Comodo Extended Validation (EV) Certification Practice Statement

Comodo CA, Ltd.

Version 1.0
8 December 2006

3rd Floor, 26 Office Village, Exchange Quay, Trafford Road,
Salford, Manchester, M5 3EQ, United Kingdom
Tel: +44 (0) 161 874 7070
Fax: +44 (0) 161 877 1767
www.comodogroup.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:

Applicant:	The Applicant is an entity applying for a Certificate.
Subscriber:	The Subscriber is an entity that has been issued a certificate.
Relying Party:	The Relying Party is an entity that relies upon the information contained within the Certificate.
Subscriber Agreement:	The Subscriber Agreement is an agreement that must be read and accepted by an Applicant before applying for a Certificate. The Subscriber Agreement is specific to the Digital Certificate product type as presented during the product online order process and is available for reference in the Repository.
Relying Party Agreement:	The Relying Party Agreement is an agreement that must be read and accepted by a Relying Party prior to validating, relying on or using a Certificate and is available for reference in the Repository.
Certificate Policy:	The Certificate Policy is a statement of the issuer that corresponds to the prescribed usage of a digital certificate within an issuance context.
Repository	The Repository is a publicly available collection of databases for storing and retrieving Digital Certificates, CRLs, agreements and other information relating to Digital Certificates and which may be accessed via the Comodo website at www.comodogroup.com/repository.

Applicant:	The Private Organization 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.
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.
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

Place of Business:	The location of any facility (such as a factory, retail store, warehouse, etc) where the Applicant's business is conducted.
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).
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.
Registered Agent:	An individual or entity that is both: 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, 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 in such entity's Jurisdiction of Incorporation.
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. A 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 / 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 the CA 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.
Technical Representative:	A person authorized by the Applicant or the Applicant Representative to submit EV Certificate Requests on behalf of the Applicant.
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 Comodo Extended Validation Certification Practice Statement (EV CPS) and outlines the legal, commercial and technical principles and practices that Comodo 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 Comodo. It also defines the underlying certification processes for Subscribers and describes Comodo'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 Comodo PKI.

1.1 Comodo

Comodo is a Certification Authority (CA) that issues high quality and highly trusted Extended Validation digital certificates ("EV Certificates") to private organizations and government entities in accordance with this EV CPS. In its role as a CA, Comodo 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 Comodo PKI. In delivering its PKI services Comodo 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.

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

1.2 Comodo EV CPS

The Comodo EV CPS is a public statement of the practices of Comodo and the conditions of issuance, revocation and renewal of an EV Certificate issued under Comodo'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 Comodo 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
3rd Floor, 26 Office Village, Exchange Quay, Trafford Road
Salford, Manchester, M5 3EQ, United Kingdom
Tel: +44 (0) 161 874 7070
Fax: +44 (0) 161 877 1767
Attention: Legal Practices

Email: legal@comodogroup.com

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

1.3 EV CPS Suitability, Amendments and Publication

The Comodo 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 Comodo'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 Comodo 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 Comodo'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 Comodo 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 Certification Services by Comodo. The list of documents contained in this clause are other documents that Comodo 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 Comodo Repository can be found at www.comodogroup.com/repository.

Document Status Location	Status	Location
Comodo Certification Practice Statement	Public	Comodo Repository
Comodo EV Certification Practice Statement	Public	Comodo Repository
Digital Certificate Terms and Conditions of Use	Public	Comodo Repository
SSL Relying Party Agreement	Public	Comodo Repository
SSL Relying Party Warranty	Public	Comodo Repository
Secure Server Subscriber Agreement	Public	Comodo Repository
Secure Email Certificate Subscriber Agreement	Public	Comodo Repository
Content Verification Certificate Subscriber Agreement	Public	Comodo Repository
Comodo TF Subscriber Agreement	Public	Comodo Repository
Multi Domain Certificate (MDC) Subscriber Agreement	Public	Comodo Repository
Code Signing Certificate Subscriber Agreement	Public	Comodo Repository
TrustLogo Subscriber Agreement	Public	Comodo Repository
IdAuthority Express Credentials Subscriber Agreement	Public	Comodo Repository
Enterprise Public Key Infrastructure Manager Agreement	Confidential	Presented to partners accordingly
Enterprise Public Key Infrastructure Manager Guide	Confidential	Presented to partners accordingly
Powered SSL Partner Agreement	Confidential	Presented to partners accordingly
Powered SSL Partner Guide	Confidential	Presented to partners accordingly
Web Host Reseller Agreement	Confidential	Presented to partners accordingly
Web Host Reseller Guide	Confidential	Presented to partners accordingly
Web Host Reseller Validation Guidelines	Confidential	Presented to partners accordingly
Reseller Agreement	Confidential	Presented to partners accordingly
Reseller Guide	Confidential	Presented to partners accordingly

1.5 Liability of Comodo

For legal liability of Comodo 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 Comodo'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

Comodo conforms to the current version of the EV Guidelines published at http://www.cabforum.org. In the event of any inconsistency between this EV CPS and the EV Guidelines, the EV Guidelines shall take precedence over this EV CPS.

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 Comodo PKI Hierarchy

Comodo uses the UTN-USERFIRST-Hardware and AddTrust External CA Root for its Root CA Certificates for EV Certificates. This allows Comodo to issue highly trusted EV Certificates by inheriting the trust level associated with the UTN root certificate (named "UTN-USERFIRST-Hardware") and the AddTrust root certificate (named "AddTrust External CA Root"). The ability to issue trusted certificates from these different roots provides Comodo with additional flexibility and trust. The following high-level representation of the Comodo PKI is used to illustrate the hierarchy utilized.

1.8.1 EV Certificates

Visible on Browsers on platforms that Trust the "COMODO Certification Authority" root as follows:

COMODO Certification Authority (serial number = 4e 81 2d 8a 82 65 e0 0b 02 ee 3e 35 02 46 e5 3d, expiry = 31 December 2029 23:59:59)

↳ COMODO EV Certification Authority (serial number = 43 19 4e 93 27 c7 e4 93 cf 91 2a 31 0d 19 77 97, expiry = 31 December 2019 23:59:59)

↳ End Entity SSL (*serial number = x, expiry = 1 year from issuance*)

Cross signed and therefore visible on other IE compatible browsers as follows:

UTN-USERFIRST-Hardware (*serial number = 44 be 0c 8b 50 00 24 b4 11 d3 36 2a fe 65 0a fd, expiry = 09 July 2019 19:19:22*)

↳ COMODO Certification Authority (serial number = 48 17 4f 91 82 04 f1 c8 31 97 60 17 45 9c de ee, expiry = 31 December 2029 23:59:59)

↳ COMODO EV Certification Authority (serial number = 43 19 4e 93 27 c7 e4 93 cf 91 2a 31 0d 19 77 97, expiry = 31 December 2019 23:59:59)

↳ End Entity SSL (*serial number = x, expiry = 1 year from issuance*)

Cross signed and therefore visible on Netscape compatible browsers as follows:

AddTrust External CA Root (*serial number = 01, expiry = 30/05/2020 10:48:38*)

↳ UTN-USERFirst-Hardware (serial number = 48 4b ac f1 aa c7 d7 13 43 d1 a2 74 35 49 97 25, expiry = 30 May 2020 11:48:38)

↳ COMODO Certification Authority (serial number = 48 17 4f 91 82 04 f1 c8 31 97 60 17 45 9c de ee, expiry = 31 December 2029 23:59:59)

↳ COMODO EV Certification Authority (serial number = 43 19 4e 93 27 c7 e4 93 cf 91 2a 31 0d 19 77 97, expiry = 31 December 2019 23:59:59)

↳ End Entity SSL (*serial number = x, expiry = 1 year from issuance*)

1.9 Comodo Certification Authority

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

- Conform its operations to the EV CPS (or other CA business practices disclosure), as the same may from time to time be modified by amendments published in the Comodo 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 Comodo 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 Comodo issued certificate (for a period disclosed in this EV CPS).

