaccurate, or there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key listed in the Digital Certificate;
 - y) promptly cease all use of the Private Key corresponding to the Public Key listed in a Digital Certificate upon expiration or revocation of such Digital Certificate;

5.16 Representations by Subscriber upon Acceptance

Upon accepting a certificate, the subscriber represents to Certicom and to relying parties that at the time of acceptance and until further notice:

- a) Digital signatures created using the private key corresponding to the public key included in the certificate is the digital signature of the subscriber and the certificate has been accepted and is properly operational at the time the digital signature is created.
- b) No unauthorized person has ever had access to the subscriber's private key.
- c) All representations made by the subscriber to Certicom regarding the information contained in the certificate are accurate and true.
- d) The certificate is used exclusively for authorized and legal purposes, consistent with this EV CPS.
- e) It will use a Certicom certificate only in conjunction with the entity named in the organization field of a digital certificate.
- f) The subscriber retains control of her private key, uses a trustworthy system, and takes reasonable precautions to prevent its loss, disclosure, modification, or unauthorized use.
- g) The subscriber is an end-user subscriber and not a CA, and will not use the private key corresponding to any public key listed in the certificate for purposes of signing any certificate (or any other format of certified public key) or CRL, as a

CA or otherwise, unless expressly agreed in writing between subscriber and Certicom.

- h) The subscriber agrees with the terms and conditions of this EV CPS, Subscriber Agreement and other agreements and policy statements of Certicom as provided to Subscriber.
- i) all Subscriber Data is, and any other documents or information provided by the Subscriber are, and will remain accurate and will not include any information or material (or any part thereof) the accessing or use of which would be unlawful, contrary to public interest or otherwise likely to damage the business or reputation of Certicom in any way;
- j) it has and will comply with all applicable consumer and other laws, regulations, instructions and guidelines, including those related to intellectual property protection, viruses, accessing computer systems, export laws and regulations for dual usage goods, as may be applicable, etc., with all relevant licenses and with all other codes of practice which apply to the Subscriber or Certicom and that the Subscriber has obtained all licenses and consents necessary to fully perform its obligations under this Agreement;
- k) it has full power and authority to enter into this Agreement and to perform all of its obligations under this Agreement;
- l) it shall have sole responsibility for all statements, acts and omissions which are made under any password provided by it to Certicom;
- m) the Subscriber grants Certicom permission to examine, evaluate, process and in some circumstances transmit to third parties located outside the United States the application data insofar as is reasonably necessary for Certicom to provide the Subscription Service; and
- n) any Digital Certificate "Warranty" or other warranty described in this CPS and provided by Certicom in connection with any Digital Certificate is provided solely for the benefit of Relying Parties, and Subscriber shall have no rights with respect thereto, including, but not limited to, any right to enforce the terms of or make any claim under any such warranty.

5.17 Indemnity by Subscriber

By accepting a certificate, the subscriber agrees to indemnify and hold Certicom, as well as its agent(s) and contractors harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind, including reasonable attorneys' fees, that Certicom, and the above mentioned parties may incur, that are caused by the use or publication of a certificate, and that arises from:

- Any false or misrepresented data supplied by the subscriber or agent(s).
- Any failure of the subscriber to disclose a material fact, if the misrepresentation or omission was made negligently or with intent to deceive Certicom, Certicom, or any person receiving or relying on the certificate.
- Failure to protect the subscriber's confidential data including their private key, or failure to take reasonable precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the subscriber's confidential data.
- Breaking any laws applicable in his/her country or territory including those related to intellectual property protection, viruses, accessing computer systems etc.

5.18 Obligations of Certicom Registration Authorities

A Certicom RA operates under the policies and practices detailed in this EV CPS and also the associated Web Host Reseller agreement, Powered SSL agreement and EPKI Manager Account agreement. The RA is bound under contract to:

- Receive applications for Certicom certificates in accordance with this EV CPS.

