June 2009
Addendum to the Comodo EV Certification Practice Statement v.1.03

Comodo CA, Ltd.
Addendum to Comodo EV CPS v. 1.03
8 June 2009

3rd Floor, Office Village, Exchange Quay, Trafford Road
Salford, Manchester, M5 3EQ, United Kingdom
www.comodogroup.com

The purpose of this Addendum to the Comodo Certification Practice Statement (“ACPS”) is to amend version 1.03 of the EV Comodo Certification Practice Statement (“CPS”) to include the recent amendments to the EV Guidelines. All provisions of the CPS not specifically amended or added herein remain in full force and effect and where applicable shall apply to the new product offerings. Amended portions in this ACPS are included within brackets. Nothing in the CPS shall be deemed omitted, deleted or amended unless expressly stated in this ACPS or identified in brackets below. Information not located in brackets is to be included in addition to all information in the CPS. Headings from the CPS are included to identify the location of the Amended information, and are not intended to be duplicative.

Terms and Acronyms Added Through this Amendment

International Organization: An International Organization is an organization founded by a constituent document, e.g., charter, treaty, convention or similar document, signed by, or on behalf of, a minimum of two or more governments.

EV Certificate Renewal: The process whereby an Applicant who has a valid unexpired and non-revoked EV certificate makes an application, to Comodo that issued the original certificate, for a newly issued EV certificate for the same organizational and domain name prior to the expiration of the applicant's existing EV Certificate but with a new 'valid to' date beyond the expiry of the current EV certificate.

EV Certificate Re-issuance: The process whereby an Applicant who has a valid unexpired and non-revoked EV certificate makes an application, to Comodo that issued the original certificate, for a newly issued EV certificate for the same organizational and domain name prior to the expiration of the applicant's existing EV Certificate but with a matching 'valid to' date of the current EV certificate.

Signing Authority. The Signing Authority signs code on behalf of a Subscriber.

Suspect code - Code that contains malicious functionality or serious vulnerabilities, including spyware, malware and other code that installs without the user's consent and/or resists its own removal, and code that can be exploited in ways not intended by its designers to compromise the trustworthiness of the platforms on which it executes.

Timestamp Authority. The Timestamp Authority timestamps data, thereby asserting that the data existed at the specified time.

. . . .

[2.4.2 EV Code Signing Certificates *(new)*

EV Code Signing Certificates are intended to be used to verify the identity of a holder of an EV code signing certificate (Subscriber) and the integrity of its code. No particular software object is identified by an EV Code-Signing Certificate, only its Subscriber is identified. EV Code Signing Certificates focus only on assuring the identity of the Subscriber and that the signed code has not been modified from its original form. EV Code Signing Certificates are not intended to provide any other assurances, representations, or warranties. Specifically, Code Signing Certificates do **not** represent that:

i) the Subject is actively engaged in doing business;
ii) the Subject complies with any laws or regulations
iii) the Subject is trustworthy, honest, or reputable in its business dealings; or
iv) it is “safe” to install code distributed by the Subject.]

. . . .

2.6.4 EV Certificate Request Requirements *(amended)*

. . . .

[(d) **<u>EV Code Signing Certificates.</u>** Dealings between the Signing Authority and its customer are be governed by an agreement. The agreement contains an obligation and warranty:

(a) To use the EV Code Signing Certificate/EV Signature solely in compliance with the requirements set forth in the applicable EV Guidelines;
(b) To use the EV Code Signing Certificate/EV Signature solely in compliance with all applicable laws;
(c) To use the EV Code Signing Certificate/EV Signature solely for authorized company business;
(d) To use the EV Code Signing Certificate/EV Signature solely in accordance with the Subscriber Agreement;
(e) To not knowingly sign or submit software for signature that contains Suspect Code;
(f) To inform Comodo if it is discovered (by whatever means) that code submitted to Comodo for signature contains malware or a serious vulnerability, if information in a certificate is or becomes invalid; or the Subscriber discovers or suspects that a copy of its private key, or keyactivation data, is no longer under its sole control.
(g)To attest to the accuracy and currency of the information provided in certificate requests.]

