Comodo Certification Practice Statement

Table of Contents

Revision History

Version	Author	Description of Change	Date Approved
4.0	Legal	1. Integrate CPS v. 3.0 Addendums 2. Add Revision History Section 3. Format 4. Add Table of Contents Section 5. Add CA/Browser Requirements	1 July 2012

Terms and Acronyms Used in the 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 at www.comodogroup.com/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 at www.comodogroup.com/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.

1 General

This document is the Comodo Certification Practice Statement (CPS) and outlines the legal, commercial and technical principles and practices that Comodo employ in providing certification services that include, but are not limited to, approving, issuing, using and managing of Digital Certificates and in maintaining a X.509 Certificate based public key infrastructure (PKIX) 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 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 digital certificates to entities including private and public companies and individuals in accordance with this 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 and the relevant law on electronic signatures and all other relevant legislation and regulation.

Comodo extends, 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.

1.1.1 CA/Browser Forum Requirements

Comodo conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org. In the event CA / Browser Forum Baseline Requirements, v. 1.0 8 of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

1.2 Comodo CPS

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

The Comodo Certificate Policy Authority maintains this 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, 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 CPS, related agreements and Certificate policies referenced within this document are available online at www.comodogroup.com/repository.

1.3 CPS Suitability, Amendments and Publication

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

Upon the Certificate Policy Authority accepting such changes deemed by the CA's Policy Authority to have significant impact on the users of this CPS an updated edition of the CPS will be published at the Comodo repository (available at www.comodogroup.com/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 the CA'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 CPS and without changing the version number of this CPS.

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

1.4 Other Practice Statements & Agreements

The CPS is only one of a set of documents relevant to the provision of Certification Services by Comodo and that the list of documents contained in this clause are other documents that this CPS will from time to time mention, although this is not an exhaustive list. 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
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	Public	Comodo Repository

Agreement		
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	Public	http://www.comodopartners.com/partner/partnerdoc.html
Web Host Reseller Validation Guidelines	Public	http://www.comodopartners.com/partner/partnerdoc.html
Reseller Agreement	Confidential	Presented to partners accordingly
Reseller Guide	Confidential	Presented to partners accordingly
Comodo Dual Use Certificate Subscriber Agreement	Public	Comodo Repository

1.5 Liability of Comodo

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

1.6 Compliance with applicable standards

The practices specified in this 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, and other industry standards related to the operation of CAs.

A regular audit is performed by an independent external auditor to assess Comodo's compliancy 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

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.

1.8 Comodo PKI Hierarchy

Comodo uses the Entrust (www.entrust.com - AICPA/CICA WebTrust Program for Certification Authorities approved security provider), BeTrusted (www.betrusted.com - AICPA/CICA WebTrust

Program for Certification Authorities approved security provider), UTN-USERFIRST-Hardware and AddTrust External CA Root for its Root CA Certificates. This allows Comodo to issue highly trusted digital certificates by inheriting the trust level associated with the Entrust root certificate (named "EntrustRoot"), BeTrusted root certificate (named "GTE CyberTrust Root"), 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 three 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 Trial and Short Term Certificates

UTN/AddTrust certificates – InstantSSL and EnterpriseSSL CA

Visible on IE compatible browsers:

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)

> ↪ End Entity SSL/End Entity Secure Email (serial number = x, expiry = 1 month or up to 10 year(s) 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)

> ↪ End Entity SSL/End Entity Secure Email (serial number = x, expiry = 1 month or up to 10 year(s) from issuance)

1.8.2 1-5 year certificates (InstantSSL and EnterpriseSSL)

Entrust Certificates

Entrust.net Secure Server Certification Authority (serial number = 37 4a d2 43, expiry = 25 MAY 2019)

> ↪ Entrust Comodo Intermediate - TBA (serial number = TBA, expiry = TBA)
> > ↪ End Entity SSL/End Entity Secure Email (serial number = x, expiry = 1, 2 or 3 years from issuance)

GTE Certificates

GTE CyberTrust Root (serial number = 01A5, expiry = 14 August 2018)

> ↪ Comodo Class 3 Security Services CA (serial number = 0200 029A, expiry = 27 August 2012)
> > ↪ End Entity SSL/End Entity Secure Email (serial number = x, expiry = 1, 2 or 3 years from issuance)

UTN/AddTrust certificates – InstantSSL and EnterpriseSSL CA

Visible on 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)

↳ End Entity SSL/End Entity Secure Email (serial number = x, expiry = 1 month or up to 10 year(s) 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)

↳ End Entity SSL/End Entity Secure Email (serial number = x, expiry = 1 month or up to 10 year(s) from issuance)

<u>Comodo Certification Authority Certificates</u>

Visible on IE compatible browsers 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 Dec ember 2029 23:59:59

↳ COMODO High Assurance Secure Server CA (serial number = 08 0a 57 82 2c c6f5 e1 4f 19 b7 09 55 c8 03 42, expiry = 31 December 2029 23:59:59)

↳ End Entity SSL Certificate (serial number = x, expiry = 1 month or up to 5 year(s) 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)

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

↳ COMODO High Assurance Secure Server CA (serial number = 08 0a 57 82 2c c6f5 e1 4f 19 b7 09 55 c8 03 42, expiry = 31 December 2029 23:59:59)

↳ End Entity SSL Certificate (serial number = x, expiry = 1 month or up to 5 year(s) from issuance)

1.8.3 PositiveSSL Certificates

Visible on IE compatible browsers as follows:

AddTrust External CA Root (serial number = 01, expiry = 30 May 2020)

↳ PositiveSSL CA 2 (serial number = 07 6f 12 46 81 45 9c 28 d5 48 d6 97 c4 0e 00 1b, expiry = 30-May-2020)

↳ End Entity SSL/End Entity Secure Email (serial number = x, expiry = 1 month or up to 10 year(s) from issuance)

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

UTN – DATACorp SGC (serial number = 44 be 0c 8b 50 00 21 b4 11 d3 2a 68 06 a9 ad 69, expiry = 24 June 2019)

↳ AddTrust External CA Root (serial number = 7e d1 a9 ab be e3 6f 46 cd 6b 4e 29 34 90 56 f3, expiry = 24 June 2019)

↳ PositiveSSL CA 2 (serial number = 07 6f 12 46 81 45 9c 28 d5 48 d6 97 c4 0e 00 1b,, expiry = 30-May-2020)

↳ End Entity SSL/End Entity Secure Email (serial number = x, expiry = 1 month or up to 63 month(s) from issuance)

1.8.4 OptimumSSL Certificates

Visible on 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)

↳ OptimumSSL CA (serial number = TBA, expiry = TBA)

↳ End Entity SSL (serial number = x, expiry = 1 month or up to 10 year(s) 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)

↳ OptimumSSL CA (serial number = TBA, expiry = TBA)

↳ End Entity SSL (serial number = x, expiry = 1 month or up to 10 year(s) from issuance)

1.8.5 Comodo SGC / Platinum SGC / Multi-Domain certificates

UTN Certificates

Visible on IE compatible browsers as follows:

UTN - DATACorp SGC (serial number = 44 be 0c 8b 50 00 21 b4 11 d3 2a 68 06 a9 ad 69, expiry = 24 June 2019 20:06:40)

↳ End Entity SSL (serial number = x, expiry = 1 month or up to 10 year(s) 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 - DATACorp SGC (serial number = 53 7b 76 56 4f 29 7f 14 dc 69 43 e9 22 ad 2c 79, expiry = 30 May 2020 11:48:38)

↳ End Entity SSL (serial number = x, expiry = 1 month or up to 10 year(s) from issuance)

Comodo Certification Authority Certificates

Visible on IE compatible browsers as follows:

UTN - DATACorp SGC (serial number = 44 be 0c 8b 50 00 21 b4 11 d3 2a 68 06 a9 ad 69, expiry = 24 June 2019 20:06:40)

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

    ↳ COMODO High Assurance Secure Server CA (serial number = 08 0a 57 82 2c c6f5 e1 4f 19 b7 09 55 c8 03 42, expiry = 31 December 2029 23:59:59)

        ↳ End Entity SSL Certificate (serial number = x, expiry = 1 month or up to 5 year(s) 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 - DATACorp SGC (serial number = 53 7b 76 56 4f 29 7f 14 dc 69 43 e9 22 ad 2c 79, expiry = 30 May 2020 11:48:38)

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

        ↳ COMODO High Assurance Secure Server CA (serial number = 08 0a 57 82 2c c6f5 e1 4f 19 b7 09 55 c8 03 42, expiry = 31 December 2029 23:59:59)

            ↳ End Entity SSL Certificate (serial number = x, expiry = 1 month or up to 5 year(s) from issuance)

1.8.6 Legacy certificates (Premium and Platinum)

Entrust Certificates

Entrust.net Secure Server Certification Authority (*serial number = 37 4a d2 43, expiry = 25 MAY 2019*)

    ↳ Entrust Comodo Intermediate - TBA (*serial number = TBA, expiry = TBA*)

        ↳ End Entity SSL/End Entity Secure Email (*serial number = x, expiry = 1-10 years from issuance*)

GTE Certificates

GTE CyberTrust Root (*serial number = 01A5, expiry = 14 August 2018*)

↳ Comodo Class 3 Security Services CA (*serial number = 0200 029A, expiry = 27 August 2012)*

    ↳ End Entity SSL/End Entity Secure Email (*serial number = x, expiry = 1-5 years from issuance*)

1.8.7 Code Signing / Time Stamping certificates

UTN-USERFirst-Object (serial number = 44 be 0c 8b 50 00 24 b4 11 d3 36 2d e0 b3 5f 1b, expiry = 09 July 2019 19:40:36)

↳ End Entity (serial number = x, expiry = 1 month or up to 10 year(s) from issuance)

1.8.8 Content Verification Certificates

Content Verification Authority (serial number = 00 e1 c4 70 13 1e e0 70 f1 c0 fe 0d fc 1e 7e d6 7b, expiry = 01 April 2030 00:59:59)

↳ Comodo Content Verification Services (serial number = 00 e2 ed f2 a4 f6 ef fd ff b6 87 39 fe b4 41 50 29, expiry = 01 Apr 2015 00:59:59)

   ↳ End Entity (serial number = x, expiry = 1 month or up to 10 year(s) from issuance)

1.8.9 Secure Email and Custom Client certificates

Visible on IE compatible browsers as follows:

UTN-USERFirst-Client Authentication and Email (serial number = 44 be 0c 8b 50 00 24 b4 11 d3 36 25 25 67 c9 89, expiry = 09 July 2019 18:36:58)

↳ End Entity (serial number = x, expiry = 1 month or up to 10 year(s) 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-Client Authentication and Email (serial number = 27 f4 ea 11 f4 7a 86 c4 6e 9d bb 6e a9 17 07 07, expiry = 30 May 2020 11:48:38)

   ↳ End Entity (serial number = x, expiry = 1 month or up to 10 year(s) from issuance)

1.8.10 Comodo TF certificates

UTN-USERFirst-Client Authentication and Email (serial number = 44 be 0c 8b 50 00 24 b4 11 d3 36 25 25 67 c9 89, expiry = 09 July 2019 18:36:58)

↳ End Entity (serial number = x, expiry = 1 month or up to 10 year(s) from issuance)

1.8.11 Corporate Secure email

Entrust Certificates

Entrust.net Secure Server Certification Authority (serial number = 37 4a d2 43, expiry = 25 MAY 2019)

   ↳ Entrust Comodo Intermediate - TBA (serial number = TBA, expiry = TBA)

      ↳ End Entity (serial number = x, expiry = 1, 2 or 3 years from issuance)

GTE Certificates

GTE CyberTrust Root (serial number = 01A5, expiry = 14 August 2018)

   ↳ Comodo Class 3 Security Services CA (serial number = 0200 029A, expiry = 27 August 2012)

      ↳ End Entity (serial number = x, expiry = 1, 2 or 3 years from issuance)

UTN/AddTrust Certificates

Visible on IE compatible browsers as follows:

UTN-USERFirst-Client Authentication and Email (serial number = 44 be 0c 8b 50 00 24 b4 11 d3 36 25 25 67 c9 89, expiry = 09 July 2019 18:36:58)

    ↳ End Entity (serial number = x, expiry = 1 month or up to 10 year(s) 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-Client Authentication and Email (serial number = 27 f4 ea 11 f4 7a 86 c4 6e 9d bb 6e a9 17 07 07, expiry = 30 May 2020 11:48:38)

        ↳ End Entity (serial number = x, expiry = 1 month or up to 10 year(s) from issuance)

1.8.12 Essential SSL Certificates

Visible on 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)

  ↳ Essential SSL CA (serial number = TBA, expiry = TBA)

    ↳ End Entity SSL/End Entity Secure Email (serial number = x, expiry = 1 month or up to 3 year(s) 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)

    ↳ Essential SSL CA (serial number = TBA, expiry = TBA)

      ↳ End Entity SSL/End Entity Secure Email (serial number = x, expiry = 1 month or up to 3 year(s) from issuance)

1.8.13 Intel Pro SSL Certificates

Visible on IE compatible browsers as follows:

Entrust.net Secure Server CA (serial number = 42 86 f2 3d, expiry = 19 October 2012)

  ↳ AAA Certificate Services (serial number = 01 d1 eb 23 a4 6d 17 d6 8f d9 25 64 c2 f1 f1 60 17 64 d8 e3 49, expiry = 01 January 2029)

    ↳ End Entity SSL (serial number = x, expiry = 1 month or up to 5 year(s) from issuance)

1.8.14 IGTF Certificates

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)

↳ End Entity SSL/End Entity Secure Email (serial number = x, expiry = 1-13 months 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)