- Perform all verification actions prescribed by the Certicom validation procedures and this EV CPS.
- Receive, verify and relay to Certicom all requests for revocation of a Certicom certificate in accordance with the Certicom revocation procedures and the EV CPS.
- Act according to relevant Law and regulations.

5.19 Obligations of a Relying Party

A party relying on a Certicom certificate accepts that in order to reasonably rely on a Certicom certificate they must:

- Minimize the risk of relying on a digital signature created by an invalid, revoked, expired or rejected certificate; the relying party must have reasonably made the effort to acquire sufficient knowledge on using digital certificates and PKI.
- Study the limitations to the usage of digital certificates and be aware through the Relying Party agreement the maximum value of the transactions that can be made using a Certicom digital certificate.
- Read and agree with the terms of the Certicom EV CPS and relying party agreement.
- Verify a Certicom certificate by referring to the relevant CRL and the CRLs of intermediate CA and root CA.
- Trust a Certicom certificate only if it is valid and has not been revoked or has expired.
- Rely on a Certicom certificate, only as may be reasonable under the circumstances listed in this section and other relevant sections of this EV CPS.

5.20 Legality of Information

Subscribers shall solely be responsible for the legality of the information they present for use in certificates issued under this EV CPS, in any jurisdiction in which such content may be used or viewed.

5.21 Subscriber Liability to Relying Parties

Without limiting other subscriber obligations stated in this EV CPS, subscribers are liable for any misrepresentations they make in certificates to third parties that reasonably rely on the representations contained therein and have verified one or more digital signatures with the certificate.

5.22 Duty to Monitor Agents

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

5.23 Use of Agents

For certificates issued at the request of a subscriber's agent, both the agent and the subscriber shall jointly and severally indemnify Certicom, and its agents and contractors.

5.24 Conditions of usage of the Certicom Repository and Web site

Parties (including subscribers and relying parties) accessing the Certicom Repository and official web site(s) agree with the provisions of this EV CPS and any other conditions of usage that Certicom may make available. Parties demonstrate acceptance of the conditions of usage of the EV CPS by using a Certicom issued certificate.

Failure to comply with the conditions of usage of the Certicom Repositories and web site may result in terminating the relationship between Certicom and the party.

5.25 Accuracy of Information

Certicom, recognizing its trusted position, makes all reasonable efforts to ensure that parties accessing its Repositories receive accurate, updated and correct information. Certicom, however, cannot accept any liability beyond the limits set in this EV CPS and the Certicom insurance policy.

Failure to comply with the conditions of usage of the Certicom Repositories and web site may result in terminating the relationship between Certicom and the party.

5.26 Obligations of Certicom

To the extent specified in the relevant sections of the EV CPS, Certicom promises to:

- Comply with this EV CPS and its internal or published policies and procedures.
- Comply with applicable laws and regulations.
- Provide infrastructure and certification services, including but not limited to the establishment and operation of the Certicom Repository and web site for the operation of PKI services.
- Provide Trust mechanisms, including a key generation mechanism, key protection, and secret sharing procedures regarding its own infrastructure.
- Provide prompt notice in case of compromise of its private key(s).
- Provide and validate application procedures for the various types of certificates that it may make publicly available.
- Issue digital certificates in accordance with this EV CPS and fulfill its obligations presented herein.
- Upon receipt of a request from an RA operating within the Certicom network; act promptly to issue a Certicom certificate in accordance with this Certicom EV CPS.
- Upon receipt of a request for revocation from an RA operating within the Certicom network; act promptly to revoke a Certicom certificate in accordance with this Certicom EV CPS.
- Publish accepted certificates in accordance with this EV CPS.
- Provide support to subscribers and relying parties as described in this EV CPS.
- Revoke certificates according to this EV CPS.
- Provide for the expiration and renewal of certificates according to this EV CPS.
- Make available a copy of this EV CPS and applicable policies to requesting parties.
- Warrant the accuracy of information published on a Qualified Certificate issued pursuant to the requirements of the European Directive 99/93.
- Warrant that the signatory held the private key at the time of issuance of a certificate issued pursuant to the requirements for Qualified Certificates as in the European Directive 99/93.
- Comply with the requirements of the (i) the then-current WebTrust Program for certification authorities, and (ii) the then-current WebTrust EV Program, or an equivalent for both (i) and (ii) as approved by the CA/Browser Forum; and
- Be licensed as a certification authority in each jurisdiction where it operates if licensing is required by the law of such jurisdiction for the issuance of EV Certificates.