1.10 Comodo Registration Authorities

Comodo may delegate the performance of all or any part of a requirement of the EV Guidelines to a registration agent (RA) or subcontractor, except for the performance of the Final Cross-Correlation and Due Diligence requirements of Section 4.2.11 of this EV CPS. Comodo has established the necessary secure infrastructure to fully manage the lifecycle of digital certificates within its PKI. Through a network of Registration Authorities (RA), Comodo also makes its certification authority services available to its subscribers. Comodo RAs:

- Accept, evaluate, approve or reject the registration of certificate applications.
- Verify the accuracy and authenticity of the information provided by the subscriber at the time of application as specified in the Comodo validation guidelines documentation.

- Use official notarized or otherwise indicated document to evaluate a subscriber application.
- Verify the accuracy and authenticity of the information provided by the subscriber at the time of reissue or renewal as specified in the Comodo validation guidelines documentation.

A Comodo RA acts locally within their own context of geographical or business partnerships on approval and authorization by Comodo in accordance with Comodo practices and procedures. Each RA, subcontractor, and Enterprise RA must comply with all applicable requirements in the EV Guidelines and this EV CPS and perform them as required of Comodo itself. Comodo will enforce compliance with such terms.

Comodo extends the use of Registration Authorities for its Web Host Reseller, Enterprise Public Key Infrastructure (EPKI) Manager and Powered SSL programs. Upon successful approval to join the respective programs the Web Host Reseller Subscriber, EPKI Manager Subscriber or Powered SSL Subscriber are permitted to act as an RA on behalf of Comodo. RAs are restricted to operating within the set validation guidelines published by Comodo to the RA upon joining the programs. EV Certificates issued through an RA contain an amended Certificate Profile within an issued certificate to represent the involvement of the RA in the issuance process to the Relying Party.

1.10.1 Reseller Partners

Comodo operates a Reseller Partner network that allows authorized partners to integrate Comodo digital certificates into their own product portfolios. Reseller Partners are responsible for referring digital certificate customers to Comodo, who maintain full control over the certificate lifecycle process, including application, issuance, renewal and revocation. Due to the nature of the Reseller program, the Reseller must authorize a pending customer order made through its Reseller account prior to Comodo instigating the validation of such certificate orders. All Reseller Partners are required to provide proof of organizational status (refer to section 4.3 for examples of documentation required) and must enter into a Comodo Reseller Partner agreement prior to being provided with Reseller Partner facilities.

1.10.2 Web Host Reseller Partners

The Web Host Reseller Partner program allows organizations providing hosting facilities to manage the certificate lifecycle on behalf of their hosted customers. Such Partners are permitted to apply for Secure Server Certificates on behalf of their hosted customers.

Through a “front-end” referred to as the “Management Area”, the Web Host Reseller Partner has access to the RA functionality including but not limited to the issuance of Secure Server Certificates. The Web Host Reseller adheres to the validation processes detailed in the validation guidelines documentation presented by Comodo as part of the agreement. The Web Host Reseller Partner is obliged to conduct validation in accordance with the validation guidelines and agrees via an online process (checking the “I have sufficiently validated this application” checkbox when applying for a Certificate) that sufficient validation has taken place prior to issuing a certificate.

All Web Host Reseller Partners are required to provide proof of organizational status (refer to section 4.3 for examples of documentation required) and must enter into a Comodo Web Host Reseller Partner agreement prior to being provided with Web Host Reseller Partner facilities.

1.10.3 EPKI Manager Account Holders

Comodo EPKI Manager is a fully outsourced enterprise public key infrastructure service that allows authorized EPKI Manager account holders to control the entire certificate lifecycle process,

including application, issuance, renewal and revocation, for certificates designated to company servers, intranets, extranets, partners, employees and hardware devices.

Through a “front-end” referred to as the “Management Area”, the EPKI Manager Account Holder has access to the RA functionality including but not limited to the issuance of Secure Server Certificates and Corporate Secure Email Certificates.

The EPKI Manager Account Holder is obliged to issue certificates only to legitimate company resources, including domain names (servers), intranets, extranets, partners, employees and hardware devices.

1.10.4 Powered SSL Partners

Comodo operates the Powered SSL service that includes an international network of approved organizations sharing the Comodo practices and policies and using a suitable brand name to issue privately labeled Secure Server Certificates to individuals and companies. Comodo controls all aspects of the certificate lifecycle, including but not limited to the validation, issuance, renewal and revocation of Powered SSL certificates, however issued certificates contain an amended certificate profile to reflect the Powered SSL status to relying parties (ultimately customers).

Through a “front-end” referred to as the “Management Area”, the Powered SSL Partner has access to the RA functionality used by a Web Host Reseller or the standard account management facilities used by a Reseller. When assuming the role of a Web Host Reseller the Powered SSL partner adheres to the validation processes detailed in the validation guidelines documentation presented by Comodo as part of the agreement. The Powered SSL Partner is obliged to conduct validation in accordance with the validation guidelines and agrees via an online process (checking the “I have sufficiently validated this application” checkbox when applying for a Certificate) that sufficient validation has taken place prior to issuing a certificate. At the same time, the Powered SSL Partner may outsource all RA functionality to Comodo.

All Powered SSL Partners are required to provide proof of organizational status (refer to section 4.3 for examples of documentation required) and must enter into a Comodo Powered SSL Partner agreement prior to being provided with Powered SSL Partner facilities.

1.10.5 Enterprise RAs

Comodo may contractually authorize the Subject of a specified valid EV Certificate to perform the RA function and authorize Comodo 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 Comodo 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 Comodo in accordance with the EV Guidelines;
(iii) Comodo 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 Comodo 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 Comodo services are individuals or companies that use PKI in relation with Comodo 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 Comodo.

1.12 Relying Parties

Relying parties may use PKI services in relation with Comodo 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 Comodo has not revoked the certificate. The CRL location is detailed within the certificate.