    ↳ End Entity SSL/End Entity Secure Email (serial number = x, expiry = 1-131 months from issuance)

1.8.15 ComodoSSL Certificates

Visible on current browsers (including IE, FireFox, Chrome, Opera) as follows:

AddTrust External CA Root (serial number = 01, expiry = 30 May 2020 10:48:38 UTC)

↳ COMODO SSL CA (serial number = 6e ba f0 8f 79 83 fa 9d e1 b2 6f 96 fc 6e 98 bf, expiry = 30 May 2020 10:48:38 UTC)

    ↳ End Entity SSL (serial number = x, expiry = from 1 month up to 60 months from issuance)

Cross-signed and therefore visible on some other browsers and platforms as follows:

UTN - DATACorp SGC (serial number = 44 be 0c 8b 50 00 21 b4 11 d3 2a 68 06 a9 ad 69, expiry = 24 June 2019 19:06:30 UTC)

↳ AddTrust External CA Root (serial number = 7e d1 a9 ab be e3 6f 46 cd 6b 4e 29 34 90 56 f3, expiry = 24 June 2019 19:06:30 UTC)

    ↳ COMODO SSL CA (serial number = 6e ba f0 8f 79 83 fa 9d e1 b2 6f 96 fc 6e 98 bf, expiry = 30 May 2020 10:48:38 UTC)

        ↳ End Entity SSL (serial number = x, expiry = from 1 month up to 60 months from issuance)

1.8.16 Comodo Unified Communication Certificates

Visible on IE compatible browsers as follows:

UTN - DATACorp SGC (serial number = 44 be 0c 8b 50 00 21 b4 11 d3 2a 68 06 a9 ad 69, expiry = 24 June 2019 20:06:40)

↳ End Entity SSL (serial number = x, expiry = 1-3 3 year(s) 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 - DATACorp SGC (serial number = 53 7b 76 56 4f 29 7f 14 dc 69 43 e9 22 ad 2c 79, expiry = 30 May 2020 11:48:38)

    ↳ End Entity SSL (serial number = x, expiry = 1- 3 year(s) from issuance)]

Entrust.net Secure Server CA (serial number = 42 86 f2 3d, expiry = 19 October 2012)

↳ AAA Certificate Services (serial number =e3 9f e0 6c 48 80 d3 8c b0 c5 2a a1 ef b0 6e ee ff f7 01 dd, expiry = 19 October 2012)

↳ End Entity SSL (serial number = x, expiry = 1 year to 5 years from issuance)

1.8.17 Dual Use Certificates

UTN-USERFirst-Client Authentication and Email (*serial number = 44 be 0c 8b 50 00 24 b4 11 d3 36 25 25 67 c9 89, expiry = 09 July 2019 18:36:58*)

↳ End Entity (*serial number = x, expiry = 1 month or up to 10 year(s) from issuance*)

1.8.18 Educational Certificates

Visible on 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)

↳ End Entity SSL/End Entity Secure Email (serial number = x, expiry = 1 month or up to 10 year(s) 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)

↳ End Entity SSL/End Entity Secure Email (serial number = x, expiry = 1 month or up to 10 year(s) 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 CPS (or other CA business practices disclosure), as the same may from time to time be modified by amendments published in the Comodo repository (www.comodogroup.com/repository).
- Issue and publish certificates in a timely manner in accordance with the issuance times set out in this CPS.
- Upon receipt of a valid request to revoke the certificate from a person authorized to request revocation using the revocation methods detailed in this 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 CPS.
- Distribute issued certificates in accordance with the methods detailed in this CPS.
- Update CRLs in a timely manner as detailed in this CPS.
- Notify subscribers via email of the imminent expiry of their Comodo issued certificate (for a period disclosed in this CPS).

1.10 Comodo Registration Authorities

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.

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. 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 available at http://www.comodopartners.com/partner/partnerdoc.html). The Web Host Reseller Partner is obliged to conduct validation in accordance with the validation guidelines prior to issuing a certificate. 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 4.3.2 for examples of documentation required) and must enter into a Comodo Powered SSL Partner agreement prior to being provided with Powered SSL Partner facilities.

1.11 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 a 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 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 not all Comodo certificate products are intended to be used in an e-commerce transaction or environment, parties who rely on certificates not intended for e-commerce do not qualify as a relying party. Please refer to Section 2.4 to determine whether a particular product is intended for use in e-commerce transactions.

To verify the validity of a digital certificate they receive, relying parties must refer to the Certificate Revocation List (CRL) or OCSP response 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. OCSP responses are sent through the OCSP responder.

1.13 Comodo Time-Stamping Authority

Comodo operates a trusted Time-Stamping Authority (TSA). The Comodo TSA provides an Authenticode time-stamping service which is intended only for use in signing software when used in conjunction with a Comodo Code-signing certificate. No warranty is offered and no liability will be accepted for any use of the Comodo TSA which is made other than signing software in conjunction with a Comodo Code-signing certificate.

The Comodo Authenticode time-stamping service is available at the URL http://timestamp.comodoca.com/authenticode.

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 are shown below in Table 2.1.1. Protection of the CA 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. The CA 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	10 years	2048

		commercially active)		
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	AddTrust Qualified CA Root	30-May-2020	2048

		Root			
40	AddTrust/UTN Object CA	AddTrust/UTN Object CA	09-Jul-2019	2048
41	Custom CA	Covered by alternative	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 Certification Authority	High Assurance SSL Certificates	31 Dec 2029	2048
153	Comodo High Assurance Secure Server CA	Intermediate for High Assurance SSL Certificates	31 Dec 2029	2048

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

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 UTN and AddTrust 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).

2.1.2 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 key was 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 CPS.

2.1.4 Procedures employed for CA Root Signing Key Changeover

The lifetime of our CA keys is set out in Table 2.1.1. Towards 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 CPS.

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 EntrustRoot certificate is present in Internet Explorer 5.00 and above, Netscape 4.5 and above, Mozilla, FireFox, Konqueror 2.2.1, Camino 1.0, Sun Java J2SE 1.42 and Opera 5.0 and above and is made available to relying parties through these browsers and clients.

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 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 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 CPS) to the Subscriber upon issuance and delivery of the Subscriber certificate.

2.1.6 Physical CA Operations

2.1.6.1 Comodo

Access to the secure part of Comodo facilities is limited using physical access control and is only accessible to appropriately authorized individuals (referred to hereon as Trusted Personnel). 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.

Comodo asserts that it makes every reasonable effort to detect and prevent material breaches, loss, damage or compromise of assets and interruption to business activities.

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.
- Storing private keys.
- Escrowing private keys.
- Generating, issuing, decommissioning, and destruction of key pairs.
- Retrieving certificates in accordance with their particular intended use.
- Verification of the domain of an applicant of a 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 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/Class3SecurityServices_3.crl

http://crl.comodoca.com/Class3SecurityServices 3.crl
http://crl.comodoca.com/ComodoHighAssuranceSecureServerCA.crl

Comodo operates an OCSP service at http://ocsp.comodo.com. Comodo's OCSP responder conforms to RFC 2560. Revocation information is made immediately available through the OCSP services. The OCSP responder and responses are available 24x7.

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

http://crl.comodoca.com/Class3SecurityServices.crl
http://crl.comodo.net/Class3SecurityServices.crl

Comodo also publishes a repository of legal notices regarding its PKI services, including this CPS, agreements and notices, references within this CPS as well as any other information it considers essential to its services. The Comodo legal repository may be accessed at www.comodogroup.com/repository.

2.4 Types of Comodo Certificates

Comodo currently offers a portfolio of digital certificates and related products that can be used in a way that addresses the needs of users for secure personal and business communications, including but not limited to secure email, protection of online transactions and identification of persons, whether legal or physical, or devices on a network or within a community.

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 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. As detailed in this CPS, Comodo offers a range of distinct certificate types. The different certificate types have differing intended usages and differing policies. Pricing and subscriber fees for the certificates are made available on the relevant official Comodo websites. The maximum warranty associated with each certificate 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 SSL 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, providing full authentication and enabling secure communication with customers and business partners. Comodo Secure Server Certificates are offered in the variants listed below.

a) PositiveSSL Certificate

PositiveSSL Certificates are low assurance level Secure Server Certificates from Comodo.

In accordance with section 4.2.2 (Validation Practices) of this CPS, PositiveSSL Certificates receive limited validation by Comodo. Comodo at its discretion may establish domain control by utilizing third party domain name registrars and directories, by verifying control of the domain by practical demonstration of the control of the domain, by implementing further validation processes including out of bands validation of the applicant's submitted information, or by relying on the accuracy of the applicant's application and the representations made in the subscriber agreement.

PositiveSSL certificates carry a warranty of $10,000 against certificate mis-issuance. Subscriber fees for a PositiveSSL Certificate are available from the official Positive SSL website.

PositiveSSL certificates are available from the following channels: Comodo Website, Reseller Network, Web Host Network, PoweredSSL Network, and EPKI Manager.

b) PositiveSSL Wildcard Certificate

PositiveSSL Wildcard certificates are low assurance Secure Server Certificates from Comodo.

In accordance with section 4.2.2 (Validation Practices) of this CPS, PositiveSSL Wildcard Certificates receive limited validation by Comodo. Comodo, at its discretion may establish domain control by utilizing third party domain name registrars and directories by verifying control of the domain by practical demonstration of the control of the domain, by implementing further validation processes including out of bands validation of the applicant's submitted information, or by relying on the accuracy of the applicant's application and the representations made in the subscriber agreement.

PositiveSSL Wildcard certificates are available from the following channels: Comodo Website, Reseller Network, Web Host Network, PoweredSSL Network, and EPKI Manager.

c) PositiveSSL Trial Certificate

PositiveSSL Trial Certificates are Secure Server Certificates designed to help customers use SSL in a test environment prior to the roll out of a full PositiveSSL solution. PositiveSSL Trial Certificates may be used in an external environment and ultimately may contain information relied upon by the relying party. PositiveSSL Trial Certificates are not intended for e-commerce use, but are for test use only and do not carry a warranty. There is no charge for a PositiveSSL Trial Certificate.

All PositiveSSL Trial Certificates are validated prior to issuance in accordance with section 4.2.2 of this CPS.

PositiveSSL Trial certificates are available from the following channels: Comodo Website, Reseller Network, Web Host Network, PoweredSSL Network, and EPKI Manager.

d) OptimumSSL Certificate

OptimumSSL 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.

In accordance with section 4.2.2 (Validation Practices) of this CPS, OptimumSSL Certificates receive limited validation by Comodo. Comodo, at its discretion may establish domain control by utilizing third party domain name registrars and directories, by verifying control of the domain by practical demonstration of the control of the domain, by implementing further validation processes including out of bands validation of the applicant's submitted information, or by relying on the accuracy of the applicant's application and the representations made in the subscriber agreement.

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

OptimumSSL certificates are available from the following channels: Comodo Website, Reseller Network, Web Host Network, PoweredSSL Network, and EPKI Manager.

e) OptimumSSL Wildcard Certificate

OptimumSSL 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.

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

In accordance with section 4.2.2 (Validation Practices) of this CPS, OptimumSSL Wildcard Certificates receive limited validation by Comodo. Comodo, at its discretion may establish domain control by utilizing third party domain name registrars and directories by verifying control of the domain by practical demonstration of the control of the domain, by implementing further validation processes including out of bands validation of the applicant's submitted information, or by relying on the accuracy of the applicant's application and the representations made in the subscriber agreement.

OptimumSSL Wildcard certificates are available from the following channels: Comodo Website, Reseller Network, Web Host Network, PoweredSSL Network, and EPKI Manager.

f) Comodo Intranet SSL Certificate

Intranet SSL Certificates are Secure Server Certificates designed to be used exclusively on internal networks. Their usage is restricted to private IP addresses or full server names only. As Intranet SSL 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 4.2.5 (Validation Practices) of this CPS, the Intranet SSL Certificate is for use only within a closed network and Comodo does not exercise validation in the issuance of an Intranet SSL Certificate. There is no warranty attached to an Intranet SSL Certificate.

Intranet SSL certificates are available from the following channels: Comodo Website, Reseller Network, Web Host Network, PoweredSSL Network, and EPKI Manager.

g) Comodo Trial SSL Certificate

Trial SSL Certificates are Secure Server Certificates designed to help customers use SSL in a test environment prior to the roll out of a full SSL solution. Trial SSL Certificates may be used in an external environment and ultimately may contain information relied upon by the relying party. Trial SSL Certificates are not intended for e-commerce use, but are for test use only and do not carry a warranty. There is no charge for a Trial SSL Certificate.

All Trial SSL Certificates are validated prior to issuance in accordance with section 4.2.3 of this CPS.

TrialSSL certificates are available from the following channels: Comodo Website, Reseller Network, Web Host Network, PoweredSSL Network, and EPKI Manager.

h) Comodo InstantSSL Certificate

InstantSSL Certificates are the entry level Secure Server Certificate from Comodo. Their intended usage is for websites conducting e-commerce or transferring data of low value and for within internal networks.

In accordance with section 4.2.3 (Validation Practices) of this CPS, InstantSSL Certificates utilize Comodo's IdAuthority to assist with application validation in order to provide increased speed of issuance. IdAuthority contains records of over 5 million unique legal entities sourced from a combination of publicly available resources. Where possible, the directory will be used to confirm the identity of a certificate applicant. If the directory cannot be used to sufficiently validate a certificate applicant, further validation processes will be used. These may include an out of bands validation of the applicant's submitted information.