Certicom further warrants to the Subscriber entering into the Subscriber Agreement for the EV Certificate, the Subject named in the EV Certificate; all Application Software Vendors with whom Certicom has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Vendors; all Relying Parties that actually rely on such EV Certificate during the period when it is Valid that, during the period when the EV Certificate is Valid, it has followed the requirements of the EV Guidelines and the Certicom CPS in issuing the EV

Certificates and in verifying the information contained in the EV Certificate, including, but not limited to, the following:

- (A) Legal Existence: Certicom has confirmed with the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration 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: Certicom has confirmed that, as of the date the EV Certificate was issued, the legal name of the Subject named in the EV Certificate matches the name on the official government records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration, and if an assumed name is also included, that the assumed name is properly registered by the Subject in the jurisdiction of its Place of Business;
- (C) Right to Use Domain Name: Certicom has taken all steps reasonably necessary to verify that, as of the date the EV Certificate was issued, the Subject named in the EV Certificate has the exclusive right to use the domain name(s) listed in the EV Certificate;
- (D) Authorization for EV Certificate: Certicom has taken all steps reasonably necessary to verify that the Subject named in the EV Certificate has authorized the issuance of the EV Certificate;
- (E) Accuracy of Information: Certicom has taken all steps reasonably necessary to verify that all of the other information in the EV Certificate is accurate, as of the date the EV Certificate was issued;
- (F) Subscriber Agreement: The Subject named in the EV Certificate has entered into a legally valid and enforceable Subscriber Agreement with Certicom that satisfies the requirements of these Guidelines;
- (G) Status: Certicom will follow the requirements of these Guidelines and maintain a 24 x 7 online-accessible Repository with current information regarding the status of the EV Certificate as Valid or revoked; and
- (H) Revocation: Certicom will follow the requirements of these Guidelines and revoke the EV Certificate upon the occurrence of any revocation event as specified in these Guidelines.

The subscriber also acknowledges that Certicom has no further obligations under this EV CPS.

5.27 Fitness for a Particular Purpose

Certicom 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.

5.28 Other Warranties

Except as it may have otherwise been stated in relation to Qualified Certificates issued pursuant to the requirements of the European Directive 99/93 Certicom does not warrant:

- The accuracy, authenticity, completeness or fitness of any unverified information contained in certificates or otherwise compiled, published, or disseminated by or on behalf of Certicom except as it may be stated in the relevant product description below in this EV CPS and in the Certicom insurance policy.
- The accuracy, authenticity, completeness or fitness of any information contained in Certicom Personal certificates class 1, free, trial or demo certificates.

- In addition, shall not incur liability for representations of information contained in a certificate except as it may be stated in the relevant product description in this EV CPS.
- Does not warrant the quality, functions or performance of any software or hardware device.
- Although Certicom is responsible for the revocation of a certificate, it cannot be held liable if it cannot execute it for reasons outside its own control.
- The validity, completeness or availability of directories of certificates issued by a third party (including an agent) unless specifically stated by Certicom.
- That the subject named in an EV Certificate is actively engaged in doing business
- That the subject named on the EV Certificate complies' with applicable laws
- That the subject named in the EV Certificate is trustworthy, honest, or reputable in its business dealings.
- That it is "safe" to do business with the subject named in the EV Certificate.

5.29 Non-Verified Subscriber Information

Notwithstanding limitation warranties under the product section of this EV CPS, Certicom shall not be responsible for non-verified subscriber information submitted to Certicom, or the Certicom directory 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.