2.7 Subscriber Private Key Protection and Backup *(amended)*

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. [For EV Code Signing Certificates, Comodo requires Subscriber's private key to be generated, stored and used in a crypto module that meets or exceeds the requirements of FIPS 140-2 level 2. This is accomplished by:

(1) having Comodo ship a suitable hardware crypto module, with a preinstalled key pair, in the form of a smartcard or USB device or similar;

(2) The Subscriber counter-signs certificate requests that can be verified by using a manufacturer's certificate indicating that the key is managed in a suitable hardware module ; or

(3) The Subscriber provides a suitable IT audit indicating that its operating environment achieves a level of security at least equivalent to that of FIPS 140-2 level 2.]

. . . .

2.12.1 Content of the EV Certificate as it relates to the identity of Comodo and the Subject of the EV Certificate *(amended)*

(a) <u>Subject Organization Information</u>

. . . .

(2) <u>Domain name</u>:

<u>Certificate Field</u>: subject:commonName (OID 2.5.4.3) or SubjectAlternativeName:dNSName

<u>Required/Optional</u>: Required (except for EV Code Signing Certificates)

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.

. . . .

[(6) **Romanized Names**. Romanization of a registered name is verified by Comodo using a system official recognized by the Government in the Applicant's jurisdiction of incorporation. If Comodo can not rely on the Romanization of the name from the government source, Comodo will rely on one of the following:

(a) A system recognized by the International Standards Organization (ISO),
(b) A system recognized by the United Nations or
(c) A lawyer opinion confirming the Romanization of the registered name.

In addition, for Japan, Comodo may use the Financial Services Agency to verify an English Name. When used, Comodo verifies that the English name is recorded in the audited Financial Statements filed with the Financial Services Agency. When relying on Articles of Incorporation to verify an English Name, the Articles of Incorporation must be accompanied either: by a document, signed with the original Japanese Corporate Stamp, that proves that the Articles of Incorporation are authentic and current, or by a lawyer's opinion letter. Comodo verifies the authenticity of the Corporate Stamp.

(7) **Latin Characters**. In order to include a Latin character name that is not a Romanization of the registered name in the EV certificate, Comodo verifies that the Latin character name is:

(a) Included in the Articles of Incorporation (or equivalent document) filed as part of the organization registration, or

(b) Recognized by a QGTIS in the Applicant's Jurisdiction of Incorporation as the applicant's recognized name for tax filings, or

(c) Confirmed with a QIIS to be the name associated with the registered organization, or

(d) Confirmed by a lawyer's opinion letter to be the trading name associated with the registered organization.]

. . . .

2.12.2 Key Usage extension field *(amended)*

. . . .

(e) keyUsage (optional) – EV Certificates

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

(f) keyUsage (required) – EV Code Signing Certificates

This extension must be present and must be marked critical. The bit position for digitalSignature must be set.

(g) extKeyUsage (required) – EV Code Signing Certificates

This extension must be present and must be marked critical. The value id-kp-codeSigning (for code signing) or id-kp-timeStamping (for time stamping) must be present.

. . . .

2.12.5 Minimum Cryptographic Algorithm and Key Sizes *(amended)*

. . . .

Comodo EV Secure Server Certificates

. . . .

subjectAltName	DNS Name= <Additional Domain Names *(up to 100 domains)*>

. . . .

4.1 Certificate Application Requirements *(amended)*

. . . .

[Comodo may issue EV Certificates to Non-Commercial Entities who do not qualify under any other section provided they qualify as an International Organization Entity under the EV Guidelines. Qualifying applicants (a) must be created by a country's government under a charter, treaty, convention, or equivalent instrument, (b) must not be headquartered in any location where Comodo cannot do business, (c) must not be listed on any governmental denial list or prohibited country list. Subsidiaries of qualified applicants may be issued EV Certificates in accordance with the EV Guidelines.]

. . . .

4.1.4 Certificate Request *(replaced*)

[Prior to the issuance of an EV Certificate, Comodo requires each Applicant to submit (via a Certificate Requester authorized to act on Applicant's behalf) a properly completed and signed EV Certificate Request. One EV Certificate Request may suffice for multiple EV Certificates to be issued to the same Applicant when the requests have been pre-authorized by Comodo. EV Certificate Requests which are not pre-authorized must contain a request from, or on behalf of, Applicant for the issuance of an EV certificate, or certificates, and a certification by, or on behalf of, Applicant that all of the information contained therein is true and correct.]