InstantSSL certificates are available from the following channels: Comodo Website, Reseller Network, Web Host Network, PoweredSSL Network, and EPKI Manager.

i) Comodo InstantSSL Pro Certificate

ProSSL Certificates are the midlevel Secure Server Certificates from Comodo. Their intended usage is for websites conducting e-commerce or transferring data and within internal networks.

In accordance with section, 4.2.4 (Validation Practices) of this CPS ProSSL Certificates may also utilize Comodo's IdAuthority to assist as part of the certificate application. All ProSSL Certificate applications include an out of bands validation of the applicant's submitted information.

ProSSL certificates are available from the following channels: Comodo Website, Reseller Network, Web Host Network, PoweredSSL Network, and EPKI Manager.

j) Comodo PremiumSSL Certificate

PremiumSSL Certificates are the professional level Secure Server Certificates from Comodo. Their intended usage is for websites conducting high value e-commerce or transferring data and within internal networks.

In accordance with section 4.2.4 (Validation Practices) of this CPS, PremiumSSL Certificates may also utilize Comodo's IdAuthority to assist as part of the certificate application. All PremiumSSL Certificate applications include an out of bands validation of the applicant's submitted information.

PremiumSSL certificates are available from the following channels: Comodo Website, Reseller Network, Web Host Network, PoweredSSL Network, and EPKI Manager.

k) Comodo PremiumSSL Wildcard Certificate

PremiumSSL Wildcard Certificates are professional level Secure Server Certificates used to secure multiple sub-domains with a single PremiumSSL Certificate. Their intended use is for websites conducting high value e-commerce or transferring data and within internal networks.

In accordance with section 4.2.4 (Validation Practices) of this CPS, PremiumSSL Wildcard Certificates may also utilize Comodo's IdAuthority to assist as part of the certificate application. All PremiumSSL Wildcard Certificate applications include an out of bands validation of the applicant's submitted information.

PremiumSSL certificates are available from the following channels: Comodo Website, Reseller Network, Web Host Network, PoweredSSL Network, and EPKI Manager.

l) Comodo SGC SSL Certificate

Comodo SGC SSL Certificates are professional level Server Gated Cryptography (SGC) enabled certificates designed to upgrade the encryption capabilities of older browsers from 40-bit encryption into full 128/256 bit encryption. Their intended usage is for websites conducting high value e-commerce or transferring data and within internal networks.

In accordance with section, 4.2.4 (Validation Practices) of this CPS Comodo SGC SSL Certificates may also utilize Comodo's IdAuthority to assist as part of the certificate application. All Comodo SGC SSL Certificate applications include an out of bands validation of the applicant's submitted information.

Comodo SGC SSL certificates are available from the following channels: Comodo Website, Reseller Network, Web Host Network, PoweredSSL Network, and EPKI Manager.

m) Comodo SGC SSL Wildcard Certificate

Comodo SGC SSL Wildcard Certificates are professional level Server Gated Cryptography (SGC) enabled certificates designed to upgrade the encryption capabilities of older browsers from 40-bit encryption into full 128/256 bit encryption and used to secure multiple sub-domains with a single Comodo SGC SSL Certificate. Their intended use is for websites conducting high value e-commerce or transferring data and within internal networks.

In accordance with section 4.2.4 (Validation Practices) of this CPS, Comodo SGC SSL Wildcard Certificates may also utilize Comodo's IdAuthority to assist as part of the certificate application. All PremiumSSL Wildcard Certificate applications include an out of bands validation of the applicant's submitted information.

Comodo SGC SSL Wildcard Certificates are available from the following channels: Comodo Website, Reseller Network, Web Host Network, PoweredSSL Network, and EPKI Manager.

n) Comodo PremiumSSL Legacy Certificate

PremiumSSL Legacy Certificates are professional level Secure Server Certificates from Comodo. Their intended usage is for websites conducting high value e-commerce or transferring data and within internal networks.

In accordance with section 4.2.4 (Validation Practices) of this CPS, PremiumSSL Legacy Certificates may also utilize Comodo's IdAuthority to assist as part of the certificate application. All PremiumSSL Legacy Certificate applications include an out of bands validation of the applicant's submitted information.

PremiumSSL Legacy certificates are available from the following channels: Comodo Website, Reseller Network, Web Host Network, PoweredSSL Network, and EPKI Manager.

o) Comodo PremiumSSL Legacy Wildcard Certificate

PremiumSSL Legacy Wildcard Certificates are professional level Secure Server Certificates used to secure multiple sub-domains with a single PremiumSSL Legacy Certificate. Their intended use is for websites conducting high value e-commerce or transferring data and within internal networks.

In accordance with section 4.2.4 (Validation Practices) of this CPS, PremiumSSL Legacy Wildcard Certificates may also utilize Comodo's IdAuthority to assist as part of the certificate application. All PremiumSSL Legacy Wildcard Certificate applications include an out of bands validation of the applicant's submitted information.

PremiumSSL Legacy Wildcard Certificates are available from the following channels: Comodo Website, Reseller Network, Web Host Network, PoweredSSL Network, and EPKI Manager.

p) Elite SSL Certificate

Elite SSL Certificates are the entry level Enterprise Secure Server Certificate from Comodo. Their intended usage is for websites conducting e-commerce or transferring data of lower value and for within internal networks.

In accordance with section 4.2.1 and 4.2.4 (Validation Practices) of this CPS, Elite SSL Certificates may also utilize Comodo's IdAuthority to assist as part of the certificate application. Where possible, the directory will be used to confirm the identity of a certificate applicant. If the directory cannot be used to sufficiently validate a certificate applicant, further validation processes will be used. These may include an out of bands validation of the applicant's submitted information.

EliteSSL certificates are available from the following channels: Comodo Website, Reseller Network, Web Host Network, PoweredSSL Network, and EPKI Manager.

q) Gold SSL Certificate

Gold SSL Certificates are the midlevel Enterprise Secure Server Certificates from Comodo. Their intended usage is for websites conducting e-commerce or transferring

data and within internal networks.

In accordance with section, 4.2.4 (Validation Practices) of this CPS Gold SSL Certificates may also utilize Comodo's IdAuthority to assist as part of the certificate application. All Gold SSL Certificate applications include an out of bands validation of the applicant's submitted information.

GoldSSL certificates are available from the following channels: Comodo Website, Reseller Network, Web Host Network, PoweredSSL Network, and EPKI Manager.

r) Platinum SSL Certificate

Platinum SSL Certificates are the professional level Enterprise Secure Server Certificates from Comodo. Their intended usage is for websites conducting high value e-commerce or transferring data and within internal networks.

In accordance with section 4.2.4 (Validation Practices) of this CPS, Platinum SSL Certificates may also utilize Comodo's IdAuthority to assist as part of the certificate application. All Platinum SSL Certificate applications include an out of bands validation of the applicant's submitted information

PlatinumSSL certificates are available from the following channels: Comodo Website, Reseller Network, Web Host Network, PoweredSSL Network, and EPKI Manager.

s) Platinum SSL Wildcard Certificate

Platinum SSL Wildcard Certificates are professional level Enterprise Secure Server Certificates used to secure multiple sub-domains with a single Platinum SSL Certificate. Their intended use is for websites conducting high value e-commerce or transferring data and within internal networks.

In accordance with section 4.2.4 (Validation Practices) of this CPS, Platinum SSL Wildcard Certificates may also utilize Comodo's IdAuthority to assist as part of the certificate application. All Platinum SSL Wildcard Certificate applications include an out of bands validation of the applicant's submitted information.

PlatinumSSL Wildcard certificates are available from the following channels: Comodo Website, Reseller Network, Web Host Network, PoweredSSL Network, and EPKI Manager.

t) PlatinumSSL SGC Certificate

PlatinumSSL SGC Certificates are professional level Enterprise Secure Server Certificates. They are Server Gated Cryptography (SGC) enabled to upgrade the encryption capabilities of older browsers from 40-bit encryption into full 128/256 bit encryption. Their intended usage is for websites conducting high value e-commerce or transferring data and within internal networks.

In accordance with section, 4.2.4 (Validation Practices) of this CPS PlatinumSSL SGC Certificates may also utilize Comodo's IdAuthority to assist as part of the certificate application. All PlatinumSSL SGC Certificate applications include an out of bands validation of the applicant's submitted information.

PlatinumSSL SGC certificates are available from the following channels: Comodo Website, Reseller Network, Web Host Network, PoweredSSL Network, and EPKI Manager.

u) PlatinumSSL SGC Wildcard Certificate

PlatinumSSL SGC Wildcard Certificates are professional level Enterprise Secure Server Certificates used to secure multiple sub-domains with a single PlatinumSSL SGC Wildcard Certificate. They are Server Gated Cryptography (SGC) enabled to upgrade the encryption capabilities of older browsers from 40-bit encryption into full 128/256 bit encryption. Their intended usage is for websites conducting high value e-commerce or transferring data and within internal networks.

In accordance with section, 4.2.4 (Validation Practices) of this CPS PlatinumSSL SGC Wildcard Certificates may also utilize Comodo's IdAuthority to assist as part of the certificate application. All PlatinumSSL SGC Wildcard Certificate applications include an out of bands validation of the applicant's submitted information.

PlatinumSSL SGC Wildcard certificates are available from the following channels: Comodo Website, Reseller Network, Web Host Network, PoweredSSL Network, and EPKI Manager.

v) PlatinumSSL Legacy Certificate

Platinum SSL Legacy Certificates are professional level Enterprise Secure Server Certificates from Comodo. Their intended usage is for websites conducting high value e-commerce or transferring data and within internal networks.

In accordance with section 4.2.4 (Validation Practices) of this CPS, Platinum SSL Legacy Certificates may also utilize Comodo's IdAuthority to assist as part of the certificate application. All Platinum SSL Legacy Certificate applications include an out of bands validation of the applicant's submitted information

PlatinumSSL Legacy certificates are available from the following channels: Comodo Website, Reseller Network, Web Host Network, PoweredSSL Network, and EPKI Manager.

w) PlatinumSSL Legacy Wildcard Certificate

Platinum SSL Legacy Wildcard Certificates are professional level Enterprise Secure Server Certificates used to secure multiple sub-domains with a single Platinum SSL Legacy Certificate. Their intended use is for websites conducting high value e-commerce or transferring data and within internal networks.

In accordance with section 4.2.4 (Validation Practices) of this CPS, Platinum SSL Legacy Wildcard Certificates may also utilize Comodo's IdAuthority to assist as part of the certificate application. All Platinum SSL Legacy Wildcard Certificate applications include an out of bands validation of the applicant's submitted information.

PlatinumSSL Legacy Wildcard certificates are available from the following channels: Comodo Website, Reseller Network, Web Host Network, PoweredSSL Network, and EPKI Manager.

x) PositiveSSL Multi-Domain SSL Certificate

Multi Domain Certificates (MDCs) are Secure Server Certificates issued by Comodo as a means of validation of domain control for the domains jointly hosted on a single server and named within the MDC.

As MDCs are not intended for e-commerce use, and due to the increased validation speed and the nature of how Comodo intends MDCs to be used, the certificates carry no warranty.

In accordance with section 4.2.2 (Validation Practices) of this CPS, MDCs 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 right to use the domain name used in the application. 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.

MDCs are available from the following channels: Comodo Website, Reseller Network, Web Host Network, and EPKI Manager.

y) Essential SSL Certificate

Essential SSL 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.

In accordance with section 4.2.2 (Validation Practices) of this CPS, Essential SSL Certificates receive limited validation by Comodo. Comodo, at its discretion may establish domain control by utilizing third party domain name registrars and directories, by verifying control of the domain by practical demonstration of the control of the domain, by implementing further validation processes including out of bands validation of the applicant's submitted information, or by relying on the accuracy of the applicant's application and the representations made in the subscriber agreement.

Due to the increased validation speed, the lack of robust validation, and the nature of how Comodo intends Essential SSL Certificates to be used, the certificates carry no warranty.

Essential SSL Certificates are available from the following channels: Comodo Website, Reseller Network, Web Host Network, PoweredSSL Network, and EPKI Manager.

z) Essential SSL Wildcard Certificates

Essential SSL 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.

Due to the increased validation speed, the lack of robust validation, and the nature of how Comodo intends Essential SSL Wildcard Certificates to be used, the certificates carry no warranty.

In accordance with section 4.2.2 (Validation Practices) of this CPS, Essential SSL Wildcard Certificates receive limited validation by Comodo. Comodo, at its discretion may establish domain control by utilizing third party domain name registrars and directories, by verifying control of the domain by practical demonstration of the control of the domain, by implementing further validation processes including out of

bands validation of the applicant's submitted information, or by relying on the accuracy of the applicant's application and the representations made in the subscriber agreement.

Essential SSL Wildcard certificates are available from the following channels: Comodo Website, Reseller Network, Web Host Network, PoweredSSL Network, and EPKI Manager.

aa) Essential SSL Trial Certificate

Essential SSL Trial Certificates are Secure Server Certificates designed to help customers use SSL in a test environment prior to the roll out of a full Essential SSL solution. Essential SSL Trial Certificates may be used in an external environment and ultimately may contain information relied upon by the relying party. Essential SSL Trial Certificates are not intended for e-commerce use, but are for test use only and do not carry a warranty. There is no charge for an Essential SSL Trial Certificate.

All Essential SSL Trial Certificates are validated prior to issuance in accordance with section 4.2.2 of this CPS.

Essential SSL Trial certificates are available from the following channels: Comodo Website, Reseller Network, Web Host Network, PoweredSSL Network, and EPKI Manager.

bb) Comodo Unified Communications Certificate

Comodo's Unified Communications Certificates (UCCs) are Microsoft-approved SSL certificates specifically designed for use with Microsoft Exchange Server 2007, Office Communications Server 2007 and Microsoft Live Communications Server. UCCs enable secure client access from the Internet and support the Domain Security feature SAN attribute required by Microsoft Exchange Server 2007 whereby multiple FQDNS may be added to each certificate. Each certificate is fully validated (domain name and business entity).