5.30 Exclusion of Certain Elements of Damages

In cases where Certicom has issued and managed the EV Certificate in compliance with the EV Guidelines and its EV CPS, Certicom shall not be liable to the EV Certificate Beneficiaries or any other third parties for any losses suffered as a result of use or reliance on such EV Certificate. In no event (except for fraud or willful misconduct) shall Certicom be liable for:

- Any indirect, incidental or consequential damages.
- Any loss of profits.
- 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 EV CPS.
- Any other damages except for those due to reliance, on the information featured on a certificate, on the verified information in a certificate.
- Any liability incurred in this case or any other case if the fault in this verified information is due to fraud or willful misconduct of the applicant. Any liability that arises from the usage of a certificate that has not been issued or used in conformance with this EV CPS.
- Any liability that arises from the usage of a certificate that is not valid.
- Any liability that arises from usage of a certificate that exceeds the limitations in usage and value and transactions stated upon it or on the EV CPS.
- Any liability that arises from security, usability, integrity of products, including hardware and software a subscriber uses.
- Any liability that arises from compromise of a subscriber's private key.

Certicom does not limit or exclude liability for death or personal injury.

5.31 Certificate Insurance Plan

In cases where Certicom has not issued or managed the EV Certificate in complete compliance with the EV Guidelines and this EV CPS, that resulted in a loss to a Subscriber or a Relying Party, Certicom limits its liability to the Subscriber and to the Relying Party for any cause of action

or legal theory involved for any and all claims, losses or damages suffered as a result of the use or reliance on such EV Certificate to US\$2,000 per Subscriber or Relying party per EV Certificate per incident, subject to the cumulative maximum limit of US \$2,000,000 for all claims related to that digital certificate. Except to the extent of willful misconduct, the liability of Certicom is limited to the negligent issuance of certificates.

Under Certicom's warranty a covered person may only receive a maximum payment of \$2,000 per online transaction ("Incident Limit") for which the Covered Person claims there was a breach of the Certicom Warranty (each an "Incident"). If multiple Covered Persons are affiliated as to a common entity, then those multiple Covered Persons collectively are eligible to receive a maximum amount of \$2,000 per Incident. Any payments to Covered Persons shall decrease by an amount equal to the sum of such payments the relevant Aggregate Limit available to any party for future payments for any claims relating to that Digital Certificate. For example, if a Digital Certificate carries a Payment Limit of \$10,000, then Covered Persons can receive payments in accordance with this warranty for up to \$2,000 per Incident until a total of \$10,000 has been paid in the aggregate for all claims by all parties related to that Digital Certificate. Upon renewal of any Digital Certificate, the total claims paid for such Digital Certificate shall be reset to zero dollars.

Certicom also maintains Professional Liability/Errors & Omissions insurance with a policy limit of \$5 million in coverage and including coverage for (i) claims for damages arising out of an act, error, or omission, unintentional breach of contract, or neglect in issuing or maintaining EV Certificates, and (ii) claims for damages arising out of infringement of the proprietary rights of any third party (excluding copyright, and trademark infringement), and invasion of privacy and advertising injury.

All of Certicom's insurance is with a company rated no less than A- as to Policy Holder's Rating in the current edition of Best's Insurance Guide (or with an association of companies each of the members of which are so rated).

5.32 Financial Limitations on Certificate Usage

Certicom certificates may only be used in connection with data transfer and transactions having a US dollar (US\$) value no greater than the max transaction value associated with the certificate, which is US \$100,000.

5.33 Damage and Loss Limitations

In no event (except for fraud or willful misconduct) will the aggregate liability of Certicom to all parties including without any limitation a subscriber, an applicant, a recipient, or a relying party for all digital signatures and transactions related to such certificate exceed the cumulative maximum liability for such certificate as stated in the Certicom insurance plan detailed section 5.31 of this EV CPS.

5.34 Conflict of Rules

When this EV CPS conflicts with other rules, guidelines, or contracts, this EV CPS shall prevail and bind the subscriber and other parties except as to other contracts either:

- Predating the first public release of the present version of this EV CPS.
- Expressly superseding this EV CPS for which such contract shall govern as to the parties thereto, and to the extent permitted by law.