2 Technology

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

2.1 Comodo CA Infrastructure

The Comodo CA 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 Comodo CA certificates for signing EV Certificates are shown below in Table 2.1.1. Protection of Comodo Root signing key pairs is ensured with the use of IBM 4578 cryptographic coprocessor devices, which are certified to FIPS 140-1 Level 4, for key generation, storage and use. Comodo Root signing key pairs are 2048 bit and were generated within the IBM 4578 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 Comodo 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
2	Class 1 Public Primary CA	Self signed root certificate for Class1 intermediates	20 years	2048
3	Class 2 Public Primary CA	Self signed root certificate for Class2 intermediates (not commercially active)	20 years	2048
4	Class 3 Public Primary CA	Self signed root certificate for Class3 intermediates	20 years	2048
5	Class 4 Public Primary CA	Self signed root certificate for Class4 intermediates (not commercially active)	20 years	2048
6	Comodo Class 1 TTB Intermediate CA	Intermediate certificate for IdAuthority Website Certificates	10 years	2048
7	Comodo Class 3 TTB/Verification Engine Intermediate CA	Intermediate certificate for IdAuthority Premium, Card Payment, & Verification Engine Certificates	10 years	2048
8	Comodo Class 1 Individual Subscriber CA – Persona Not Validated	Intermediate certificate for Class 1 email certificates	10 years	2048
9	Comodo Class 3 Secure Server CA	Intermediate certificate for SSL certificates (not commercially active)	10 years	2048
10	Comodo Class 3 Software Developer CA	Intermediate certificate for code signing certificates (not commercially active)	10 years	2048
11	'Global Sign' Class 3 Security Services CA	Intermediate certificate for SSL certificates	To 28-jan-2014	2048

11	*'BeTrusted' Signed Class 3 Security Services CA (2018)*	Intermediate certificate for code signing	*To 27 August 2012*	*2048*
11	*'BeTrusted' Signed Class 3 Security Services CA (2006)*	Intermediate certificate for SSL certificates, Class 1 & 3 email certificates	*To 23-feb-2006*	*2048*
12	Comodo Certified Delivery Plug-in CA	Intermediate certificate for "Certified Delivery Plug-in" certificates (not commercially active)	10 years	2048
13	Comodo Certified Delivery Manager CA	Intermediate certificate for "Certified Delivery Manager" certificates (not commercially active)	10 years	2048
14	Comodo Certified Delivery Authority CA	Intermediate certificate for "certified delivery authority" certificates (not commercially active)	10 years	2048
15	Comodo Licensing CA	Self signed root certificate for Comodo Licence Certificates	20 years	2048
16	AAA Certificate Services	AAA Certificate Services	31-Dec-2028	2048
17	Secure Certificate Services	Secure Certificate Services	31-Dec-2028	2048
18	Trusted Certificate Services	Trusted Certificate Services	31-Dec-2028	2048
19	Custom CA	Covered by alternative CPS	11-Nov-2024	1024
20	Custom CA	Covered by alternative CPS	11-Nov-2021	2048
22	Custom CA	Covered by alternative CPS	28-May-2008	2048
22	Custom CA	Covered by alternative CPS	15-Jun-2012	2048
23	Custom CA	Covered by alternative CPS	27-Aug-2012	2048
24		Comodo Time Stamping CA	14-Jul-2014	2048
25	Custom CA	Covered by alternative CPS	14-Jul-2008	2048
25	Custom CA	Covered by alternative CPS	13-Oct-2011	2048
26		Comodo Code Signing CA	15-Jul-2004	2048
27	Custom CA	Covered by alternative CPS	30-Sep-2011	2048
28	Custom CA	Covered by alternative CPS	08-Feb-2012	2048
29	Custom CA	Covered by alternative CPS	01-Jun-2012	2048
30	UTN-USERFirst-Client Authentication and Email	UTN-USERFirst-Client Authentication and Email	09-Jul-2019	2048
31	UTN - DATACorp SGC	UTN - DATACorp SGC	24-Jun-2019	2048
32	UTN-USERFirst-Hardware	UTN-USERFirst-Hardware	09-Jul-2019	2048
33	UTN-USERFirst-Object	UTN-USERFirst-Object	09-Jul-2019	2048
34	Content Verification Authority	Content Verification Authority	31-Mar-2030	2048
35	Comodo Content Verification Services	Comodo Content Verification Services	31-Mar-2015	2048
36	Custom CA	Covered by alternative CPS	31-Mar-2015	2048
37	AddTrust Class 1 CA Root	AddTrust Class 1 CA Root	30-May-2020	2048
37	AddTrust/UTN Client CA	AddTrust/UTN Client CA	09-Jul-2019	2048
38	AddTrust External CA Root	AddTrust External CA Root	30-May-2020	2048
38	AddTrust/UTN SGC CA	AddTrust/UTN SGC CA	24-Jun-2019	2048
38	AddTrust/UTN Server CA	AddTrust/UTN Server CA	09-Jul-2019	2048
39	AddTrust Public CA Root	AddTrust Public CA Root	30-May-2020	2048
40	AddTrust Qualified CA Root	AddTrust Qualified CA Root	30-May-2020	2048
40	AddTrust/UTN Object CA	AddTrust/UTN Object CA	09-Jul-2019	2048

41	Custom CA	Covered by alternative CPS	12-May-2012	2048
41	Custom CA	Covered by alternative CPS	30 June 2012	2048
42	Custom CA	Covered by alternative CPS	12 May 2012	2048
42	Custom CA	Covered by alternative CPS	30 June 2012	2048
43	Custom CA	Covered by alternative CPS	12 May 2012	2048
43	Custom CA	Covered by alternative CPS	30 June 2012	2048
44	LiteSSL CA	LiteSSL Certificates	30 May 2020	2048
45	LiteSSL High Assurance CA	LiteSSL High Assurance Certificates	09 July 2019	2048
46	Custom CA	Covered by alternative CPS	09 July 2019	2048
47	Custom CA	Covered by alternative CPS	09 July 2019	2048
48	Custom CA	Covered by alternative CPS	09 July 2019	2048
49	Custom CA	Covered by alternative CPS	09 July 2019	2048
50	Custom CA	Covered by alternative CPS	09 July 2019	2048
51	Custom CA	Covered by alternative CPS	09 July 2019	2048
52	Custom CA	Covered by alternative CPS	24 June 2019	2048
53	Custom CA	Covered by alternative CPS	24 June 2019	2048
54	Custom CA	Covered by alternative CPS	09 July 2019	2048
55	Custom CA	Covered by alternative CPS	09 July 2019	2048
56	Custom CA	Covered by alternative CPS	09 July 2019	2048
57	Custom CA	Covered by alternative CPS	09 July 2019	2048
58	Custom CA	Covered by alternative CPS	09 July 2019	2048
59	Custom CA	Covered by alternative CPS	09 July 2019	2048
61	Custom CA	Covered by alternative CPS	30 May 2020	2048
62	Custom CA	Covered by alternative CPS	30 May 2020	2048
66	Custom CA	Covered by alternative CPS	30 May 2020	2048
67	Custom CA	Covered by alternative CPS	30 May 2020	2048
68	Custom CA	Covered by alternative CPS	30 May 2020	2048
79	PositiveSSL CA	PositiveSSL Certificates	30 May 2020	2048
80	OptimumSSL CA	OptimumSSL Certificates	30 May 2020	2048
90	COMODO Certiication Authority	Root CA for COMODO Certificates, including EV	31 December 2029	2048
91	COMODO EV Certification Authority	Intermediate CA for EV certificates	31 December 2019	2048
92	Custom CA	Covered by alternative CPS	31 December 2029	2048
93	Custom CA	Covered by alternative CPS	31 December 2019	2048

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

2.1.2 CA Root Signing Key Generation Process

Comodo securely generates and protects its own private key(s) using a trustworthy system (IBM 4758 accredited to FIPS PUB 140-1 level 4), and takes necessary precautions to prevent the compromise or unauthorized usage of it.