. . . .

4.2.1 Verification of Applicant's Legal Existence and Identity *(amended)*

. . . .

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

. . . .

[(4) Non-Commercial Entities (International Organization Entities)

a. Legal Existence. Verify that Applicant is a legally recognized International Organization Entity.

b. Entity Name. Verify that Applicant's formal legal name matches Applicant's name in the EV Certificate Request.

c. Registration Number. Comodo attempts to obtain Applicant's date of formation, or the identifier for the legislative act that created the International Organization Entity. In circumstances where this information is not available, Comodo enters appropriate language to indicate that the Subject is an International Organization Entity.]

(b) Acceptable Method of Verification.

. . . .

[(5) Non-Commercial Entities (International Organization Entities): All items listed must be verified either:

(a) With reference to the constituent document under which the International Organization was formed; or

(b) Directly with a signatory country's government where Comodo is permitted to do business. Such verification may be obtained from an appropriate government agency or from the laws of that country, or by verifying that the country's government has a mission to represent it at the International Organization; or

(c) Directly against any current list of qualified entities maintained by the CABForum

(d) If the applicant is a subsidiary, agent, or organization of the International Organization then Comodo may verify the International Organization applicant directly with the verified umbrella International Organization.]

4.2.3 Verification of Applicant’s Physical Existence

(a) Address of Applicant’s Place of Business *(replaced)*

(1) Verification Requirements. To verify Applicant's physical existence and business presence, Comodo verifies that the physical address provided by Applicant is an address where Applicant or a Parent/Subsidiary Company conducts business operations (e.g., not a mail drop or P.O. box, or 'care of' (C/O) address, such as an address for an agent of the Organization), 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 Applicant's Jurisdiction of Incorporation or Registration:

(1) For Applicants whose Place of Business is NOT the same as that indicated in the relevant Qualified Government Information Source used to verify legal existence:

(i) For Applicants listed at the same Place of Business address in the current version of either at least one Qualified Independent Information Source or a Qualified Governmental Tax Information Source, Comodo confirms that Applicant's address as listed in the EV Certificate Request is a valid business address for Applicant or a Parent/Subsidiary Company by reference to such Qualified Independent Information Sources or a Qualified Governmental Tax Information Source, and may rely on Applicant's representation that such address is its Place of Business;

(ii) For Applicants who are not listed at the same Place of Business address in the current version of either at least one Qualified Independent Information Source or a Qualified Governmental Tax Information Source, Comodo confirms that the address provided by Applicant in the EV

Certificate Request is in fact Applicant's or a Parent/Subsidiary Company's business address, by obtaining documentation of a site visit to the business address, which must be performed by a reliable individual or firm. The documentation of the site visit must:

(a) Verify that 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 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 Applicant's name, if present, and showing the street address if possible), and (ii) the interior reception area or workspace

(iii) For all Applicants, Comodo may alternatively rely on a Verified Legal Opinion or a Verified Accountant Letter that indicates the address of Applicant's or a Parent/Subsidiary Company's Place of Business and that business operations are conducted there.

(iv) For Government Entity Applicants, Comodo may rely on the address contained in the records of the QGIS in Applicant's Jurisdiction.

(2) For Applicants where the Qualified Government Information Source used in to verify legal existence contains a business address for the Applicant, Comodo may rely on the Address in the QGIS to confirm the Applicant's or a Parent/Subsidiary Company address as listed in the EV Certificate Request, and may rely on Applicant's representation that such address is its Place of Business.

(B) For Applicants whose Place of Business is not in the same country as Applicant's Jurisdiction of Incorporation or Registration, Comodo relies 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 *(replaced)*

(1) **Verification Requirements.** To further verify Applicant's physical existence and business presence, as well as to assist in confirming other verification requirements, Comodo verifies that the telephone number provided by Applicant is a main phone number for Applicant's Place of Business.