5.35 Certicom Intellectual Property Rights

Certicom or its partners or associates own all intellectual property rights associated with its databases, web sites, Certicom digital certificates and any other publication originating from Certicom including this EV CPS.

5.36 Infringement and Other Damaging Material

Certicom subscribers represent and warrant that when submitting to Certicom and using a domain and distinguished name (and all other certificate application information) they do not interfere with or infringe any 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, and confusing or misleading a person, whether natural or incorporated.

Although Certicom will provide all reasonable assistance, certificate subscribers shall defend, indemnify, and hold Certicom harmless for any loss or damage resulting from any such interference or infringement and shall be responsible for defending all actions on behalf of Certicom.

5.37 Ownership

Certificates are the property of Certicom. Certicom gives permission to reproduce and distribute certificates on a nonexclusive, royalty-free basis, provided that they are reproduced and distributed in full. Certicom reserves the right to revoke the certificate at any time. Private and public keys are property of the subscribers who rightfully issue and hold them. All secret shares (distributed elements) of the Certicom private key remain the property of Certicom.

5.38 Governing Law

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

5.39 Jurisdiction

Each party, including Certicom partners, subscribers and relying parties, irrevocably agrees that the Court of Manhattan District, New York, USA has 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 EV CPS or the provision of Certicom PKI services.

5.40 Dispute Resolution

Before resorting to any dispute resolution mechanism including adjudication or any type of Alternative Dispute Resolution (including without exception mini-trial, arbitration, binding expert's advice, co-operation monitoring and normal expert's advice) parties agree to notify Certicom of the dispute with a view to seek dispute resolution.

5.41 Successors and Assigns

This EV CPS shall be binding upon the successors, executors, heirs, representatives, administrators, and assigns, whether express, implied, or apparent, of the parties. The rights and obligations detailed in this EV CPS are assignable by the parties, by operation of law (including

as a result of merger or a transfer of a controlling interest in voting securities) or otherwise, provided such assignment is undertaken consistent with this EV CPS articles on termination or cessation of operations, and provided that such assignment does not effect a novation of any other debts or obligations the assigning party owes to other parties at the time of such assignment.

5.42 Severability

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

Each and every provision of this EV 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.

5.43 Interpretation

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

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

Appendices and definitions to this EV CPS are for all purposes an integral and binding part of the EV CPS.

5.44 No Waiver

This EV CPS shall be enforced as a whole, whilst failure by any person to enforce any provision of this EV CPS shall not be deemed a waiver of future enforcement of that or any other provision.

5.45 Notice

Certicom accepts notices related to this EV CPS by means of digitally signed messages or in paper form. Upon receipt of a valid, digitally signed acknowledgment of receipt from Certicom, the sender of the notice shall deem their communication effective. The sender must receive such acknowledgment within five (5) days, or else written notice must then be sent in paper form through a courier service that confirms delivery or via certified or registered mail, postage prepaid, return receipt requested, addressed to sales@certicom.com:

This EV CPS, related agreements and Certificate policies referenced within this document are available online at www.Certicom.com/repository.

5.46 Fees

Certicom charges Subscriber fees the EV certificate services it offers, including issuance, renewal and reissues (in accordance with the Certicom Reissue Policy stated in 5.47 of this EV CPS). Such fees are detailed on the official Certicom website.

Certicom does not charge fees for the revocation of a certificate or for a Relying Party to check the validity status of a Certicom issued certificate using Certificate Revocation Lists.

Certicom retains its right to affect changes to such fees. Certicom partners, including Resellers, Web Host Resellers, EPKI Manager Account Holders and Powered SSL Partners, will be suitably advised of price amendments as detailed in the relevant partner agreements.