The Comodo CA 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 Comodo CA 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

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

The UTN USERFirst Hardware certificate is present in Explorer 5.01 and above, Netscape 8.1 and above, Opera 8.0 and above, Mozilla 1.76 and above, Konqueror 3.5.2 and above, Safari 1.2 and above, FireFox 1.02 and above, Camino and SeaMonkey and is made available through these browsers.

The AddTrust External CA Root certificate is present in Netscape 4.x and above, Opera 8.00 and above, Mozilla .06 and above, Konqueror, Safari 1.0 and above, Camino and SeaMonkey and is made available to relying parties through these browsers.

Comodo 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 Comodo 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). Comodo 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 Comodo CA physical machinery within the secure facility is protected with locked cabinets and logical access control. Comodo 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.

Comodo 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

Comodo 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 Comodo's possession or control or to which Comodo has access ("EV Data"), and (ii) the keys, software, processes, and procedures by which Comodo 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 Comodo by law.

Comodo'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 Comodo has in place to control such risks.

Based on such Risk Assessment, Comodo 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 Comodo. Such Security Plan includes administrative, organizational, technical, and physical safeguards appropriate to the size, complexity, nature, and scope of the Comodo'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.

2.2 Digital Certificate Management

Comodo 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.

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

2.3 Comodo Directories, Repository and Certificate Revocation Lists

Comodo manages and makes publicly available directories of revoked certificates using Certificate Revocation Lists (CRLs). All CRLs issued by Comodo 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. Comodo 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 the following URLs:

http://crl.comodo.net/COMODOEVCertificationAuthority.crl
http://crl.comodoca.com/COMODOEVCertificationAuthority.crl

Revoked intermediate and higher level certificates are published in the CRL accessed via:

http://crl.comodoca.com/COMODOCertificationAuthority.crl
http://crl.comodo.net/COMODOCertificationAuthority.crl

Comodo 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 Comodo Certificates

Comodo 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 Comodo products creates no claims by any third party. Upon the inclusion of a new certificate product in the Comodo hierarchy, an amended version of this EV CPS will be made public on the official Comodo 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 Comodo directories. Comodo does not perform escrow of subscriber private keys.

Pricing and subscriber fees for the EV certificates are made available on the relevant official Comodo 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 Comodo EV Certificates

Comodo 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.

Comodo EV Certificates are professional level Secure Server Certificates from Comodo 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 Comodo 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: Comodo Website, Reseller Network, Web Host Network, PoweredSSL Network, and EPKI Manager.

2.5 Extensions and Naming

2.5.1 Digital Certificate Extensions

Comodo uses the standard X.509, version 3 to construct digital certificates for use within the Comodo PKI. X.509v3 allows a CA to add certain certificate extensions to the basic certificate structure. Comodo 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 Comodo 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. Comodo does not provide key generation, escrow, recovery or backup facilities.

Upon making a certificate application, the Subscriber is solely responsible for the generation of an RSA 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, Comodo 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 Comodo 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 employed by the Applicant, or an authorized agent who has express authority to represent the Applicant who has authority on behalf of the Applicant to sign Subscriber Agreements on behalf of the Applicant.

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 an EV Certificate, Comodo must obtain from the Applicant (via a Certificate Requester authorized to act on Applicant's behalf) a properly completed and signed EV Certificate Request in a form prescribed by Comodo and that complies with the EV Guidelines. One EV Certificate Request may suffice for multiple EV Certificates to be issued to the same Applicant at the same time.

(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 Comodo to obtain from the Applicant in order to comply with the EV Guidelines and Comodo's own policies. In cases where the EV Certificate Request does not contain all necessary information about the Applicant, Comodo 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. Comodo maintains no involvement in the generation, protection or distribution of such keys.

Comodo 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 Comodo

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

Issued Subscriber Secure Server Certificates applied for through a Web Host Reseller Partner on behalf of the Subscriber are emailed to the administrator contact of the Web Host Reseller Partner account. For Web Host Reseller Partners using the "auto-apply" interface, Web Host Resellers have the added option of collecting an issued certificate from a Web Host Reseller account specific URL.

2.11 Delivery of Issued Subscriber Certificate to EPKI Manager Account Holder

Issued Subscriber Secure Server Certificates applied for through an EPKI Manager Account are emailed to the administrator contact of the account.

2.12 Comodo 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 Comodo and the Subject 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 Agency in the Subject's Jurisdiction of Incorporation. In addition, an assumed name 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 or d/b/a name exceeds 64 bytes as defined by RFC 3280, Comodo will use only the full legal organization name in the 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) Jurisdiction of Incorporation:

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 – e.g., the Jurisdiction of Incorporation for an Incorporating Agency 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 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 will be specified using the full name of the applicable jurisdiction.

Compliance with European Union Qualified Certificates Standard: In addition, Comodo 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 Agency in its Jurisdiction of Incorporation (for Private Organization Subjects only).

(5) Physical Address of Place of Business:

Certificate Fields:

Number & street (optional)	subject:streetAddress (OID 2.5.4.9)
City or town	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.

2.12.1 Key Usage extension field

In order to use and rely on a Comodo certificate a relying party must use X.509v3 compliant software. Comodo 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 used with X.509v3 compliant software. Reliance on key usage extension fields is dependent on correct software implementations of the X.509v3 standard and is outside the control of Comodo.

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 Comodo.

The EV Certificates certificate extensions are as follows:

Root CA Certificate

Root certificates generated after October 2006 are X.509 v3 compliant.

(a) basicConstraints

If the certificate is v3 and is created after October 2006, this extension appears as a critical extension in all Comodo 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

If the certificate is v3 and is created after October 2006, 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 Comodo's extended validation 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 Comodo's CRL service.

(c) authorityInformationAccess

will be present and will not be marked critical. It will contain the HTTP URL of Comodo's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1). An HTTP accessMethod
It may be included for Comodo'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. Comodo 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 Comodo's extended validation 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 Comodo'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 Comodo's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1). An HTTP accessMethod
may be included for Comodo'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, Comodo 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.