(2) **Acceptable Methods of Verification.** Comodo verifies telephone numbers by calling the telephone number and obtaining an affirmative response sufficient to enable a reasonable person to conclude that Applicant is reachable by telephone at the number dialed and either

(A) confirming that the telephone number provided by Applicant is listed as Applicant's or Parent/Subsidiary Company's telephone number for the verified address of its Place of Business in records provided by the applicable phone company, or, alternatively, in either at least one Qualified Independent Information Source or Qualified Governmental Information Source, or in a Qualified Governmental Tax Information Source; or

(B) relying on a Verified Legal Opinion or a Verified Accountant Letter to the effect that Applicant's telephone number, as provided, is a main phone number for Applicant's Place of Business.

. . . .

4.2.6 Verification of Name, Title, and Authority of Contract Signer and Certificate Approver *(amended)*

(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:

. . . .

[(6) **Prior Equivalent Authority.** Comodo may verify the signing authority of the Contract Signer, and/or the EV authority of the Certificate Approver by relying on a demonstration of Prior Equivalent Authority.

(A) Comodo may rely on this authority for confirmation or verification of the signing authority of the Contract Signer when the Contract Signer has executed a binding contract between Comodo and the Applicant with a legally valid and enforceable seal or handwritten signature and only when the contract was executed more than 90 days prior to the EV certificate application. Comodo records details of the agreement to correctly identify it and associate it with the EV application.

(B) Comodo may rely on Prior Equivalent Authority for confirmation or verification of the EV authority of the Certificate Approver when the Certificate Approver has performed one or more of the following:

(1) The Certificate Approver has served (or is serving) as an Enterprise RA for the Applicant

(2) The Certificate Approver has previously approved an SSL certificate issued by Comodo and the certificate is used on a public server operated by the Applicant. In this case, Comodo will contact the Certificate Approver by phone at a previously validated phone number or require a signed and notarized letter approving the certificate request.]

4.2.7 Verification of Signature on Subscriber Agreement and EV Certificate Requests. *(replaced)*

[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.]

. . . .

4.2.9 Verification of Certain Information Sources

. . . .

(d) Independent Confirmation From Applicant. *(amended)*

[(3) Comodo may rely on a verified Confirming Person to confirm their own contact information: email address, telephone number, and facsimile number. Comodo may rely on this verified contact information for future correspondence with the Confirming Person if:

1. The domain of the e-mail address is owned by the Applicant and is the Confirming Person's own e-mail address and not a group e-mail alias,

2. The Confirming Person's telephone/fax number is verified by Comodo to be a telephone number that is part of the organization's telephone system, and is not the personal phone number for the person.]

. . . .

4.3.2. Validity Period for Validated Data *(replaced)*

[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:

(1) Legal existence and identity - thirteen months;
(2) Assumed name - thirteen months;
(3) Address of Place of Business - thirteen months, but thereafter data may be refreshed by checking a Qualified Independent Information Source, even where a site visit was originally required;
(4) Telephone number for Place of Business - thirteen months;
(5) Bank account verification - thirteen months;
(6) Domain name - thirteen months;
(7) Identity and authority of Certificate Approver - thirteen months, unless a contract is in place between Comodo and 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.]

. . . .

4.4 Validation Requirements for Certificate Applications *(amended)*

. . . .

(2) Applicant is a registered holder or has exclusive control of the [domain name(s)] to be included in the EV Certificate;and

. . . .

4.8 Certificate Validity *(amended)*

. . . .

[EV Code Signing Certificates have a maximum validity of thirty-nine months. In the absence of time stamping, their code signatures will no longer be valid once their certificate has expired. Timestamp Authorities and Signing Authorities may obtain an EV Timestamp Certificate or EV Code-Signing Certificate (respectively) with a validity period not exceeding one hundred and twenty three months.

Ordinarily, a code signature created by a Subscriber may be considered valid for a period of up to thirty-nine months. However, a code signature may be treated as valid for a period of up to one hundred and twenty three months by means of the “timestamp” method or the “Signing Authority” method.

(a) Timestamp method. In this method, the Subscriber signs the code, appends its EV Code-Signing Certificate (whose expiration time is less than thirty-nine months in the future) and submits it to an EV Timestamp Authority to be timestamped. The resulting package can be considered valid up to the expiration time of the timestamp certificate (which may be up to one hundred and twenty three months in the future).

