PositiveSSL Addendum to the Comodo Certification Practice Statement

Comodo CA Limited
PositiveSSL Addendum to Comodo CPS,
Version 2.4 Amendments
23 June 2006

New Court, Regents Place, Regent Road,
Manchester M5 4HB United Kingdom
Tel: +44 (0) 161 874 7070
Fax: +44 (0) 161 877 1767
www.comodogroup.com

Beginning June 23, 2006 Comodo CA Ltd. ("Comodo") will offer a domain only SSL certificate designed for use in non e-commerce applications. The name of the product line is PositiveSSL. The purpose of this Addendum to the Comodo Certification Practice Statement ("ACPS") is to amend version 2.4 of the Comodo Certification Practice Statement ("CPS") to include the PositiveSSL product offering. All provisions of the CPS not specifically amended or added herein remain in full force and effect and where applicable shall apply to PositiveSSL. 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.

. . . .

1.7 Digital Certificate Policy Overview

. . . .

Applicant	Certificate Type	Channels Available	Validation Levels[1]	Suggested Usage
Individual or Company	**Secure Server Certificate**: *PositiveSSL*	- PositiveSSL Website - Reseller Network - Web Host Network - Powered SSL Network - EPKI Manager	Confirmation of right to use the domain name used in the application.	Establishes SSL/TLS session between the server housing the Secure Server Certificate and a client / customer / website visitor. The protocol is designed to authenticate a server to a client and provide confidentiality of data passed through the SSL/TLS session.
Individual or Company	**Secure Server Certificate:** *PositiveSSL Wildcard*	- PositiveSSL Website - Reseller Network - Web Host Network - Powered SSL Network - EPKI Manager	Confirmation of right to use the domain name used in the application.	Establishes SSL/TLS session between the server housing the Secure Server Certificate and a client / customer / website visitor. The protocol is designed to authenticate a server to a client and provide confidentiality of data passed through the SSL/TLS session.

1.8 Comodo PKI Hierarchy

Comodo uses the BeTrusted (www.betrusted.com - AICPA/CICA WebTrust Program for Certification Authorities approved security provider), UTN-USERFIRST-Hardware and AddTrust External CA Roots for its Root CA Certificates. The following high-level representation of the Comodo PKI is used to illustrate the hierarchy utilized.

1.8.3 PositiveSSL Certificates

UTN-USERFIRST-Hardware

↳ AddTrust External CA Root

↳ PositiveSSL CA

↳ End Entity SSL

1.12 Relying Parties

[Relying parties use PKI services in relation with various Comodo 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. Because PositiveSSL and PositiveSSL Wildcard certificates are not intended to be used in an e-commerce transaction or environment, parties who rely on a PositiveSSL or PositiveSSL Wildcard certificate do not qualify as a relying party.]

. . . .

2 Technology

. . . .

2.1.1 Root CA Signing Key Protection & Recovery

. . . .

[BeTrusted ensures the protection of its CA Root signing key pair in accordance with its AICPA/CICA WebTrust program compliant infrastructure and CPS. Details of BeTrusted's WebTrust compliancy are available at its official website (www.betrusted.com).

In a similar manner Comodo protects its CA Root key pairs in accordance with its AICPA/CICA WebTrust program compliant infrastructure and CPS. Details of Comodo's WebTrust compliancy are available at its official website (www.comodogroup.com).]

. . . .

2.1.5 CA Root Public Key Delivery to Subscribers

[Comodo makes all its CA Root Certificates available in online repositories at www.comodogroup.com/repository. The GTE CyberTrust Root certificate is present in Internet Explorer 5.00 and above, Netscape 4.x and above and Opera 5.0 and above and is made available to relying parties through these and other browsers. 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 5.0 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.]

. . . .

2.2 Digital Certificate Management

. . . .

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

• Verification of the domain of an applicant of a certificate.

. . . .

2.4 Types of Comodo Certificates

. . . .

2.4.1 Comodo Secure Server Certificates

[Comodo makes available Secure Server Certificates that in combination with a Secure Socket Layer (SSL) web server attest the public server's identity and/or domain, allowing full authentication and enabling secure communication with customers and business partners. Comodo Secure Server Certificates are offered in six InstantSSL variants; InstantSSL, InstantSSL Pro,PremiumSSL, PremiumSSL Wildcard, Intranet SSL, Trial SSL; two PositiveSSL variants: PositiveSSL and PositiveSSL Wildcard; and four Enterprise SSL variants; Elite SSL, Gold SSL, Platinum SSL and Platinum SSL Wildcard. Pricing for the certificates are made available on the relevant official Comodo websites.]

. . . .

k) PositiveSSL Certificate

PositiveSSL Certificates are low assurance level Secure Server Certificates from Comodo ideal for mail servers and server to server communications. They are not intended to be used for websites conducting e-commerce or transferring data of value. Only the InstantSSL, InstantSSL Pro, PremiumSSL, PremiumSSL Wildcard, Elite SSL, Gold SSL, Platinum SSL and Platinum SSL Wildcard certificates are intended for an e-commerce environment.

As PositiveSSL Certificates are not used commercially, the relying party does not require Comodo, the trusted third party, to provide a warranty against mis-issuance.

In accordance with section 4.2.7 (Validation Practices) of this CPS, PositiveSSL Certificates utilize third party domain name registrars and directories to assist with application validation in order to provide increased speed of issuance. Where possible, the third parties will be used to confirm the domain control of a certificate applicant. If the directory cannot be used to sufficiently validate a certificate applicant’s domain control, further validation processes may be used. These may include an out of bands validation of the applicant’s submitted information.

Due to the increased validation speed and the nature of how PositiveSSL intends PositiveSSL certificates to be used, the certificates carry no warranty..