In accordance with section 4.2.2 (Validation Practices) of this CPS, UCCs 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 right to use the domain name used in the application. 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.

Comodo UCCs are available from the following channels: Comodo Website, Reseller Network, Web Host Network, and EPKI Manager.

cc) Intel Pro SSL Certificate

Intel Pro SSL certificates are specifically designed for use with Intel® vPro™ processor technology-based PCs and Intel® Centrino Pro processor technology-based notebooks. Intel Pro Series SSL Certificates provide authentication and encryption for the remote configuration of Intel® vPro™ processor technology based PCs and Intel® Centrino Pro processor technology based notebooks. Each certificate contains a unique value in EKU field (2.16.840.1.113741.1.2.3) and is fully validated (domain name and business entity), providing a high level of trust and authentication.

In accordance with section 4.2.2 (Validation Practices) of this CPS, Intel Pro SSL 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 right to use the domain name used in the application. 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.

Intel Pro SSL Certificates are available from the following channels: Comodo Website, Reseller Network, Web Host Network, PoweredSSL Network, and EPKI Manager.

dd) ComodoSSL Certificates

In accordance with section 4.2.2 (Validation Practices) of this CPS, ComodoSSL 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 right to use the domain name used in the application. 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 band validation of the applicant's submitted information.

ComodoSSL certificates are available from the following channels: Comodo Website, Reseller Network, Web Host Network, PoweredSSL Network, and EPKI Manager.

ee) Educational Certificates and IGTF Certificates

Comodo Educational and IGTF Certificates are designed for distribution by Comodo's partners to educational, research, and non-profit entities to use to conduct non-credit card transactions with their website.

2.4.2 Comodo SSL Client / Secure Email Certificates

Comodo makes available Secure Email Certificates that in combination with an S/MIME compliant email application allow subscribers to digitally sign email for relying parties, or relying parties to encrypt email for the subscriber. Pricing for the certificates is made available on the relevant official Comodo websites. From time to time Comodo reserves the right to make available promotional offers that may affect the standard price card.

a) Personal Secure Email Certificate

Personal Secure Email Certificates are issued to natural persons only and may not be used by an individual as a means of representation for a specific company.

In accordance with section 4.2.6 (Validation Practices) of this CPS, and using an email ownership validation check, Comodo asserts that the subscriber owns, or has direct access to, the email address stated within the Personal Secure Email Certificates.

However, as verification of the subscriber does not take place the identity of the subscriber cannot be warranted.

b) Corporate Secure Email Certificate

Corporate Secure Email Certificates are issued to natural persons only and may be used by an individual as a means of representation for a company named within the certificate.

Corporate Secure Email Certificates are available to holders of a Comodo EPKI Manager account. The EPKI Manager account may be used to apply for Comodo certificates (SSL and Secure Email) and will contain the corporate details (name, address, country) of the account holding company. EPKI Manager authorized administrators may log into the EPKI Manager online account and apply for Corporate Secure Email Certificates for employees or authorized representatives of the company only.

In accordance with section 4.2.7 (Validation Practices) of this CPS, Comodo validates the right of the company to use the domain name specified within the Corporate Secure Email Certificate. The company must attest to the identity of the individual named within the application prior to the issuance of the Corporate Secure Email Certificate.

c) Comodo TF Certificates

Comodo TF Certificates are Custom Client certificates issued to customers of large merchants providing online services, including but not limited to banks and financial services. Comodo TF Certificates, in conjunction with the Comodo TF Authentication Solution, allow for two-factor authentication of a Client's right to access a service provider's online services.

In accordance with section 4.2.9 (Validation Practices), validation procedures of applicants for Comodo TF Certificates are performed by approved organizations using the customer's existing online account username and password.

d) Custom Client Certificates

Custom Client Certificates are versatile client certificates that may be used for authentication, encryption, digital signing of documents, and other purposes. The fields in these certificates are customizable to allow their use in a wide range of applications requiring client authentication.

The flexibility of the subject fields of these certificates lends them particularly to backward compatibility with legacy applications requiring a fixed format as well as to new applications with unusual requirements.

These certificates are issued to both individuals and corporations. Depending on the purpose of the certificate, Custom Client Certificates may be persona non-validated, validated by domain name, or validated as to the organizational entity receiving the certificate.

Custom Client Certificates issued through a Comodo partner may have validation requirements set by the Comodo partner. Anyone wanting to use or rely on a Custom Client Certificate from a Comodo partner should contact the Comodo partner first to obtain all of the important validation information about the certificate's issuance. .

e) Comodo Dual Use Certificates
Comodo Dual Use Certificates are high assurance certificates used as email and identification certificates that are issued through the Certificate Manager software to

the end users of the Certificate Manager subscriber. These certificates are used for secure remote access to the subscriber's computer networks by its employees, agents, and contractors as well as providing these individuals with secure email services.

In accordance with section 4.2.12 (Validation Practices), validation procedures of applicants for Comodo Dual Use Certificates are by having the Certificate Applicant appear before an agent of the CA, RA, or before a notary public or other official with comparable authority within the Applicant's jurisdiction.

2.4.3 Software Publishing Certificates

a) Code Signing Certificate

Code Signing Certificates are designed for commercial software developers to provide assurance regarding the developer's identity, and are designed to represent the level of assurance provided today by retail channels for software. With a Code Signing Certificate, a digital signature can be appended to the executable code itself, thus providing assurance to recipients that the code or software does indeed come from the signer of the software.

In accordance with section 4.2.1 (Validation Practices) of this CPS, Comodo will take measures to confirm the identity of a Code Signing Certificate applicant. All Code Signing Certificate applications include an out of bands validation of the applicant's submitted information.

b) Time Stamping Certificate

Time Stamping Certificates are designed to ensure that the code-signing took place at a specific point in time, specifically during the period for which the Code Signing Certificate was valid, thus extending the validity of the code past its certificate expiration date.

In accordance with section 4.2.1 (Validation Practices) of this CPS, Comodo will take measures to confirm the identity of a Code Signing Certificate applicant. All Code Signing Certificate applications include an out of bands validation of the applicant's submitted information.

2.4.4 Content Verification Certificates

a) Content Verification Certificate

Content Verification Certificates (CVCs) are digital certificates that protect "web page content" such as graphics, logos and login boxes so that, in conjunction with Comodo's VerificationEngine, an Internet user can verify the website's identity. The content requiring protection is digitally bound within an X.509 compliant certificate also holding location information.

In accordance with section 4.2.3 (Validation Practices) of this CPS, Comodo will take measures to confirm the identity of a Content Verification Certificate applicant. Content Verification Certificates may also utilize Comodo's IdAuthority to assist as part of the certificate application. All Content Verification Certificate applications include an out of bands validation of the applicant's submitted information.

b) Payment Credential CVC (1 logo) / Payment Credential CVC (3 logos)

Payment Credential CVCs, for either 1 logo or 3 logos, in conjunction with Comodo's VerificationEngine, provide assurance to website visitors that the website vendor is authorized to accept online payments via the credit card issuer whose logo is protected by the Payment Credential CVC.

These CVCs are only issued to subscribers after confirmation that the website merchant is approved by the card issuer to accept payment by that credit card.

c) Payment Credential CVC (Wildcard)

Payment Credential Wildcard CVCs, in conjunction with Comodo's VerificationEngine, provide assurance to website visitors that the website vendor is authorized to accept online payments via the credit card issuer whose logo is protected by the Payment Credential CVC on multiple subdomains.

These CVCs are only issued to subscribers after confirmation that the website merchant is approved by the card issuer to accept payment by that credit card.

Payment Credential Wildcard CVC are available from the following channels: Comodo Website, Reseller Network, Web Host Network, PoweredSSL Network, and EPKI Manager.

d) Trial Payment Credential CVC

Trial Payment Credential CVCs are designed to help customers use SSL in a test environment prior to the roll out of a Payment Credential CVC. Trial Payment Credential CVCs may be used in an external environment and ultimately may contain information relied upon by the relying party. Trial Payment Credential CVCs are not intended for e-commerce use, but are for test use only and do not carry a warranty.

All Trial Payment Credential CVCs are validated to confirm that the website merchant is approved by the card issuer to accept payment by that credit card.

Trial Payment Credential CVCs are 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 Process

The Subscriber is solely responsible for the generation of the private key used in the certificate request. However, for certain products, Comodo does not provide the option of key generation, escrow, recovery, and backup facilities for private keys. Keys generated by Comodo are generated during the order process for the certificate. Where keys are backed-up or escrowed, the keys are generated on Comodo's servers and then delivered to the subscriber over an encrypted communication. At the request of certain qualifying subscribers, Comodo will escrow the private keys it generates by encrypting the private key and storing it on a Comodo server.

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).

Secure Server Certificate requests are generated using the key generation facilities available in the Subscriber's webserver software.

Client Certificate requests are generated using the FIPS 140-1 Level 1 cryptographic service provider module software present in popular browsers.

Code Signing Certificate and Time Stamping Certificate requests are generated using the FIPS 140-1 Level 1 cryptographic service provider module software present in Microsoft Internet Explorer.

Comodo TF Certificate requests are generated using the FIPS 140-1 Level 1 cryptographic service provider module software present in popular browsers. In cases when the customer's browser is incapable of generating the private key, the Comodo TF software generates the private key on behalf of the customer and delivers the private key and certificate to the customer.

Comodo Dual Use Certificate requests are generated by Comodo on the Comodo Servers. The Comodo Certificate Manager software generates the private key on behalf of the end user and delivers the private key and certificate to the end user.

The private key of key-pairs generated by Comodo through its Comodo TF software are not held by Comodo after being transferred to the customer. All such keys are securely deleted after being transferred to the subscriber. Logical and physical controls prevent access to private key's generated by subscribers. All keys sent to subscribers are protected during delivery using an authenticated and secure connection to Comodo's servers.

2.7 Subscriber Private Key Protection and Backup

Generally, the Subscriber is solely responsible for protection of their private keys. However, Comodo offers certain subscribers the optional feature of having Comodo back up the private keys Comodo generates on their behalf. Comodo protects these keys by having an agent or agents of the Certificate Manager Subscriber (typically, the employer of the individual receiving

the client certificate) encrypt a PKCS#12 format that contains the keys before they are stored on a secure server. Keys stored by Comodo can only be decrypted using the keys held by the selected agents of the Certificate Manager Subscriber. Encrypted keys are sent via a secure connection and decrypted by the agent of the Certificate Manager Subscriber on their own computers.

Escrowed private key can only be recovered after Comodo confirms the authority of the party requesting the private key. Private keys may only recovered for lawful and legitimate purposes. Comodo recommends to its Certificate Manager subscribers that they notify their customers and subscribers that their private keys are escrowed, that they protect escrowed keys from unauthorized disclosure, and that they do not disclose or allow to be disclosed any escrowed keys or escrowed-key related information to a third party unless required by law. Certificate Manager Users are required to revoke the certificate associated with an escrowed private key prior to retrieving the escrowed key from Comodo.

Escrowed Private Keys are kept for three years after the corresponding certificate's expiry prior to their destruction. Private Keys are destroyed by deleting the key from the storage material immediately, and from all related back up material within a further 12 month period.

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.

Secure Email Certificate requests are generated using the Subscriber's cryptographic service provider software present in the Subscriber's browser and submitted to Comodo in the form of a PKCS#10 Certificate Signing Request (CSR). The Subscriber's browser generally makes submission automatically.

CVC requests are generated through a sales representative over the phone or online from www.contentverification.com.

Code Signing Certificate and Time Stamping Certificate requests are generated using the Subscriber's cryptographic service provider software present in the Subscriber's browser and submitted automatically to Comodo in the form of a PKCS#10 Certificate Signing Request (CSR). The private key may either be allowed to remain in the cryptographic service provider, or may be exported to the subscriber's hard drive.

Comodo TF Certificate requests are generated and submitted to Comodo using Comodo's TF Server software.

2.9 Delivery of Issued Subscriber Certificate to Subscriber

Delivery of Subscriber certificates to the associated Subscriber is dependent on the certificate product type:

2.9.1 Secure Server Certificate: InstantSSL product type

If the Comodo operated IdAuthority database holds sufficient validation information, an automatic validation of the InstantSSL certificate application may take place. In the event of such an automated validation the InstantSSL certificate is delivered to commonly used generic email addresses ordinarily belonging to authorized personnel at the domain name used in the application, such as webmaster@... admin@... postmaster@... Confirmation of the certificate delivery location is provided to the administrator contact provided during the application process.

2.9.2 Secure Server Certificates

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

2.9.3 Content Verification Certificates

Content Verification Certificates are delivered to the Subscriber via e-mail, or they are stored via Comodo's database servers.

2.9.4 Code Signing Certificates

Code Signing Certificates are delivered via email to the Subscriber using the administrator contact email address provided during the application process.

2.9.5 Comodo TF Certificates

Comodo TF Certificates are downloaded by the subscriber customers automatically from the Comodo TF Server Software.

2.9.6 Secure Email Certificate: Personal Secure Email and Corporate Secure Email Certificates

Upon issuance of a Personal Secure Email Certificate or Corporate Secure Email Certificate, the Subscriber is emailed a collection link using the email provided during the application. The Subscriber must visit the collection link using the same computer from which the original certificate request was made. The Subscriber's cryptographic service provider software is initiated to ensure the Subscriber holds the private key corresponding to the public key submitted during application. Pending a successful challenge, the issued certificate is installed automatically onto the Subscriber's computer.