2.12.4 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 Comodo to a Subscriber contains an OID defined by Comodo in the certificate's certificatePolicies extension that: (i) indicates which CA policy statement relates to that certificate, (ii) asserts Comodo'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 Comodo 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-1*, SHA-256, SHA-384 or SHA-512
RSA	1024	2048
ECC	224, 233, 256 or 283	224, 233, 256 or 283

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	224, 233, 256 or 283	224, 233, 256 or 283

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	224, 233, 256 or 283	224, 233, 256 or 283

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

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

Comodo EV Secure Server Certificates			
Signature Algorithm	Sha1		
Issuer	CN	COMODO EV Certification Authority	
	O	COMODO CA Limited	
	L	Salford	
	S	Greater Manchester	
	C	GB	
Validity	1 year		
Subject	CN	Domain name	
	OU	Comodo EV SSL	
	OU (0 or 1 of)	*Hosted by [Web Host Reseller Subscriber Name]* *Issued through [EPKI Manager Subscriber Name]* *Provided by [Powered SSL Subscriber Name]*	
	O	Organization	
	OU	Organization Unit	
	L	Locality (City)	
	STREET	Street	
	S	State	
	PostalCode	Zip or Postal Code	
	C	Country	
	jurisdictionOfIncorporationLocalityName		Locality
	jurisdictionOfIncorporationStateOrProvinceName		State
	jurisdictionOfIncorporationCountryName		Country
	serialNumber	Registration Number	
Authority Key Identifier	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.comodoca.com		
Key Usage (NonCritical)	Digital Signature, Key Encipherment(A0)		

Extended Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)
Netscape Certificate Type	SSL Client Authentication, SSL Server Authentication(c0)
Basic Constraint	Subject Type = End Entity Path Length Constraint = None
Certificate Policies	[1] Certificate Policy: PolicyIdentifier = 1.3.6.1.4.1.6449.1.2.1.5.1 [1,1]Policy Qualifier Info: Policy Qualifier Id = CPS Qualifier: http://www.comodogroup.com/repository/EV_CPS.pdf
CRL Distribution Policies	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.comodoca.com/COMODOEVCertificationAuthority.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.comodo.net/COMODOEVCertificationAuthority.crl
Thumbprint Algorithm	*SHA1*
Thumbprint	

2.13 Comodo Certificate Revocation List Profile

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

Version	[Version 1]	
Issuer Name	[EV CA Certificate Subject]	
This Update	[Date of Issuance]	
Next Update	[Date of Issuance + 24 hours]	
Revoked Certificates	CRL Entries	
	Certificate Serial Number	[Certificate Serial Number]
	Date and Time of Revocation	[Date and Time of Revocation]

3 Organization

Comodo operates within the United Kingdom 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

Comodo 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, Comodo will provide timely notice and transfer of responsibilities to succeeding entities, maintenance of records, and remedies. Before terminating its own CA activities, Comodo 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 Comodo'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

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

Comodo 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 Comodo Registration Authority. In their role as a Comodo 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 Comodo and as stated in this EV CPS.

3.4 Records Retention Period

Comodo 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, Comodo 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 Comodo 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.

3.5 Logs for Core Functions

For audit purposes, and for compliance with the EV Guidelines, Comodo maintains 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 Comodo 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 Comodo 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) Comodo 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 Comodo, 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) Comodo 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, Comodo 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 Comodo will endeavor to minimize interruptions to its CA operations.

3.7 Availability of Revocation Data

Comodo publishes Certificate Revocation Lists (CRLs) to allow relying parties to verify a digital signature made using a Comodo issued digital certificate. Each CRL contains entries for all revoked un-expired certificates issued and is valid for 24 hours. Comodo issues a new CRL every 24 hours and includes a monotonically increasing sequence number for each CRL issued. Under special circumstances, Comodo 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. Comodo does not yet support OCSP (Online Certificate Status Protocol).

3.8 Publication of Critical Information

Comodo publishes this EV CPS, certificate terms and conditions, the relying party agreement and copies of all subscriber agreements in the official Comodo Repository. The Comodo Certificate Policy Authority maintains the Comodo 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

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

3.9.1 Types of Information deemed as Confidential

Comodo 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 Comodo.
- Contingency plans and disaster recovery plans.
- Internal tracks and records on the operations of Comodo 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 Comodo CA 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

Comodo 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 Comodo 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 Comodo 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 Comodo 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 Comodo'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 Comodo for engagement in the EV Certificate process, whether as an employee, agent, or an independent contractor, of Comodo, Comodo 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/or
(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 Comodo at the time of the adoption of the EV Guidelines whose identity and background has not previously been verified as set forth above, Comodo 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) Comodo 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) Comodo 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 Comodo's training and performance programs.

(4) Comodo ensures that its Validation Specialists qualify for each skill level required by the corresponding validation task before granting privilege to perform said task.

(5) Comodo 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

Comodo 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

Comodo has implemented a privacy policy that complies with this EV CPS. The Comodo privacy policy is published in the Comodo Repository.

3.12 Publication of information

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

- On the web: www.comodogroup.com
- By email from legal@comodogroup.com
- and by mail from:

Comodo CA Ltd.
Attention: Legal Practices,
3rd Floor, Office Village, Exchange Quay, Trafford Road
Salford, Manchester, M5 3EQ, United Kingdom
Tel: + 44(0) 161 874 7070
Fax: + 44(0) 161 877 1767
Email: legal@comodogroup.com

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

Comodo 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 (e.g., by issuance of a certificate of incorporation);
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;
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 and/or its Place of Business is not in any country where Comodo is prohibited from doing business or issuing a certificate by the laws of Comodo’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 Comodo’s jurisdiction.

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

a) The legal existence of the Government Entity is established by the law of the Jurisdiction of Incorporation;
b) The Government Entity is not in any country where Comodo is prohibited from doing business or issuing a certificate by the laws of Comodo’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 Comodo’s jurisdiction.

Until additional criteria for validation are defined by the EV Guidelines, Comodo will not issue EV Certificates to any person or any organization or entity that does not satisfy the requirements above, including but not limited to the following:

d) General partnerships
e) Unincorporated associations
f) Sole proprietorships
g) Individuals (natural persons)

Validation criteria for these organizations or entities may be addressed in the next major revision of the EV Guidelines.

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

- Generate a RSA key pair and demonstrate to Comodo 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 Comodo TF certificates)
- Make all reasonable efforts to protect the integrity the private key half of the key pair
- Submit to Comodo 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 Comodo during the enrolment process

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

4.1.1 Web Host Reseller Partner Certificate Applications

Web Host Reseller Partners may act as RAs under the practices and policies stated within this EV CPS. The RA may make the application on behalf of the applicant pursuant to the Web Host Reseller program.

Under such circumstances, the RA is responsible for all the functions on behalf of the applicant detailed in section 4.1 of this EV CPS. Such responsibilities are detailed and maintained within the Web Host Reseller agreement and guidelines.

4.1.2 EPKI Manager Account Holder Certificate Applications

EPKI Manager Account Holders act as RAs under the practices and policies stated within this EV CPS. The RA makes the application for a secure server certificate to be used by a named server, or a secure email certificate to be used by a named employee, partner or extranet user under a domain name that Comodo has validated either belongs to, or may legally be used by the EPKI Manager Account holding organization.

4.1.3 Methods of application

Generally, applicants will complete the online forms made available by Comodo 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 Comodo or its RAs.

EPKI Manager Account Holder applications are made through the EPKI Manager Management Console – a web based console hosted and supported by Comodo.

4.2 Application Validation

Prior to issuing an EV Certificate, Comodo employs controls to validate the identity of the subscriber information featured in the certificate application.

4.2. Comodo EV Certificates Validation Process

Before issuing an EV Certificate, Comodo 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 Comodo pursuant to its verification processes.