5.47 Certicom Reissue Policy

Certicom offers a 30-day reissue policy. During a 30-day period (beginning when a certificate is first issued) the Subscriber may request a reissue of their certificate and incur no further fees for the reissue. If details other than just the public key require amendment, Certicom reserves the right to revalidate the application in accordance with the validation processes detailed within this EV CPS. If the reissue request does not pass the validation process, Certicom reserves the right to refuse the reissue application. Under such circumstances, the original certificate may be revoked and a refund provided to the applicant.

Certicom is not obliged to reissue a certificate after the 30-day reissue policy period has expired.

5.48 Certicom Refund Policy

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

6 General Issuance Procedure

6.1 General - Certicom

Certicom offers different certificate types to make use of SSL technology for secure online transactions. Prior to the issuance of a certificate Certicom will validate an application in accordance with this EV CPS, which may involve the request by Certicom to the applicant for relevant official documentation supporting the application.

Certicom certificates are issued to organizations.

The validity period of Certicom certificates will typically be valid for 1 year. Certicom reserves the right to, at its discretion, issues certificates that may fall outside of these set periods.

6.2 Certificates issued to Individuals and Organizations

A certificate request can be done according to the following means:

On-line: Via the Web (https). The certificate applicant submits an application via a secure online link according to a procedure provided by Certicom. Additional documentation in support of the application may be required so that Certicom verifies the identity of the applicant. The applicant submits to Certicom such additional documentation. Upon verification of identity, Certicom issues the certificate and sends a notice to the applicant. The applicant downloads and installs the certificate to its device. The applicant must notify Certicom of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of informational content to be included in the certificate.

Certicom may at its discretion, accept applications via email.

6.3 Content

Typical content of information published on a Certicom certificate may include but is not limited to the following elements of information:

6.3.1 Secure Server Certificates

- Applicant's fully qualified domain name.
- Applicant's organizational name.
- Code of applicant's country.
- Organizational unit name, street address, city, state.
- Issuing certification authority (Certicom).
- Applicant's public key.
- Certicom digital signature.
- Type of algorithm.
- Validity period of the digital certificate.
- Serial number of the digital certificate.

6.4 Time to Confirm Submitted Data

Certicom makes reasonable efforts to confirm certificate application information and issue a digital certificate within a reasonable time frame. The time frame is greatly dependent on the Subscriber providing the necessary details and / or documentation in a timely manner.

From time to time, events outside of the control of Certicom may delay the issuance process, however Certicom will make every reasonable effort to meet issuance times and to make applicants aware of any factors that may affect issuance times in a timely manner.

6.5 Issuing Procedure

The following steps describe the milestones to issue a Secure Server Certificate:

- a) The applicant fills out the online request on Certicom's web site and the applicant submits the required information: Certificate Signing Request (CSR), e-mail address, common name, organizational information, country code, verification method and billing information.
- b) The applicant accepts the on line subscriber agreement.
- c) The applicant submits the required information to Certicom.
- d) The applicant pays the certificate fees.
- e) Certicom verifies the submitted information
- f) Upon successful validation of the application information, Certicom may issue the certificate to the applicant or should the application be rejected, Certicom will alert the applicant that the application has been unsuccessful.
- g) Renewal is conducted as per the procedures outlined in this EV CPS and the official Certicom websites.
- h) Revocation is conducted as per the procedures outlined in this EV CPS.

Document Control

This document is version 1.00 of the Certicom EV CPS, created and published on 1 Dec. 2008 and signed off by the Certicom Certificate Policy Authority

Certificate Policy Authority
5520 Explorer Drive, 4th Floor
Mississauga, ON, Canada L4W 5L1

Copyright Notice

Copyright Certicom Corp. 2008. All rights reserved.

No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means (electronic, mechanical, photocopying, recording or otherwise) without prior written permission of Certicom Limited. Requests for any other permission to reproduce this Certicom document (as well as requests for copies from Certicom) must be addressed to:

Certicom Corp.
Attn: General Counsel
5520 Explorer Drive, 4th Floor
Mississauga, ON, Canada L4W 5L1

The trademarks "Certicom" is a trademark of Certicom Corp..