2.9.7 Comodo Dual Use Certificates

Comodo Dual Use Certificates are downloaded by the subscribers from the Comodo Certificate Manager Software.

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 Key Usage extension field

Comodo certificates are general purpose and may be used without restriction on geographical area or industry. In order to use and rely on a Comodo certificate the 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 of the control of Comodo.

The possible key purposes identified by the X.509v3 standard are the following:

   a) Digital signature, for verifying digital signatures that have purposes other than those identified in b), f) or g), that is, for entity authentication and data origin authentication with integrity
   b) Non-repudiation, for verifying digital signatures used in providing a nonrepudiation service which protects against the signing entity falsely denying some action (excluding certificate or CRL signing, as in f) or g) below)
   c) Key encipherment, for enciphering keys or other security information, e.g. for key transport
   d) Data encipherment, for enciphering user data, but not keys or other security information as in c) above
   e) Key agreement, for use as a public key agreement key
   f) Key certificate signing, for verifying a CA's signature on certificates, used in CA certificates only
   g) CRL signing, for verifying a CA's signature on CRLs
   h) Encipher only, public key agreement key for use only in enciphering data when used with key agreement

i) Decipher only, public key agreement key for use only in deciphering data when used with key agreement

2.12.2 Extension Criticality Field

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.

2.12.3 Basic Constraints Extension

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.

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.

Specific Comodo certificate profiles are as per the tables below:

Comodo Secure Server Certificates – InstantSSL / InstantSSL Pro / InstantSSL Wildcard / PremiumSSL / PremiumSSL Wildcard / EliteSSL / GoldSSL / PlatinumSSL / PlatinumSSL Wildcard / PremiumSSL Legacy / PremiumSSL Legacy Wildcard / PlatinumSSL Legacy / PlatinumSSL Legacy Wildcard / PlatinumSSL SGC Legacy / PlatinumSSL SGC Legacy Wildcard / Comodo SGC SSL / Comodo SGC SSL Wildcard / Trial SSL / Intranet SSL / Other SSL Certificates		
Signature Algorithm	Sha1	
Issuer (option 1) **(not for any SGC type)**	CN	Comodo Class 3 Security Services CA
	OU	(c) 2002 Comodo Limited
	OU	Terms and Conditions of use: http://www.comodo.net/repository
	OU	Comodo Trust Network
	O	Comodo Limited
	C	GB
Issuer (option 2) **(not for any SGC type)**	CN	UTN-USERFIRST-Hardware
	OU	http://www.usertrust.com
	O	The USERTRUST Network
	L	Salt Lake City
	S	UT
	C	US
Issuer (option 3) **for SGC types only.**	CN	UTN - DATACorp SGC
	OU	http://www.usertrust.com
	O	The USERTRUST Network
	L	Salt Lake City
	S	UT
	C	US

Issuer (option 4) **(not for any SGC type)**	CN	Comodo Class 3 Security Services CA
	OU	(c) 2006 Comodo CA Limited
	OU	Terms and Conditions of use: http://www.comodo.com/repository
	OU	Comodo Trust Network
	O	Comodo CA Limited
	C	GB
Issuer (option 5)	CN	Comodo High Assurance Secure Server CA
	OU	© 2008 Comodo CA Limited
	OU	Terms and Conditions of use: http://www.comodo.com/repository
	OU	Comodo Trust Network
	C	GB
Validity	1 - 5 Years	
Subject	CN	Common Name
	OU	InstantSSL / ProSSL/PremiumSSL / PremiumSSL Wildcard / EliteSSL /GoldSSL / PlatinumSSL / PlatinumSSL Wildcard / PremiumSSL Legacy / PremiumSSL Legacy Wildcard / PlatinumSSL Legacy / PlatinumSSL Legacy Wildcard / PlatinumSSL SGC Legacy / PlatinumSSL SGC Legacy Wildcard / Comodo SGC SSL / Comodo SGC SSL Wildcard / Other SSL Certificate name / *Powered SSL product name*
	OU (0 or 1 of)	*Hosted by [Web Host Reseller Subscriber Name]* *Issued through [EPKI Manager Subscriber Name]* *Provided by [Powered SSL Subscriber Name]*
	OU (for Intranet SSL only)	INTRANET USE ONLY – NO WARRANTY ATTACHED – COMPANY NOT VALIDATED
	OU (for Trial SSL only)	TEST USE ONLY - NO WARRANTY ATTACHED
	O	Organization
	OU	Organization Unit
	L	Locality
	STREET	Street
	S	State
	PostalCode	Zip or Postal Code
	C	Country
Authority Key Identifier	KeyID only is specified.	
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)	
(Additional usages for SGC types only)	Microsoft SGC (1.3.6.1.4.1.311.10.3.3) Netscape SGC (2.16.840.1.113730.4.1)	
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 = 1.3.6.1.4.1.6449.1.2.1.3.4 [1,1]Policy Qualifier Info: Policy Qualifier Id = CPS Qualifier: https://secure.comodo.net/CPS	

CRL Distribution Policies	[1]CRL Distribution Point
	   Distribution Point Name:
	     Full Name:
	       URL=<Primary CDP URL>
	
	[2]CRL Distribution Point
	   Distribution Point Name:
	     Full Name: URL=<Secondary CDP URL>

(only when the Issuing CA is "Comodo Class 3 Security Services CA")	[3]CRL Distribution Point
	   Distribution Point Name:
	     Full Name:
	     RFC822
	      Name=<CRL Request Email Address>

Authority Information Access (omitted when Issuing CA is "Comodo Class 3 Security Services CA")
 	
(non-critical)
	[1]Authority Info Access
	   Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)
	   Alternative Name:
	     URL=<Primary AIA URL>
	[2]Authority Info Access
	   Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)
	   Alternative Name:
	     URL=<Secondary AIA URL>

Thumbprint Algorithm	SHA1
Thumbprint	

Comodo Secure Server Certificate – Secure Email Certificate (Free Version) / Secure Email Certificate (Corporate Version) / Custom Client Certificates / Comodo TF / Dual Use Certificates		
Signature Algorithm	Sha1	
Issuer (option 1)	CN	Comodo Class 3 Security Services CA
	OU	(c) 2002 Comodo CA Limited
	OU	Terms and Conditions of use: http://www.comodo.net/repository
	OU	Comodo Trust Network
	O	Comodo Limited
	C	GB
Issuer (option 2)	CN	UTN-USERFirst-Client Authentication and Email
	OU	http://www.usertrust.com
	O	The USERTRUST Network
	L	Salt Lake City
	S	UT
	C	US
Issuer (option 3)	CN	Comodo Class 3 Security Services CA
	OU	(c) 2006 Comodo CA Limited
	OU	Terms and Conditions of use: http://www.comodo.com/repository
	OU	Comodo Trust Network
	O	Comodo CA Limited
	C	GB
Validity	1 year / 2 year / 3 year	
Subject (for Free version)	E	Email address
	CN	Common Name (name of subscriber)
	OU	(c)2003 Comodo Limited
	OU	Terms and Conditions of use: http://www.comodo.net/repository
	OU	Comodo Trust Network - PERSONA NOT VALIDATED
Subject (for Corporate version)	E	Email address
	CN	Common Name (name of subscriber)

	OU	Corporate Secure Email
	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
	STREET	Street
	S	State
	PostalCode	Zip or Postal Code
	C	Country
Subject (for Custom Client and Comodo TF version)	All fields are customizable on a per-certificate basis.	
Authority Key Identifier	KeyID only is specified.	
Extended Key Usage (NonCritical) (Free Version Only)	Secure Email (1.3.6.1.5.5.7.3.4) Receive Certified Delivery Email (Discontinued) (1.3.6.1.4.1.6449.1.3.5.2)	
Extended Key Usage (NonCritical) (Corporate Client versions)	Secure Email (1.3.6.1.5.5.7.3.4) Client Authentication (1.3.6.1.5.5.7.3.2)	
Extended Key Usage (NonCritical) (Custom Client Certificates)	serverAuth (1.3.6.1.5.5.7.3.1) clientAuth (1.3.6.1.5.5.7.3.2) codeSigning (1.3.6.1.5.5.7.3.3) emailProtection (1.3.6.1.5.5.7.3.4) ipsecEndSystem (1.3.6.1.5.5.7.3.5) ipsecTunnel (1.3.6.1.5.5.7.3.6) ipsecUser (1.3.6.1.5.5.7.3.7)	
Key Usage (NonCritical) (Custom Client Certificates)	digitalSignature(0), nonRepudiation(1), keyEncipherment(2)	
Netscape Certificate Type (Corporate Version Only)	SSL Client Authentication, SMIME (a0)	
Netscape Certificate Type (Free and Custom Client versions)	SMIME(20)	
Basic Constraint	Subject Type = End Entity Path Length Constraint = None	

Certificate Policies	[1] Certificate Policy:
	  PolicyIdentifier = 1.3.6.1.4.1.6449.1.2.1.3.5
	  [1,1]Policy Qualifier Info:
	    Policy Qualifier Id = CPS
	  Qualifier:
	https://secure.comodo.net/CPS	

CRL Distribution Policies	[1]CRL Distribution Point
	    Distribution Point Name:
	      Full Name:
	        URL=<Primary CDP URL>
	
	[2]CRL Distribution Point
	    Distribution Point Name:
	      Full Name: URL=<Secondary CDP URL>	

(Only for certificates issued by "Comodo Class 3 Security Services CA")	[3]CRL Distribution Point
	    Distribution Point Name:
	      Full Name:
	      RFC822
	        Name=<CRL Request Email Address>	

Authority Information Access (omitted when Issuing CA is "Comodo Class 3 Security Services CA")	[1]Authority Info Access
	    Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)
	    Alternative Name:
	        URL=<Primary AIA URL>
	[2]Authority Info Access
	    Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)
	    Alternative Name:
	        URL=<Secondary AIA URL>

Subject Alternate Name (omitted from Custom Client version)	RFC822 Name = email address
Thumbprint Algorithm	SHA1
Thumbprint	

PositiveSSL Secure Server Certificate – PositiveSSL / PositiveSSL Wildcard		
Signature Algorithm	Sha1	
Issuer	CN	PositiveSSL CA
	O	Comodo CA Limited
	L	Salford
	S	Greater Manchester
	C	GB
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	PositiveSSL
	OU	Domain Control Validated[1]
Authority Key Identifier	KeyID only.	
Key Usage (NonCritical)	Digital Signature , Key Encipherment(A0)	
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:
	    Policy Identifier=1.3.6.1.4.1.6449.1.2.2.7
	    [1,1]Policy Qualifier Info:
	        Policy Qualifier Id=CPS
	        Qualifier:
	            http://www.positivessl.com/CPS	

CRL Distribution Policies	[1]CRL Distribution Point
	    Distribution Point Name:
	        Full Name:
	            URL=<Primary CDP URL>
	[2]CRL Distribution Point
	    Distribution Point Name:
	        Full Name:
	            URL=<Secondary CDP URL>	

Authority Information Access	[1]Authority Info Access
	    Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)
	    Alternative Name:
	        URL=<Primary AIA URL>
	[2]Authority Info Access
	    Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)
	    Alternative Name:
	        URL=<Secondary AIA URL>	

Thumbprint Algorithm	SHA1	
Thumbprint		

PositiveSSL Secure Server Certificate – OptimumSSL / OptimumSSL Wildcard		
Signature Algorithm	Sha1	
Issuer	CN	OptimumSSL CA
	O	Comodo CA Limited
	L	Salford
	S	Greater Manchester
	C	GB
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	OptimumSSL
	OU	Domain Control Validated[1]
Authority Key Identifier	KeyID only.	
Key Usage (NonCritical)	Digital Signature , Key Encipherment(A0)	
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:
	    Policy Identifier=1.3.6.1.4.1.6449.1.2.2.7
	      [1,1]Policy Qualifier Info:
	        Policy Qualifier Id=CPS
	        Qualifier:
	            http://www.Optimumssl.com/CPS	

CRL Distribution Policies	[1]CRL Distribution Point
	    Distribution Point Name:
	        Full Name:
	          URL=<Primary CDP URL>
	[2]CRL Distribution Point
	    Distribution Point Name:
	        Full Name:
	          URL=<Secondary CDP URL>	

Authority Information Access	[1]Authority Info Access
	    Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)
	    Alternative Name:
	        URL=<Primary AIA URL>
	[2]Authority Info Access
	    Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)
	    Alternative Name:
	        URL=<Secondary AIA URL>	

Thumbprint Algorithm	SHA1	
Thumbprint		

Comodo MDC		
Signature Algorithm	Sha1	
Issuer (Option 1)	CN	UTN - DATACorp SGC
	OU	http://www.usertrust.com
	O	The USERTRUST Network
	L	Salt Lake City
	S	UT
	C	US
Issuer (Option 2)	CN	Comodo High Assurance Secure Server CA
	OU	© 2008 Comodo CA Limited
	OU	Terms and Conditions of Use: http://www.usertrust.com
	OU	Comodo Trust Network
	O	Comodo CA Limited
	C	US
Validity	1 Year / 2 Year / 3 Year	