Subscriber fees for a PositiveSSL Certificate are available from the official PositiveSSL website.

l) PositiveSSL Wildcard Certificate

PositiveSSL Wildcard certificates are low assurance Secure Server Certificates from Comodo ideal for mail servers and server to server communications. They are not intended to be used for websites conducting e-commerce or transferring data of value. Only the InstantSSL, InstantSSL Pro, PremiumSSL, PremiumSSL Wildcard, Intranet SSL, Elite SSL, Gold SSL, Platinum SSL and Platinum SSL Wildcard certificates are intended for an e-commerce environment.

As PositiveSSL Wildcard Certificates are not used commercially, the relying party does not require Comodo, the trusted third party, to provide a warranty against mis-issuance.

In accordance with section 4.2.7 (Validation Practices) of this CPS, PositiveSSL Wildcard Certificates utilize third party domain name registrars and directories to assist with application validation in order to provide increased speed of issuance. Where possible, the third parties will be used to confirm the domain control of a certificate applicant. If the directory cannot be used to sufficiently validate a certificate applicant's domain control, further validation processes may be used. These may include an out of bands validation of the applicant's submitted information.

Due to the increased validation speed and the nature of how PositiveSSL intends PositiveSSL Wildcard Certificates to be used, the certificates carry no warranty.

Subscriber fees for a PositiveSSL Wildcard Certificate are available from the official PositiveSSL website.

. . . .

2.9 Delivery of Issued Subscriber Certificate to Subscriber

. . . .

2.9.5 Secure Server Certificate: PositiveSSL eCommerce and PositiveSSL eCommerce Wildcard

PositiveSSL and PositiveSSL Wildcard certificates are delivered via email to the Subscriber using the administrator contact email address provided during the application process.

. . . .

2.12 Comodo Certificates Profile

. . . .

2.12.4 Certificate Policy (CP)

. . . .

PositiveSSL Secure Server Certificate – PositiveSSL / PositiveSSL Wildcard		
Signature Algorithm	Sha1	
Issuer	CN	Comodo CA
	OU	(c) Comodo CA, Ltd.
	OU	Terms and Conditions of use: http://www.comodogroup.com/repository
	OU	
	O	Comodo CA, Ltd.
	C	US
Validity	1 Year / 2 Year / 3 Year / 4 Year / 5 Year / 6 Year / 7 Year / 8 Year / 9 Year / 10 Year	
Subject	CN	<domain name>
	OU	Domain Control Validated[1]

Authority Key Identifier	
Key Usage (NonCritical)	Digital Signature , Key Encipherment(A0)
Netscape Certificate Type	SSL Server Authentication(40)
Basic Constraint	
Certificate Policies	
CRL Distribution Policies	
Subject Alternate Name	
NetscapeSSLServerName	
Thumbprint Algorithm	
Thumbprint	

. . . .

4 Practices and Procedures

. . . .

4.1 Certificate Application Requirements

[All Certificate applicants must complete the enrolment process, which may include:]

. . . .

4.2 Application Validation

. . . .

4.2.1 Secure Server Certificate Application Two Step Validation Process

[Comodo utilizes a two-step validation process prior to the issuance of a Secure Server Certificate (other than PositiveSSL type certificates) which are validated according to the process identified in 4.2.7.]

. . . .

4.2.7 PositiveSSL and PositiveSSL Wildcard Secure Server Certificates

To validate PositiveSSL and PositiveSSL Wildcard Secure Server Certificates, Comodo checks that the Subscriber has control over the Domain name at the time the Subscriber submitted its enrollment certificates by reviewing the application information provided by the applicant (as per Section 4.3 of this CPS) and:

> Reviewing domain name ownership records publicly available through Internet approved global domain registrars; and the use of generic e-mails which ordinarily are only available to person(s) controlling the domain name administration, for example, webmaster@ . . ., postmaster@ . . ., admin@; or
>
> Requesting documentation that verifies control of the domain.

. . . .

4.8 Certificate Validity

. . . .

PositiveSSL and PositiveSSL Wildcard certificates are valid upon issuance by Comodo and acceptance by the Subscriber. Generally, the certificate validity period will be from 1 to 10 years, however Comodo reserves the right to offer validity periods outside of this standard validity period.

. . . .

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 CPS and named as Object Identifiers in the certificate profile.
- The digital certificate applied for is appropriate for the application it is used in, i.e. relying party's should not rely on PositiveSSL or PositiveSSL Wildcard certificates for e-commerce uses.]

. . . .

5 Legal Conditions of Issuance

. . . .

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 certificates issued under its own root within the limits of the Comodo insurance policy and in accordance with this CPS.]

. . . .

5.31 Certificate Insurance Plan

. . . .

5.31.11 PositiveSSL Certificate

There is no liability of Comodo to applicants, subscribers and relying parties of PositiveSSL Certificates.

5.31.12 PositiveSSL Wildcard Certificate

There is no liability of Comodo to applicants, subscribers and relying parties of PositiveSSL Certificates.

. . . .

5.46 Fees

[Comodo charges Subscriber fees for some of the certificate services it offers, including issuance, renewal and reissues (in accordance with the Comodo Reissue Policy stated in 5.47 of this CPS). Such fees are detailed on the official Comodo websites (www.comodogroup.com, www.instantssl.com, www.enterprisessl.com and www.positivessl.com).]

. . . .

Document Control

This document is the PositiveSSL Addendum to Comodo CPS Version 2.4, first published 23 May 2006 and effective on 23 June 2006 and signed off by the Comodo Certificate Policy Authority.

Comodo CA Limited
New Court, Regents Place, Regent Road,
Manchester M5 4HB, 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