As a general rule, Comodo 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 Comodo. In all cases, however, Comodo 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, Comodo will do the following:

(1) Legal Existence: Verify that the Applicant is a legally recognized entity, in existence and validly formed (e.g., incorporated) with the Incorporating Agency in Applicant's Jurisdiction of Incorporation, and not designated on the records of the Incorporating Agency by labels such as "inactive," "invalid," "not current," or the equivalent.

(2) Organization Name: Verify that the Applicant's formal legal name as recorded with the Incorporating Agency in Applicant's Jurisdiction of Incorporation matches Applicant's name in the EV Certificate Request.

(3) Registration Number: Obtain the specific unique Registration Number assigned to Applicant by the Incorporating Agency in the Applicant's Jurisdiction of Incorporation

(4) 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.

(b) Acceptable Method of Verification. All of the foregoing will be verified directly with or obtained directly from the Incorporating Agency in the Applicant's Jurisdiction of Incorporation. 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.

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 Agency in Applicant's Jurisdiction of Incorporation, 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, Comodo 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) Comodo 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; or
(2) Comodo 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.
(3) Comodo may rely on a Verified Legal Opinion, or a 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, Comodo 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:

(1) For Applicants listed at the same Place of Business address in the current version of at least one (1) Qualified Independent Information Source, Comodo 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, Comodo 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, Comodo 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.

(B) For Applicants whose Place of Business is not in the same country as the Applicant's Jurisdiction of Incorporation, Comodo 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, Comodo 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, Comodo 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 the Applicant is listed as the Applicant's telephone number for the verified address of its Place of Business in records provided by the applicable phone company or alternatively in at least one (1) Qualified Independent 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. Comodo 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 telephone number provided is a main phone number for Applicant's Place of Business;

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 Agency, ***and*** is not listed in the current version of one (1) Qualified Independent Information Source, Comodo will verify that the Applicant has the ability to engage in business.

(b) Acceptable Methods of Verification. To verify the Applicant's operational existence, Comodo will perform one of the following:

(1) Verify the Applicant has an active current Demand Deposit Account with a Regulated Financial Institution. Comodo will receive authenticated documentation directly from a Regulated Financial Institution verifying that the Applicant has an active current Demand Deposit Account with the institution.

(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, Comodo 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.

(3) The 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 Comodo 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; or

(B) Communicating with the contact listed on the WHOIS record to confirm that the Applicant is the registered holder of the domain name and having the contact update the WHOIS records to reflect the proper domain registration;

(C) In cases where domain registration information is private, Comodo 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, Comodo 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, Comodo 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, Comodo 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, Comodo 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), Comodo 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, Comodo will obtain positive confirmation from the domain holder of internet.co.uk.

In addition, Comodo 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 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;

(B) In cases where the registered domain holder cannot be contacted, Comodo 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 Comodo 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. Comodo 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. Comodo 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, Comodo will verify the following:

(1) Name, Title and Agency. Comodo will verify the name and title of the Contract Signer and the Certificate Approver, as applicable. Comodo will also verify that the Contract Signer and the Certificate Approver are agents representing the Applicant.

(2) Authorization of Contract Signer. Comodo 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. Comodo 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 Comodo 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: Comodo 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: Comodo 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

Comodo may also verify the agency of the Certificate Approver via a certification from the Contract Signer (including in a contract between Comodo 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) Comodo can 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 Comodo 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 Comodo and the Applicant contemplate the submission of multiple future EV Certificate Requests, then, after Comodo:

(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,

Comodo 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 and 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 Comodo 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. Comodo 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.

(4) Notarization by a notary, provided that Comodo 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 Comodo may issue the requested EV Certificate, Comodo 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 of The EV Guidelines.

4.2.9 Verification of Certain Information Sources

(a) Verified Legal Opinion.

(1) Verification Requirements. Before relying on any legal opinion submitted to Comodo, Comodo will verify that such legal opinion meets the following requirements ("Verified Legal Opinion"):

(A) Status of Author. Comodo 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 any jurisdiction where the Applicant maintains an office or physical facility; or

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

(B) Basis of Opinion. Comodo 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. Comodo 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. Comodo will verify the professional status of the author of the legal opinion by directly contacting 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 clear that the Legal Practitioner is acting on behalf of the 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, Comodo 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.

(b) Verified Accountant Letter.

(1) Verification Requirements. Before relying on any accountant letter submitted to Comodo, Comodo will verify that such accountant letter meets the following requirements ("Verified Accountant Letter"):

(A) Status of Author. Comodo 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. Comodo 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. Comodo 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. Comodo will verify the professional status of the author of the accountant letter by directly contacting 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. Acceptable forms of an accountant letter is attached as Appendix D

(C) Authenticity. To confirm the authenticity of the accountant's opinion, Comodo 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.

(c) 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 Comodo from a person employed by the Applicant (other than the person who is the subject of the inquiry) that has the appropriate authority to confirm such a fact ("Confirming Person"), and who represents that he/she has confirmed such fact;

(ii) Received by Comodo 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: Comodo 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 Verified Legal Opinion, a Verified Accountant Letter, or by contacting the Applicant's Human Resources Department by phone or mail

(at the phone number or address for Applicant's Place of Business, verified in accordance with the 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.

(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 Comodo 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 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 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 Comodoll 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 Verified Legal Opinion, or a Verified Accountant Letter. The cover page must be clearly addressed to the Confirming Person.

(2) Confirmation Response: Comodo 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 Comodo by telephone, by e-mail, or by paper mail, so long as Comodo can reliably verify that it was provided by a Confirming Person in response to the Confirmation Request.

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

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

(3) the database provider identifies how frequently they update the information in their database;

(4) changes in the data that will be relied upon will be reflected in the database in no more than 12 months; and

(5) the database provider uses authoritative sources independent of the subject or multiple corroborated sources to which the data pertains.

Databases in which Comodo or its owners or affiliated companies maintain a controlling interest, or in which any registration agents (RAs) or subcontractors to whom Comodo 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. Comodo may check the accuracy of the database and ensure its data is acceptable.

(e) Qualified Government Information Source (QGIS). 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 provided they are maintained by a Government Entity, the reporting of data is required by law and false or misleading reporting is punishable with criminal or civil penalties.

4.2.10 Other Verification Requirements

(a) High Risk Status

(1) Verification Requirements. Comodo 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. Comodo 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 Comodo 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, Comodo 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. Comodo will verify that if the Applicant, the Contract Signer or Certificate Approver, or if the Applicant's Jurisdiction of Incorporation or Place of Business is on any such list:

(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 Comodo's jurisdiction(s) of operation; and

(b) Has its Jurisdiction of Incorporation *or* Place of Business in any country with which the laws of Comodo's jurisdiction prohibit doing business

Comodo 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 Place of Business is on any such list.

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

If Comodo has operations in the U.S., Comodo 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 Comodo has operations in any other country, Comodo may 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

(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, Comodo 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 and look for discrepancies or other details requiring further explanation except for EV Subscriber Certificates approved by an Enterprise RA.

(b) Comodo 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) Comodo 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 Comodo 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, Comodo may decline the EV Certificate Request and notify the Applicant accordingly.