Subject	CN	Common Name [Name Windows displays as "Issued To" – Typically Entity Name like O field]
	OU	Hosted by [Web Host Reseller Subscriber Name] Issued through [EPKI Manager Subscriber Name] Provided by [Powered SSL Subscriber Name]
	O	Organisation
	OU	Organisation Unit
	L	Locality
	S	Street
	C	Country
	CN	Domain Name 1
	CN	Domain Name 2
	CN	Domain Name 3 (etc. to Domain Name 100)
	CN	Common Name [Name Windows displays as "Issued To" – Typically Entity Name like O field]
Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2) Microsoft SGC (1.3.6.1.4.1.311.10.3.3) Netscape SGC (2.16.840.1.113730.4.1)	
Key Usage (NonCritical)	Digital Signature , Key Encipherment(A0)	
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: Policy Identifier=1.3.6.1.4.1.6449.1.2.1.3.4 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://secure.comodo.net/CPS	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= <Primary CDP URL> [2]CRL Distribution Point Distribution Point Name: Full Name: URL=<Secondary CDP URL>	
Authority Information Access (non-critical)	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=<Primary AIA URL> [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=<Secondary AIA URL>	
Subject Alternate Name	DNS Name=Domain Name 1 DNS Name=Domain Name 2 DNS Name=Domain Name 3 ….up to DNS Name=Domain Name 100	
Thumbprint Algorithm	SHA1	
Thumbprint		

Code Signing Certificate		
Signature Algorithm	Sha1	
Issuer	CN	UTN-USERFirst-Object
	OU	http://www.usertrust.com
	O	The USERTRUST Network
	L	Salt Lake City
	S	UT

	C	US
Validity	1 Year / 2 Year / 3 Year	
Subject	CN	Common Name (name of subscriber)
	O	Organization
	OU	Organization Unit
	L	Locality
	STREET	Street
	S	State
	PostalCode	Zip or Postal Code
	C	Country
Authority Key Identifier	KeyID only.	
Key Usage (NonCritical)	Digital Signature , Key Encipherment(A0)	
Netscape Certificate Type	Signature (10)	
Extended Key Usage	Code Signing (1.3.6.1.5.5.7.3.3)	
Basic Constraint	Subject Type=End Entity Path Length Constraint=None	

Certificate Policies	[1]Certificate Policy:
	   Policy Identifier=1.3.6.1.4.1.6449.1.2.1.3.2
	    [1,1]Policy Qualifier Info:
	      Policy Qualifier Id=CPS
	      Qualifier:
	        http://www.positivessl.com/CPS	

CRL Distribution Policies	[1]CRL Distribution Point
	   Distribution Point Name:
	     Full Name:
	      URL=<Primary CDP URL>	

Subject Alternative Name	RFC822 Name = <Email Address>	
Thumbprint Algorithm	SHA1	
Thumbprint		

Content Verification Certificate		
Signature Algorithm	Sha1 / RSA	
Issuer	CN	Comodo Content Verification Services
	OU	http://crt.comodo.com/comodocontentverificationservices.crt
	O	Comodo CA Limited
	L	Salford
	S	Greater Manchester
	C	GB
Validity	30 days / 1 Year	
Subject	CN	
	O	
	OU	
	L	
	STREET	
	S	
	PostalCode	
	C	
Authority Key Identifier	KeyID only.	
Key Usage (Critical)	Digital Signature	
Netscape Certificate Type	Signature (10)	
Extended Key Usage	1.3.6.1.4.1.6449.1.3.1	
Basic Constraint	Subject Type=End Entity Path Length Constraint=None	

Certificate Policies	[1]Certificate Policy:
	    Policy Identifier=1.3.6.1.4.1.6449.1.2.1.3.2
	     [1,1]Policy Qualifier Info:
	       Policy Qualifier Id=CPS
	       Qualifier:
	          http://www.positivessl.com/CPS

CRL Distribution Policies	[1]CRL Distribution Point
	   Distribution Point Name:
	     Full Name:
	       URL=<Primary CDP URL>

Subject Alternative Name	RFC822 Name = <Email Address>
Thumbprint Algorithm	SHA1
Thumbprint	

Essential SSL Secure Server Certificate – Essential SSL / Essential SSL Wildcard / Essential SSL Trial		
Signature Algorithm	Sha1 / RSA	
Issuer	CN	Essential SSL
	O	Comodo CA Limited
	L	Salford
	S	Greater Manchester
	C	GB
Validity	1 Year / 2 Year / 3 year	
Subject	CN	<domain name>
	OU	Essential SSL
	OU	Domain Control Validated[1]
Authority Key Identifier	Key ID only.	
Key Usage (NonCritical)	Digital Signature , Key Encipherment (A0)	
Netscape Certificate Type	SSL Client Authentication, SSL Server Authentication (c0)	
Basic Constraint	Subject Type=End Entity Path Length Constraint=None	

Certificate Policies	[1]CRL Distribution Point
	   Distribution Point Name:
	     Full Name:
	       URL=<Primary CDP URL>
	[2]CRL Distribution Point
	   Distribution Point Name:
	     Full Name:
	       URL=<Secondary CDP URL>	

Authority Information Access	[1]Authority Info Access
	   Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)
	   Alternative Name:
	     URL=<Primary AIA URL>
	[2]Authority Info Access
	   Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)
	   Alternative Name:
	     URL=<Secondary AIA URL>	

Thumbprint Algorithm	SHA1	
Thumbprint		

Unified Communications Certificate		
Version	V3	
Serial Number	Serial Number of Certificate	
Signature Algorithm	Sha1RSA	
Issuer (option 1)	CN	Essential SSL
	O	Comodo CA Limited

	L	Salford
	S	Greater Manchester
	C	GB
Issuer (option 2)	CN	UTN – DATACorp SGC
	OU	http://www.usetrust.com
	O	The USERTRUST Network
	L	Salt Lake City
	S	UT
	C	US
Validity	1 Year, 2 Years, or 3 Years	
Subject	CN	<domain name>
	OU	Comodo Unified Communications
	O	<organization name>
	Street	<organization address>
	L	<organization city/locality>
	S	<organization state>
	PostalCode	<organization postal code>
	C	<organization country code>
Public Key	<Public Key of Certificate>	
Authority Key Identifier	KeyID only.	
Subject Key Identified	Subject Key ID	
Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	

Certificate Policies	[1]Certificate Policy:
	   Policy Identifier=1.3.6.1.4.1.6449.1.2.1.3.4
	    [1,1]Policy Qualifier Info:
	     Policy Qualifier Id=CPS
	     Qualifier:
	       https://secure.comodo.net/CPS	

CRL Distribution Policies	[1]CRL Distribution Point
	  Distribution Point Name:
	    Full Name:
	      URL=<primary CRL URL>
	[2]CRL Distribution Point
	  Distribution Point Name:
	    Full Name:
	      URL=<secondary CRL URL>	

Authority Information Access	[1]Authority Info Access
	  Access Method = On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)
	  Alternative Name:
	    URL=<OCSP URL>	

Subject Alternative Name	DNS Name = <domain name> (up to 100 DNS listings>	
Key Usage (NonCritical)	Digital Signature , Key Encipherment (a0)	
Thumbprint Algorithm	sha1	
Thumbprint		

Intel Pro SSL		
Signature Algorithm	Sha1	
Issuer	CN	Intel Pro SSL
	O	Comodo CA Limited
	L	Salford
	S	Greater Manchester
	C	GB
Validity	1 -5 Years	
Subject	CN	<domain name>
	OU	Instant DV SSL
	OU	Domain Control Validated[1]
Authority Key Identifier	KeyID only.	
Key Usage (NonCritical)	Digital Signature , Key Encipherment(A0)	

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:
	    Policy Identifier=1.3.6.1.4.1.6449.1.2.2.7
	        [1,1]Policy Qualifier Info:
	            Policy Qualifier Id=CPS
	            Qualifier:
	                http://www.comodogroup.com/respository/CPS

CRL Distribution Policies	[1]CRL Distribution Point
	    Distribution Point Name:
	        Full Name:
	            URL=<Primary CDP URL>
	[2]CRL Distribution Point
	    Distribution Point Name:
	        Full Name:
	            URL=<Secondary CDP URL>

Authority Information Access	[1]Authority Info Access
	    Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)
	    Alternative Name:
	        URL=<Primary AIA URL>
	[2]Authority Info Access
	    Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)
	    Alternative Name:
	        URL=<Secondary AIA URL>

Thumbprint Algorithm	SHA1
Thumbprint	

Educational Certificates		
Signature Algorithm	Sha1	
Issuer (Option 1)	CN	UTN-USERFIRST-Hardware
	OU	http://www.usertrust.com
	O	The USERTRUST Network
	L	Salt Lake City
	S	UT
	C	US
Issuer (Option 2)	CN	UTN – DATACorp SGC
	OU	http://www.usertrust.com
	O	The USERTRUST Network
	L	Salt Lake City
	S	UT
	C	US
Validity	1 Year / 2 Year / 3 Year / 4 Year / 5 Year	
Subject	CN	Common Name
	OU	Educational Certificate
	OU	NOT FOR TRANSACTION OF MONEY
	O	Organization
	OU	Organization Unit (optional)
	L	Locality (optional)
	Street	Street (optional)
	S	State (optional)
	Postal Code	Zip or Postal Code (optional)
	C	Country
Authority Key Identifier	KeyID only is specified.	
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 = 1.3.6.1.4.1.6449.1.2.1.3.4
	  [1,1]Policy Qualifier Info:
	    Policy Qualifier Id = CPS
	  Qualifier:
	https://secure.comodo.net/CPS

Subject Alternative Name	Up to 100 Domain Names

Authority Information Access	1]Authority Info Access
	   Access Method = id-ad-caIssuers (1.3.6.1.5.5.7.48.2)
	   URL=<Primary AIA URL>
	[2]Authority Info Access
	   Access Method = id-ad-ocsp (1.3.6.1.5.5.7.48.1)
	   URL = http://ocsp.comodoca.com

CRL Distribution Policies	[1]CRL Distribution Point
	   Distribution Point Name:
	     Full Name:
	      URL=<Primary CDP URL>
	[2]CRL Distribution Point
	   Distribution Point Name:
	     Full Name:
	      URL=<Secondary CDP URL>

Thumbprint Algorithm	SHA1
Thumbprint	

IGTF Certificate		
Signature Algorithm	Sha1	
Issuer (Option 1)	CN	UTN-USERFIRST-Hardware
	OU	http://www.usertrust.com
	O	The USERTRUST Network
	L	Salt Lake City
	S	UT
	C	US
Issuer (Option 2)	CN	UTN – DATACorp SGC
	OU	http://www.usertrust.com
	O	The USERTRUST Network
	L	Salt Lake City
	S	UT
	C	US
Validity	13 Months	
Subject	DC	Type of Authenticating Organization
	DC	Name of Authenticating Organization
	DC	Unit of Authenticating Organization
	CN	Common Name
	OU	IGTF Certificate
	OU	NOT FOR TRANSACTIONS OF MONEY
	O	Organization
	L	Locality (optional)
	Street	Street (optional)
	S	State (optional)
	Postal Code	Zip or Postal Code (optional)
	C	Country
Authority Key Identifier	KeyID only is specified.	
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 = 1.3.6.1.4.1.6449.1.2.1.3.4
	[1,1]Policy Qualifier Info:
	Policy Qualifier Id = CPS
	Qualifier:
	https://secure.comodo.net/CPS
	[2} Certificate Policy:
	1.2.840.113612.5.2.2.1
Subject Alternative Name	Up to 100 Domain Names
Authority Information Access	1]Authority Info Access
	Access Method = id-ad-caIssuers (1.3.6.1.5.5.7.48.2)
	URL=<Primary AIA URL>
	[2]Authority Info Access
	Access Method = id-ad-ocsp (1.3.6.1.5.5.7.48.1)
	URL = http://ocsp.comodoca.com
CRL Distribution Policies	[1]CRL Distribution Point
	Distribution Point Name:
	Full Name:
	URL=<Primary CDP URL>
	[2]CRL Distribution Point
	Distribution Point Name:
	Full Name:
	URL=<Secondary CDP URL>
Thumbprint Algorithm	SHA1
Thumbprint	

ComodoSSL Certificates		
Signature Algorithm	Sha1	
Issuer (Option 1)	CN	COMODO SSL CA
	O	COMODO CA Limited
	L	Salford
	S	Greater Manchester
	C	GB
Validity	1 month thru 60 months	
	CN	Common Name (domain name)
	OU	COMODO SSL
	OU	Domain Control Validated
Authority Key Identifier	KeyID only is specified.	
Key Usage (Critical)	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)	
Basic Constraint	Subject Type = End Entity	
	Path Length Constraint = None	
Certificate Policies	[1] Certificate Policy:	
	PolicyIdentifier = 1.3.6.1.4.1.6449.1.2.2.7.	
	[1,1]Policy Qualifier Info:	
	Policy Qualifier Id = CPS	
	Qualifier:	
	https://secure.comodo.com/CPS	
Subject Alternative Name	Up to 200 Domain Names	
Authority Information Access	1]Authority Info Access	
	Access Method = id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	
	Alternative Name:	
	URL=http://crt.comodoca.com/COMODOSSLCA.crt	
	[2]Authority Info Access	
	Access Method = id-ad-ocsp (1.3.6.1.5.5.7.48.1)	
	URL = http://ocsp.comodoca.com	

CRL Distribution Policies	[1]CRL Distribution Point
	   Distribution Point Name:
	     Full Name:
	       URL=http://crt.comodoca.com/COMODOSSLCA.crl	

Thumbprint Algorithm	SHA1	
Thumbprint		

2.13 Comodo Certificate Revocation List Profile

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

Version	[Version 1]	
Issuer Name	CountryName = [Root Certificate Country Name], OrganizationName=[Root Certificate Organization], CommonName=[Root Certificate Common Name] [UTF8String encoding]	
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 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 CPS

Comodo conforms to this 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 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 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 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 the Reseller Partner agreements, Web Host Reseller Partner agreements, EPKI Manager Account Holder agreement, Powered SSL Partner agreement, 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 CPS.