(b) Signing Authority method. In this method, the Subscriber submits the code, or a digest of the code, to an EV Signing Authority for signature. The resulting signature is valid up to the expiration time of the Signing Authority certificate (which may be up to one hundred and twenty three months in the future).]

. . . .

4.13 Certificate Revocation and Compromise *(amended)*

. . . .

j) Comodo receives notice or otherwise becomes aware that a court or arbitrator has revoked Subscriber’s right to use [a domain name] listed in the EV Certificate, or that Subscriber has failed to renew [a domain name];

. . . .

r) install the Digital Certificate only on the server accessible at the [domain name(s)] 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;

. . . .

[4.13.4 EV Code Signing Certificate Revocation and Compromise *(new)*

(a) Revocation reasons*.* Subscribers are expected to not intentionally include Suspect Code in their signed software. Intentionally signing Suspect Code is a violation of the terms of the Subscriber Agreement, and will likely result in revocation of an EV code signing certificate. Comodo will respond to all plausible notices that a signed software object containing Suspect Code verifies with a certificate that it has issued by setting the revocation status of that certificate to ‘revoked’. Comodo’s gives notice that it will revoke certificates issued to Subscribers who use them to digitally sign Suspect Code.

(b) Revocation status information*.* Comodo provides accurate and up-to-date revocation status information for at least one year following the expiration of the associated certificate.

(c) Revocation consequences. A certificate may have a one-to-one relationship with the software object that it verifies. In such cases, revocation of the certificate only invalidates the signature on the code that is suspect. If, on the other hand, a certificate has a one-to-many relationship with the software objects that it verifies, then revocation of the certificate invalidates the signatures on all those software objects, some of which may be perfectly sound.]

[4.14 Renewal *(replaced)*

(a) Validation for Renewal Requests. In conjunction with the EV Certificate Renewal process, Comodo performs all authentication and verification tasks required to ensure that the renewal request is properly authorized by Applicant and that the information in the EV Certificate is still accurate and valid.

(b) Validation of Reissuance Requests. Comodo may rely on previously verified information to issue a replacement certificate where:

(1) The expiration date of the replacement certificate is the same as the expiration date of the currently valid EV certificate being replaced, and
(2) The certificate subject of the Replacement Certificate is the same as the certificate subject contained in the currently valid EV certificate.

(c) Renewal Exceptions. Comodo when performing the authentication and verification requirements for a renewal may rely on :

(1) information in an EV Certificate previously issued by Comodo. Reuse of information is limited to authentication and verification of:
  (a) A Principal Individual of a Business Entity if the Principal Individual is the same as the Principal Individual verified by Comodo in connection with the previously issued EV Certificate,
  (b) Applicant's Place of Business
  (c) The verification of telephone number of Applicant's Place of Business (however, Comodo still performs the verification required by Section 16(b)(2)(a) of the EV Guidelines),
  (d) Applicant's Operational Existence
  (e) The name, title, and authority of the Contract Signer, Certificate Approver, and Certificate Requester, except where a contract is in place between Comodo and Applicant that specifies a specific term for the authority of the Contract Signer, and/or the Certificate Approver, and/or Certificate Requester in which case, the term specified in such contract will control,
  (f) The prior verification of the email address used by Comodo for independent confirmation from applicant under Section 22(d)(1)(B)(ii) of the EV Guidelines.
(2) a prior Verified Legal/Accountant Opinion that established:
  (a) Applicant's exclusive right to use the specified domain name, except Comodo verifies that either the WHOIS record still shows the same registrant as when Comodo received the prior Verified Legal Opinion, or the Applicant establishes domain control via a practical demonstration.
  (b) Verification that Applicant is aware that it has exclusive control of the domain name.

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.]

. . . .

6.3.1 Secure Server Certificates *(amended)*

- Applicant’s fully qualified [domain name(s)]

. . . .

Document Control
This document is the Addendum to Comodo CPS Version 1.03, created on 8 June 2009 and signed off by the Comodo Certificate Policy Authority.

Comodo CA Limited
3rd Floor, 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