(d) Comodo will perform the requirements of this Final Cross-Correlation and Due Diligence section 4.2.11 through employees under its control and having appropriate training, experience, and judgment in confirming organizational identification and authorization. Notwithstanding the foregoing, 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 Comodo certificates are supported by appropriate documentation to establish the identity of an applicant.

From time to time, Comodo may modify the requirements related to application information for individuals, to respond to Comodo'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
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 EV Certificate, as recorded with the Incorporating Agency in Applicant's Jurisdiction of Incorporation (for Private Organizations), or as specified in the law of Applicant's Jurisdiction of Incorporation (for Government Entities);

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 applicable;

c) Domain Name: Applicant's domain name to be included in the EV Certificate;

d) Jurisdiction of Incorporation: Applicant's Jurisdiction of Incorporation 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 Agency: The name of the Applicant's Incorporating Agency;

f) Registration Number: The unique registration number assigned to Applicant by the Incorporating Agency in Applicant's Jurisdiction of Incorporation and to be included in the EV Certificate (for Private Organization Applicants only).

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.

The following elements are critical information elements for a Comodo certificate issued to an Organization.

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 Comodo 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

Comodo 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 Comodo 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 Comodo 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 Comodo 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, Comodo will repeat the verification processes required in this EV CPS.

4.4 Validation Requirements for Certificate Applications

Upon receipt of an application for a digital certificate and based on the submitted information, Comodo 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
(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 Comodo EV certificates, the subscriber has a continuous obligation to monitor the accuracy of the submitted information and notify Comodo 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

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

4.5 Time to Confirm Submitted Data

Comodo 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 Comodo may approve an application for a digital certificate.

If the validation of a certificate application fails, Comodo rejects the certificate application. Comodo 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 Comodo 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

Comodo 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 Comodo accepts a certificate application.

4.8 Certificate Validity

Certificates are valid upon issuance by Comodo and acceptance by the subscriber. The Maximum Validity Period for an EV Certificate is twenty seven (27) months. Generally, the Comodo EV Certificate standard validity period will be 1 year, however, Comodo 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 Comodo 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

Comodo 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. Comodo may revoke a Digital Certificate it has issued in the event that Comodo has reasonable grounds to believe that any of the following events has occurred:

a) Either the Subscriber's or Comodo'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 Comodo.
e) Subscriber requests revocation of its Digital Certificate;
f) Subscriber indicates that the original Digital Certificate Request was not authorized and does not retroactively grant authorization;
g) Comodo obtains reasonable evidence that the Subscriber's Private Key (corresponding to the Public Key in the Digital Certificate) has been compromised, or that the Digital 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) Comodo receives notice or otherwise become aware that a Subscriber violates any of its material obligations under the Subscriber Agreement or this EV CPS;
i) Subcriber has used the Subscription Service contrary to law, rule or regulation or Comodo reasonably believes that the Subscriber is using the certificate, directly or indirectly, to engage in illegal or fraudulent activity;

j) Comodo receives notice or otherwise becomes aware that a court or arbitrator has revoked Subscriber's right to use the domain name listed in the Digital Certificate, or that Subscriber has failed to renew its domain name;
k) Comodo receives notice or otherwise becomes aware of a material change in the information contained in the Digital Certificate;
l) a determination, in Comodo's sole discretion, that the Digital Certificate was not issued in accordance with the terms and conditions of the EV Guidelines or Comodo's EV Policies, including Comodo's CPS;
m) Comodo determines that any of the information appearing in the Digital Certificate is not accurate;
n) Comodo ceases operations for any reason and has not arranged for another certificate authority to provide revocation support for the Digital Certificate;
o) Comodo's right to issue Digital Certificates under the EV Guidelines expires or is revoked or terminated [unless Comodo makes arrangements to continue maintaining the CRL/OCSP Repository];
p) Comodo's Private Key for Subscriber's Digital Certificate has been 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 Comodo for use with the Subscription Service;
s) such additional revocation events as Comodo publishes in its EV Policies; or
t) Comodo 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 Comodo'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 Comodo 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 Comodo employs the following procedure for authenticating a revocation request:
• The revocation request must be sent by the Administrator contact associated with the certificate application. Comodo may if necessary also request that the revocation request be made by the organizational contact and billing contact.
• Upon receipt of the revocation request Comodo will request confirmation from the known administrator out of bands contact details, either by telephone or by fax.
• Comodo 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 Comodo website every 24 hours; however, under special circumstances the CRL may be published more frequently.

4.13.3 EV Certificate Problem Reporting and Response Capability

(a) In addition to EV Certificate revocation, Comodo 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) Comodo 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 in force.

(c) Comodo 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, Comodo 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 displayed in the EV Certificate is still accurate and valid.

Renewal fees are detailed on the official Comodo 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

Comodo 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 Comodo digital certificates.

5.1 Comodo Representations

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

5.2 Information Incorporated by Reference into a Comodo Digital Certificate

Comodo 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 Comodo 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

Comodo 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 Comodo Terms & Conditions before signing-up for a certificate. To communicate information Comodo may use:

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

5.4 Publication of Certificate Revocation Data

Comodo reserves its right to publish a CRL (Certificate Revocation List) as may be indicated.

5.5 Duty to Monitor the Accuracy of Submitted Information

In all cases and for all types of Comodo certificates the subscriber has a continuous obligation to monitor the accuracy of the submitted information and notify Comodo 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 Comodo Implementation

Subscribers, relying parties and any other parties shall not interfere with, or reverse engineer the technical implementation of Comodo PKI services including the key generation process, the public web site and the Comodo repositories except as explicitly permitted by this EV CPS or

upon prior written approval of Comodo. 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 Comodo repository and any Digital Certificate or Service provided by Comodo.

5.8 Standards

Comodo 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. Comodo cannot warrant that such user software will support and enforce controls required by Comodo, while the user should seek appropriate advice.

5.9 Comodo Partnerships Limitations

Partners of the Comodo network shall not undertake any actions that might imperil, put in doubt or reduce the trust associated with the Comodo products and services. Comodo 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 Comodo repository and any Digital Certificate or Service provided by Comodo.

5.10 Comodo Limitation of Liability for a Comodo Partner

As the Comodo network includes RAs that operate under Comodo practices and procedures Comodo warrants the integrity of any certificate issued under its own root within the limits of the Comodo 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 Comodo. 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 Comodo, assumes in whole.