3.4 Records Retention Period

Comodo retains the records of Comodo digital certificates and the associated documentation for a term of than 7 years, or as necessary to comply with applicable laws. The retention term begins on the date of expiration or revocation. Copies of certificates are held, regardless of their status (such as expired or revoked). Such records may be retained in electronic, in paper-based format or any other format that Comodo may see fit.

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, Comodo maintains electronic or manual logs of the following events for core functions. 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.

All logs include the following elements:

- Date and time of entry
- Serial or sequence number of entry
- Method of entry
- Source of entry
- Identity of entity making log entry

3.5.1 CA & Certificate Lifecycle Management

- CA Root signing key functions, including key generation, backup, recovery and destruction
- Subscriber certificate life cycle management, including successful and unsuccessful certificate applications, certificate issuances, certificate re-issuances and certificate renewals
- Subscriber certificate revocation requests, including revocation reason
- Subscriber changes of affiliation that would invalidate the validity of an existing certificate
- Certificate Revocation List updates, generations and issuances
- Custody of keys and of devices and media holding keys
- Compromise of a private key

3.5.2 Security Related Events

- System downtime, software crashes and hardware failures

- CA system actions performed by Comodo personnel, including software updates, hardware replacements and upgrades
- Cryptographic hardware security module events, such as usage, de-installation, service or repair and retirement
- Successful and unsuccessful Comodo PKI access attempts
- Secure CA facility visitor entry and exit

3.5.3 Certificate Application Information

- The documentation and other related information presented by the applicant as part of the application validation process
- Storage locations, whether physical or electronic, of presented documents

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.

- 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 the CA, and allows us to specify a maximum system outage time (in case of critical systems failure) of 1 hour.
- Backup of critical CA software is performed weekly and is stored offsite.
- Backup of critical business information is performed daily and is stored offsite.
- Comodo operations are distributed across several sites worldwide. 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 CPS) for a period of 7 years or longer if applicable. For Code Signing Certificates revoked due to key compromise or that have been issued to unauthorized persons, Comodo will maintain certificate information on CRLs for at least 20 years.

Comodo also publishes certificate status information using Online Certificate Status Protocol (OCSP). Comodo's OCSP responders are capable of providing a 'good' or 'revoked' status for all certificates issued under the terms of this CPS. In the case of Code Signing Certificates only, the OCSP responders will continue to give a 'good' status for unrevoked certificates even after their expiry – for at least 20 years from issuance. In the case of all other certificate types the OCSP responders will give an 'unknown' response for expired certificates.

3.8 Publication of Critical Information

Comodo publishes this CPS, certificate terms and conditions, the relying party agreement and copies of all subscriber agreements in the official Comodo repository at www.comodogroup.com/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 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 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 Types of 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. Subscriber application data marked as "Public" in the relevant subscriber agreement and submitted as part of a certificate application is published within an issued digital certificate in accordance with section 2.12.4 of this CPS.

3.9.3 Access to Confidential Information

All personnel in trusted positions 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 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.

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.

3.10.2 Personnel controls

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.

3.11 Privacy Policy

Comodo has implemented a privacy policy, which complies with this CPS. The Comodo privacy policy is published at the Comodo repository at www.comodogroup.com/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

All 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 or Dual Use certificates)
- Make all reasonable efforts to protect the integrity the private key half of the key pair
- Submit to Comodo a certificate application, including application information as detailed in this 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. The following table details the entity(s) involved in the processing of certificate applications. Comodo issues all certificates regardless of the processing entity.

Certificate Type	Enrolment Entity	Processing Entity	Issuing Authority
Secure Server Certificate - *all types as per section 2.4.1 of this CPS*	End Entity Subscriber	Comodo	Comodo
Secure Server Certificate - *all types as per section 2.4.1 of this CPS*	Web Host Reseller on behalf of End Entity Subscriber	Web Host Reseller	Comodo
Personal Secure Email Certificate	End Entity Subscriber	Comodo	Comodo
Corporate Secure Email Certificate	End Entity Subscriber	EPKI Manager Account Holder	Comodo
Comodo TF Certificate	End User Subscriber	Financial Institution	Comodo
Content Verification Certificate	End Entity Subscriber	Comodo	Comodo
Code Signing Certificate	End Entity Subscriber	Comodo	Comodo

Comodo Dual Use Certificate	End User or Administrator of Subscriber	Subscriber	Comodo

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 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 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 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. Validation for adding domains to the EPKI Manager account may occur solely using a domain authorization letter.

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 a Certificate or issuing a Site Seal, Comodo employs controls to validate the identity of the subscriber information featured in the certificate application. Such controls are indicative of the product type:

4.2.1 Secure Server Certificates Validation Process

Comodo utilizes a two-step validation process prior to the issuance of a Secure Server Certificate, or three-step process prior to issuing a Code Signing Certificate.

This process involves Comodo, automatically or manually, reviewing the application information provided by the applicant (as per section 4.3 of this CPS) for the following :

1. That the applicant has the right to use the domain name in the application (or, in the case of Code Signing Certificates, the domain name used in the application email address, i.e., for email address someone@example.com, applicant must demonstrate exclusive control of example.com), which is validated by:

    i. Reviewing domain name ownership records available publicly through Internet or approved global domain name registrars, or
    ii. For government and educational institution associated with a .EDU or .GOB domain only, receiving a letter on official departmental letterhead, with the order details and a statement verifying that the signor (which must be a WHOIS contact or senior member of management) is authorized to act on behalf of the organization.
    iii. Validation may also be supplemented: (1) by sending an email to a generic address only available to the person(s) controlling the domain name administration, e.g., webmaster@example.com, postmaster@example.com, admin@example.com, etc. or (2) direct communication with the administrator associated with the domain name register record.

2. To authenticate the identity of the certificate requestor, which is done by one of the following:

    i. For organization entities, identity is authenticated by using at least one third party database or service, or organizational documentation filed or issued with a government agency or competent authority, or
    ii. For non-organization individuals, identity is authenticated by documentation such as a bank statement, passport, driving license, or other such documents.

3. When validating Code Signing Certificates, the applicant will be contacted at a verified telephone number to confirm that the applicant requested the Certificate, and in the case of organizations, that the person submitting the application on behalf of that organization is authorized to do so. Telephone numbers are verified through third party databases or submission of a telephone bill under the name and address of the applicant to confirm the number.

The above assertions are reviewed through an automated process, manual review of supporting documentation and reference to third party official databases.

4.2.2 PositiveSSL / PositiveSSL Wildcard / PositiveSSL Trial / OptimumSSL / OptimumSSL Wildcard / Comodo Multi-Domain / Instant DV SSL / Instant DV SSL Wildcard / Instant DV SSL Trial / Intel Pro SSL / Unified Communications / ComodoSSL

To validate these 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

1. Reviewing domain name ownership records publicly available through Internet approved global domain registrars and using generic e-mails which ordinarily are only available to person(s) controlling the domain name administration, for example, webmaster@ . . ., postmaster@ . . ., admin@; or

2. Requesting documentation that verifies control of the domain.

In addition, Comodo at its discretion may establish domain control by utilizing third party domain name registrars and directories, by verifying control of the domain by practical demonstration of the control of the domain, by implementing further validation processes including out of bands validation of the applicant's submitted information, or by relying on the accuracy of the applicant's application and the representations made in the subscriber agreement.

4.2.3 InstantSSL / Trial SSL / Content Verification Certificates

Comodo operates a website identity assurance database referred to as IdAuthority. The database contains pre-validated identification records for known domain names and uses automated algorithms to marry domain name ownership records (from global domain name registrars) with company ownership identification records (from official government and third party company information sources).

If IdAuthority contains sufficient pre-validated records for the domain name used in an application, Comodo may employ the data held by IdAuthority to expedite the validation process. If application data matches the records held by IdAuthority, manual validation intervention is not required. In the event that the application data does not match the prevalidated records, the application is processed manually by a Comodo validation officer in accordance with the two-step process outlined in section 4.2.1 of this CPS.

4.2.4 InstantSSL / ProSSL / PremiumSSL / PremiumSSL Wildcard / EliteSSL /GoldSSL / PlatinumSSL / PlatinumSSL Wildcard / PremiumSSL Legacy / PremiumSSL Legacy Wildcard / PlatinumSSL Legacy / PlatinumSSL Legacy Wildcard / PlatinumSSL SGC Legacy / PlatinumSSL SGC Legacy Wildcard / Comodo SGC SSL / Comodo SGC SSL Wildcard / Educational Certificate / IGTF Certificate

These certificates are processed by a Comodo validation officer in accordance with the process outlined in section 4.2.1 of this CPS. Comodo may employ the data held by IdAuthority to expedite the validation process. If application data matches the records held by IdAuthority, manual validation intervention is not required. In the event that the application data does not match the pre-validated records, the application is processed manually by a Comodo validation officer in accordance with the process outlined in section 4.2.1 of this CPS.

4.2.5 Intranet SSL

Intranet certificate applications are only accepted for servers on internal networks, which are defined as non-Fully Qualified Domain Names and non-public IP addresses. During the application process Comodo verifies in real time that the common name (server name) submitted in the application is neither a Domain Name nor a publicly available IP address. Upon successful verification that the Intranet certificate cannot be used publicly on the Internet, the certificate will be issued.

Comodo validates that an Intranet certificate cannot be used as a public certificate. As the Intranet certificate is restricted for use only within a closed network, the company identity associated with the certificate need not, nor is, validated.

4.2.6 Personal Secure Email Certificate

The Personal Secure Email Certificate is *persona non-validated*. Comodo only validates the right for the applicant to use the submitted email address. This is achieved through the delivery via email of unique login details to online certificate collection facilities hosted by Comodo. The login details are sent via email to the address submitted during the certificate application.

Once logged into the online certificate collection facilities and prior to the installation of the Personal Secure Email Certificate, Comodo validates using an automated cryptographic challenge that the applicant holds the private key associated with the public key submitted during the application process. If the automated challenge is successful, Comodo will release the digital certificate to the subscriber.

4.2.7 Corporate Secure Email Certificate

Corporate Secure Email Certificates are only available through the EPKI Manager and will only be issued to email addresses within approved domain names. The EPKI Manager Account Holder must first submit a domain name to Comodo and appropriate domain name ownership, or right to use a domain name, validation takes place in accordance with 4.2.1 of this CPS except that a domain authorization letter may be used in substitution of any domain ownership validation. Upon successful validation of a submitted domain name or receipt of domain authorization letter, Comodo allows the EPKI Manager Account Holder to utilize email addresses within the domain name.

The EPKI Manager nominated administrator applies for Corporate Secure Email Certificates. The administrator will submit the secure email certificate end-entity information on behalf of the end-entity. An email is then delivered to the end-entity containing unique login details to online certificate generation and collection facilities hosted by Comodo. Once logged into the online certificate generation and collection facilities, the end-entity's browser creates a public and private key pair. The public key is submitted to Comodo who will issue a Corporate Secure Email Certificate containing the public key. Comodo then validates using an automated cryptographic challenge that the applicant holds the private key associated with the public key submitted during this automated application process. If the automated challenge is successful, Comodo will release the digital certificate to the end-entity subscriber.

4.2.8 Code Signing Certificate / Time Stamping Certificate

Code Signing Certificates and Time Stamping Certificates are processed by a Comodo validation officer in accordance with the process outlined in section 4.2.1 of this CPS.

4.2.9 Comodo TF

Validation procedures of applicants for Comodo TF Certificates are performed by approved financial institutions validating the subscriber's existing online account username and password.

4.2.10 [Reserved]

4.2.11 Custom Client Certificates

Comodo Custom Client Certificates may receive one of the following levels of verification:

- Persona non validated: No identity validation is performed. The subscriber may be required to show their access to an email address identified in the certificate. Persona non validated is further described in 4.2.6.
- Domain validation: The subscriber's must demonstrate their access to a domain name specified in the certificate. Domain validation is further described in Section 4.2.2
- Identity validation: Information about an entity's identity is verified as described in Section 4.2.4. For individuals this might include requiring the individual to appear before the CA, an agent of the CA, or a notary or similar official. The official must check the identity of the subscriber against recognized government identification.

Custom Client Certificates issued from partners are validated in accordance with the validation procedures set by the partner. Interested parties are directed to the partner for full information on the validation of their custom client certificates.

4.2.12 Comodo Dual Use Certificates

Validation procedures of applicants for Comodo Dual Use Certificates are performed by Comodo or an RA. Authentication is based on the physical presence of the Applicant before an agent of the CA or RA or before a notary or other official with comparable authority. The agent, notary, or other official is responsible for checking the identity of the Applicant. An RA may issue the Certificate to its own employees and users if the organization authenticates the employment of the employee and the employee's authorization to obtain a Certificate. Verification by Comodo is based on the confirmation of the identity of the Applicant in connection with their Application.

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

The following elements are critical information elements for a Comodo certificate issued to an Organization. Those elements marked with PUBLIC are present within an issued certificate and are therefore within the public domain. Those elements not marked with PUBLIC remain confidential in line with the privacy and protection of data provisions outlined in this CPS.