By means of this EV CPS, Comodo 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

Comodo 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. Comodo 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 Comodo or a Comodo RA.
c) Ensure that the public key submitted to Comodo or a Comodo RA corresponds with the private key used.
d) Ensure that the public key submitted to Comodo or a Comodo RA is the correct one.
e) Provide correct and accurate information in its communications with Comodo or a Comodo RA.
f) Alert Comodo or a Comodo RA if at any stage while the certificate is valid, any information originally submitted has changed since it had been submitted to Comodo.
g) Generate a new, secure key pair to be used in association with a certificate that it requests from Comodo or a Comodo RA.
h) Read, understand and agree with all terms and conditions in this Comodo EV CPS and associated policies published in the Comodo Repository.
i) Refrain from tampering with a Comodo certificate.
j) Use Comodo certificates for legal and authorized purposes in accordance with the suggested usages and practices in this EV CPS.
k) Cease using a Comodo certificate if any information in it becomes misleading, obsolete or invalid.
l) Cease using a Comodo 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 Comodo 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 Comodo certificate.
o) Request the revocation of a certificate in case of an occurrence that materially affects the integrity of a Comodo 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 Comodo from time to time or specified by Comodo 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 Comodo expressly agrees to obtain the same under the terms of this Agreement;
u) bind each and every Relying Party using the Subscriber's Comodo Certificate(s) to substantially the following terms: "By relying upon a Comodo digital certificate, the user agrees to be bound by the Comodo Relying Party Agreement, which is incorporated herein in its entirety, and which can be found at https://www.Comodo.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 Comodo 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 Comodo at all times, both upon requesting a Digital Certificate and thereafter as requested by Comodo in connection with the issuance of the Digital Certificate, and immediately inform Comodo if any of the Subscriber Data or information provided by the Subscriber to Comodo 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 Comodo 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 Comodo 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 Comodo 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 Comodo 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 Comodo.
h) The subscriber agrees with the terms and conditions of this EV CPS, Subscriber Agreement and other agreements and policy statements of Comodo 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 Comodo 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 Comodo 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 Comodo;
m) the Subscriber grants Comodo 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 Comodo to provide the Subscription Service; and
n) any Digital Certificate “Warranty” or other warranty described in this CPS and provided by Comodo 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 Comodo, 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 Comodo, 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 Comodo, Comodo, 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 Comodo Registration Authorities

A Comodo 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 Comodo certificates in accordance with this EV CPS.
- Perform all verification actions prescribed by the Comodo validation procedures and this EV CPS.
- Receive, verify and relay to Comodo all requests for revocation of a Comodo certificate in accordance with the Comodo 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 Comodo certificate accepts that in order to reasonably rely on a Comodo 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 Comodo digital certificate.
- Read and agree with the terms of the Comodo EV CPS and relying party agreement.
- Verify a Comodo certificate by referring to the relevant CRL and the CRLs of intermediate CA and root CA.
- Trust a Comodo certificate only if it is valid and has not been revoked or has expired.
- Rely on a Comodo 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 Comodo. 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 Comodo, and its agents and contractors.

5.24 Conditions of usage of the Comodo Repository and Web site

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

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

5.25 Accuracy of Information

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

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

5.26 Obligations of Comodo

To the extent specified in the relevant sections of the EV CPS, Comodo 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 Comodo 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 Comodo network; act promptly to issue a Comodo certificate in accordance with this Comodo EV CPS.
- Upon receipt of a request for revocation from an RA operating within the Comodo network; act promptly to revoke a Comodo certificate in accordance with this Comodo 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.

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

5.27 Fitness for a Particular Purpose

Comodo 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 Comodo 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 Comodo except as it may be stated in the relevant product description below in this EV CPS and in the Comodo insurance policy.
- The accuracy, authenticity, completeness or fitness of any information contained in Comodo 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 Comodo 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 Comodo.

5.29 Non-Verified Subscriber Information

Notwithstanding limitation warranties under the product section of this EV CPS, Comodo shall not be responsible for non-verified subscriber information submitted to Comodo, or the Comodo 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 Comodo has issued and managed the EV Certificate in compliance with the EV Guidelines and its EV CPS, Comodo 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 Comodo 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.

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

5.31 Certificate Insurance Plan

In cases where Comodo 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, Comodo 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 $1,000,000 for all claims related to that digital certificate. Except to the extent of willful misconduct, the liability of Comodo is limited to the negligent issuance of certificates.

Under Comodo'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 Comodo 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.

5.32 Financial Limitations on Certificate Usage

Comodo 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 Comodo 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 Comodo 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, dated 8 December 2006, 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 Comodo Intellectual Property Rights

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

5.36 Infringement and Other Damaging Material

Comodo subscribers represent and warrant that when submitting to Comodo 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 Comodo will provide all reasonable assistance, certificate subscribers shall defend, indemnify, and hold Comodo harmless for any loss or damage resulting from any such interference or infringement and shall be responsible for defending all actions on behalf of Comodo.

5.37 Ownership

Certificates are the property of Comodo. Comodo gives permission to reproduce and distribute certificates on a nonexclusive, royalty-free basis, provided that they are reproduced and distributed in full. Comodo 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 Comodo private key remain the property of Comodo.

5.38 Governing Law

This EV CPS is governed by, and construed in accordance with English law. 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 Comodo digital certificates or other products and services. English law applies in all Comodo commercial or contractual relationships in which this EV CPS may apply or quoted implicitly or explicitly in relation to Comodo products and services where Comodo acts as a provider, supplier, beneficiary receiver or otherwise.

5.39 Jurisdiction

Each party, including Comodo partners, subscribers and relying parties, irrevocably agrees that the courts of England and Wales have exclusive jurisdiction to hear and decide any suit, action or proceedings, and to settle any disputes, which may arise out of or in connection with this EV CPS or the provision of Comodo 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 Comodo 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 Comodo 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

Comodo 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 Comodo, 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 as follows:

Certificate Policy Authority
3rd Floor, Office Village, Exchange Quay, Trafford Road
Salford, Manchester, M5 3EQ, United Kingdom
Attention: Legal Practices

Email: legal@comodogroup.com

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

5.46 Fees

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

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

Comodo retains its right to affect changes to such fees. Comodo 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 Comodo Reissue Policy

Comodo 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, Comodo 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, Comodo reserves the right to refuse the reissue application. Under such circumstances, the original certificate may be revoked and a refund provided to the applicant.

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

5.48 Comodo Refund Policy

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

6 General Issuance Procedure

6.1 General - Comodo

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

Comodo certificates are issued to organizations.

The validity period of Comodo certificates will typically be valid for 1 year. Comodo 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 Comodo. Additional documentation in support of the application may be required so that Comodo verifies the identity of the applicant. The applicant submits to Comodo such additional documentation. Upon verification of identity, Comodo issues the certificate and sends a notice to the applicant. The applicant downloads and installs the certificate to its device. The applicant must notify Comodo 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.

Comodo may at its discretion, accept applications via email.

6.3 Content

Typical content of information published on a Comodo 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 (Comodo).
- Applicant's public key.
- Comodo digital signature.
- Type of algorithm.
- Validity period of the digital certificate.
- Serial number of the digital certificate.

6.4 Time to Confirm Submitted Data

Comodo 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 Comodo may delay the issuance process, however Comodo 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 Comodo'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 Comodo.
d) The applicant pays the certificate fees.
e) Comodo verifies the submitted information
f) Upon successful validation of the application information, Comodo may issue the certificate to the applicant or should the application be rejected, Comodo 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 Comodo websites.
h) Revocation is conducted as per the procedures outlined in this EV CPS.

Document Control

This document is version 1.0 of the Comodo EV CPS, created and published on 8 December 2006 and signed off by the Comodo Certificate Policy Authority

Certificate Policy Authority
3rd Floor, 26 Office Village, Exchange Quay, Trafford Road
Salford, Manchester, M5 3EQ, United Kingdom

URL: http://www.comodogroup.com
Email: legal@comodogroup.com

Tel: +44 (0) 161 874 7070
Fax: +44 (0) 161 877 1767

Copyright Notice