- Legal Name of the Organization (PUBLIC)
- Organizational unit (PUBLIC)
- Street, city, postal/zip code, country (PUBLIC)
- VAT-number (if applicable)
- Company / DUNS number (if available)
- Server Software Identification
- Payment Information
- Administrator contact full name, email address and telephone

- Billing contact persons and organizational representative
- Fully Qualified Domain Name / Network Server Name / Public or Private IP (PUBLIC)
- Public Key (PUBLIC)
- Proof of right to use name
- Proof of existence and organizational status of the Organization
- Subscriber agreement, signed (if applying out of bands)

4.3.2 Supporting Documentation for Organizational Applicants

Documentation requirements for Organizational applicants include any / all of the following:

- Articles of Association
- Business License
- Certificate of Compliance
- Certificate of Incorporation
- Certificate of Authority to Transact Business
- Tax Certification
- Corporate Charter
- Official letter from an authorized representative of a government organization
- Official letter from office of Dean or Principal (for Educational Institutions)

Comodo may accept at its discretion other official organizational documentation supporting an application.

4.3.3 Application Information for Individual Applicants

The following elements are critical information elements for a Comodo certificate issued to an individual:

- Legal Name of the Individual (PUBLIC)
- Organizational unit (PUBLIC)
- Street, city, postal/zip code, country (PUBLIC)
- VAT-number (if applicable)
- Server Software Identification
- Payment Information
- Administrator contact full name, email address and telephone
- Billing contact persons and organizational representative
- Fully Qualified Domain Name / Network Server Name / Public or Private IP (PUBLIC)
- Public Key (PUBLIC)
- Proof of right to use name
- Proof of existence and organizational status of the Organization
- Subscriber agreement, signed (if applying out of bands)

4.3.4 Supporting Documentation for Individual Applicants

Documentation requirements for Individual applicants shall include identification elements such as:

- Passport
- Driving License
- Bank statement

Comodo may accept at its discretion other official documentation supporting an application.

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:

- The certificate applicant is the same person as the person identified in the certificate request.
- The certificate applicant holds the private key corresponding to the public key to be included in the certificate.
- The information to be published in the certificate is accurate, except for non-verified subscriber information.
- Any agents who apply for a certificate listing the certificate applicant's public key are duly authorized to do so.

In all types of Comodo 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 Third-Party Confirmation of Business Entity Information

Comodo may use the services of a third party to confirm information on a business entity that applies for a digital certificate. Comodo accepts confirmation from third party organizations, other third party databases and government entities.

Comodo's controls may also include Trade Registry transcripts that confirm the registration of the applicant company and state the members of the board, the management and Directors representing the company.

Comodo may use any means of communication at its disposal to ascertain the identity of an organizational or individual applicant. Comodo reserves right of refusal in its absolute discretion.

4.4.2 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.

Comodo assures that all certificates will be issued within 2 working days after the receipt of all required validation information as per this CPS.

4.6 Approval and Rejection of Certificate Applications

Following successful completion of all required validations of a certificate application Comodo approves 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 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. 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. Comodo verifies all information that is included in SSL certificates at time intervals of thirty-nine months or less.

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 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 CPS and within the relying party agreement. If the circumstances of reliance exceed the assurances delivered by Comodo under the provisions made in this 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

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 if any of the following occur:

- There has been loss, theft, modification, unauthorized disclosure, or other compromise of the private key associated with the certificate;
- The Subscriber or Comodo has breached a material obligation under this CPS or the relevant Subscriber Agreement;
- Either the Subscriber's or Comodo's obligations under this 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;
- There has been a modification of the information pertaining to the Subscriber that is contained within the certificate;
- 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;
- A Subscriber's Digital Certificate has not been issued in accordance with the policies set out in this CPS;
- The subscriber 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;
- The certificate was issued to persons or entities identified as publishers of malicious software or that impersonated other persons or entities;
- The certificate was issued as a result of fraud or negligence; or
- The certificate, if not revoked, will compromise the trust status of Comodo.

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 or individual entity that has made the certificate application.
- Made by the RA on behalf of the organization or individual 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 either / or 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 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 sometime 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. In addition, Comodo's systems are configured to pre-generate OCSP responses using the private key of the certificate. This provides real-time information regarding the validity of the Certificate making the revocation information immediately available through the OCSP.

4.14 Renewal

Depending on the option selected during application, the validity period of Comodo certificates is 1, 2 or 3 years from the date of issuance and is detailed in the relevant field within the certificate.

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 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 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 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 CPS. Comodo cannot warrant that such user software will support and enforce controls required by Comodo, whilst 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 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 or using the Comodo OCSP responder. 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, assume in whole.

By means of this CPS, Comodo has adequately informed relying parties on the usage and validation of digital signatures through this CPS and other documentation published in its public repository available at www.comodogroup.com/repository or by contacting via out of bands means via the contact address as specified in the Document Control section of this 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 CPS, subscribers shall exclusively be responsible:

- To minimize internal risk of private key compromise by ensuring adequate knowledge and training on PKI is provided internally.
- To generate their own private / public key pair to be used in association with the certificate request submitted to Comodo or a Comodo RA.
- Ensure that the public key submitted to Comodo or a Comodo RA corresponds with the private key used.
- Ensure that the public key submitted to Comodo or a Comodo RA is the correct one.
- Provide correct and accurate information in its communications with Comodo or a Comodo RA.
- Alert Comodo or a Comodo RA if at any stage whilst the certificate is valid, any information originally submitted has changed since it had been submitted to Comodo.
- Generate a new, secure key pair to be used in association with a certificate that it requests from Comodo or a Comodo RA.
- Read, understand and agree with all terms and conditions in this Comodo CPS and associated policies published in the Comodo Repository at www.comodogroup.com/repository.
- Refrain from tampering with a Comodo certificate.
- Use Comodo certificates for legal and authorized purposes in accordance with the suggested usages and practices in this CPS.
- Cease using a Comodo certificate if any information in it becomes misleading obsolete or invalid.
- Cease using a Comodo certificate if such certificate is expired and remove it from any applications and/or devices it has been installed on.
- 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.
- 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.
- Request the revocation of a certificate in case of an occurrence that materially affects the integrity of a Comodo certificate.

- For acts and omissions of partners and agents, they use to generate, retain, escrow, or destroy their private keys.

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:

- 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.
- No unauthorized person has ever had access to the subscriber's private key.
- All representations made by the subscriber to Comodo regarding the information contained in the certificate are accurate and true.
- All information contained in the certificate is accurate and true to the best of the subscriber's knowledge or to the extent that the subscriber had notice of such information whilst the subscriber shall act promptly to notify Comodo of any material inaccuracies in such information.
- The certificate is used exclusively for authorized and legal purposes, consistent with this CPS.
- It will use a Comodo certificate only in conjunction with the entity named in the organization field of a digital certificate (if applicable).
- 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.
- 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.
- The subscriber agrees with the terms and conditions of this CPS and other agreements and policy statements of Comodo.
- The subscriber abides by the laws applicable in his/her country or territory including those related to intellectual property protection, viruses, accessing computer systems etc.
- The subscriber complies with all export laws and regulations for dual usage goods as may be applicable.

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 the CA, 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 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 CPS.
- Perform all verification actions prescribed by the Comodo validation procedures and this CPS.
- Receive, verify and relay to Comodo all requests for revocation of a Comodo certificate in accordance with the Comodo revocation procedures and the 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 CPS and relying party agreement.
- Verify a Comodo certificate by referring to the relevant CRL and the CRLs of intermediate CA and root CA or by checking the OCSP response using the Comodo OCSP responder.
- 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 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 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 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 (www.comodogroup.com/repository) and official web site(s) agree with the provisions of this CPS and any other conditions of usage that Comodo may make available. Parties demonstrate acceptance of the conditions of usage of the 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 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 CPS, Comodo promises to:

- Comply with this 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 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 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 CPS.
- Publish accepted certificates in accordance with this CPS.
- Provide support to subscribers and relying parties as described in this CPS.
- Revoke certificates according to this CPS.
- Provide for the expiration and renewal of certificates according to this CPS.
- Make available a copy of this 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 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 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 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 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 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 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 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 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

If Comodo was negligent in issuing a digital certificate that resulted in a loss to a Relying Party, Relying Party may be eligible under Comodo's certificate warranty to receive up to the Maximum Certificate Coverage per incident, subject to the Total Payment Limit shown in Table 5.31 below 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. The Maximum Certificate Coverage of Comodo to all applicants, subscribers and relying parties for each certificate is set forth in Table 5.31 below. Under Comodo's warranty a covered person may only receive a payment in accordance with the Maximum Certificate Coverage set forth in Table 5.31 per online transaction 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 in accordance with the Maximum Certificate Coverage set forth in Table 5.31 per Incident. Any payments to Covered Persons shall be limited by the Total Payment Limit for any claims relating to that Digital Certificate. For example, if a Digital Certificate carries a Total Payment Limit of $10,000, then Covered Persons can receive payments in accordance with this warranty for up to the Maximum Certificate Coverage 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.

Table 5.31

Comodo Certificate Type	Max Transaction Value	Cumulative Max Liability
ComodoSSL	$10,000	$250,000
ComodoSSL Wildcard	$10,000	$250,000
PositiveSSL Certificate	$1,000	$10,000
PositiveSSL Wildcard Certificate	$1,000	$10,000
PositiveSSL Trial Certificate	$1,000	$10,000
PositiveSSL Multi-Domain Certificate	$0	$0
OptimumSSL Certificate	$0	$0
OptimumSSL Wildcard Certificate	$0	$0
Comodo IntranetSSL Certificate	$0	$0
Comodo TrialSSL Certificate	$0	$0
Comodo InstantSSL Certificate	$5,000	$50,000
Comodo InstantSSL Pro Certificate	$10,000	$100,000

Comodo PremiumSSL Certificate	$10,000	$250,000
Comodo PremiumSSL Wildcard Certificate	$10,000	$250,000
Comodo SGC SSL Certificate	$10,000	$250,000
Comodo SGC SSL Wildcard Certificate	$10,000	$250,000
Comodo Multi-Domain Certificate	$0	$0
Comodo PremiumSSL Legacy Certificate	$10,000	$250,000
Comodo PremiumSSL Legacy Wildcard Certificate	$10,000	$250,000
EliteSSL Certificate	$10,000	$500,000
GoldSSL Certificate	$10,000	$750,000
PlatinumSSL Certificate	$10,000	$1,000,000
PlatinumSSL Wildcard Certificate	$10,000	$1,000,000
PlatinumSSL SGC Certificate	$10,000	$1,000,000
PlatinumSSL SGC Wildcard Certificate	$10,000	$1,000,000
PlatinumSSL Legacy Certificate	$10,000	$1,000,000
PlatinumSSL Legacy Wildcard Certificate	$10,000	$1,000,000
EV SSL Certificate	$10,000	$250,000
EV SSL SGC Certificate	$10,000	$250,000
EV Multi-Domain Certificate	$10,000	$250,000
Personal Secure Email Certificate	$0	$0
Corporate Secure Email Certificate	$0	$0
Code Signing Certificate	$0	$50,000
Time Stamping Certificate	$0	$0
Comodo TF Certificate	$0	$0
Content Verification Certificate	$0	$0
Trial Payment Credential CVC	$0	$0
Payment Credential CVC (1 logo)	$0	$0
Payment Credential CVC (3 logos)	$0	$0
Payment Credential CVC (Wildcard)	$0	$0
Essential SSL Certificate	$1,000	$10,000
Essential SSL Wildcard Certificate	$1,000	$10,000
Essential SSL Trial Certificate	$1,000	$10,000
Unified Communications Certificate	$0	$0
Intel Pro SSL Certificate	$0	$0
Comodo Dual Use Certificate	$0	$0
Education Certificate	$0	$0
IGTF Certificate	$0	$0

5.32 Financial Limitations on Certificate Usage

Comodo certificates may only be used in connection with data transfer and transactions completed using a credit card and having a US dollar (US$) value no greater than the max

transaction value associated with the certificate and detailed in the table in section 5.31 of this CPS.

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 CPS.

5.34 Conflict of Rules

When this CPS conflicts with other rules, guidelines, or contracts, this CPS, dated 3 February 2005, 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 CPS.
- Expressly superseding this 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 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 CPS is governed by, and construed in accordance with English law. This choice of law is made to ensure uniform interpretation of this 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 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 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 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 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 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 CPS or the application thereof, is for any reason and to any extent found to be invalid or unenforceable, the remainder of this CPS (and the application of the invalid or unenforceable provision to other persons or circumstances) shall be interpreted in such manner as to affect the original intention of the parties.

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

5.43 Interpretation

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

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

5.44 No Waiver

This CPS shall be enforced as a whole, whilst failure by any person to enforce any provision of this 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 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 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 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,and www.enterprisessl.com).

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 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 and S/MIME technology for secure online transactions and secure email respectively. Prior to the issuance of a certificate Comodo will validate an application in accordance with this CPS which may involve the request by Comodo to the applicant for relevant official documentation supporting the application.

Comodo certificates are issued to organizations or individuals.

The validity period of Comodo certificates varies dependent on the certificate type, but typically, a certificate will be valid for either 1 year, 2 years or 3 years. 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.

6.3.2 Secure Email Certificates

- Applicant's e-mail address.
- Applicant's name.
- Code of applicant's country.
- Organization name, organizational unit name, street address, city, state.
- Applicant's public key.
- Issuing certification authority (Comodo).
- 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. Upon the receipt of the necessary details and / or documentation, Comodo aims to confirm submitted application data and to complete the validation process and issue / reject a certificate application within 2 working days.

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 using third party databases and Government records
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 CPS and the official Comodo websites.
h) Revocation is conducted as per the procedures outlined in this CPS.

Document Control

This document is version 4.0 of the Comodo CPS, created and published on 1 July 2012 and signed off by the Comodo Certificate Policy Authority

Certificate Policy Authority
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

Copyright Comodo CA Limited 2012. All rights reserved.

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

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

Comodo ® is a registered trademark of Comodo CA Limited, Comodo Security Solutions, Inc. and Comodo Group, Inc.