

Comodo Certification Practice Statement

Incorporating Registry Services Corporation Certification Practise
Statement

Comodo Group

Version
27 May 2004

New Court, Regents Place, Regent Road,
Manchester M5 4HB United Kingdom,

v06032004

Tel: +44 (0) 161 874 7070
Fax: +44 (0) 161 877 1767
www.comodogroup.com

1	General	9
1.1	<i>Comodo</i>	9
1.2	<i>Registry Services Corporation.....</i>	9
1.3	<i>Comodo CPS</i>	9
1.4	<i>RegistryPro CPS.....</i>	10
1.5	<i>CPS Suitability, Amendments and Publication.....</i>	10
1.6	<i>Other Practice Statements & Agreements</i>	11
1.7	<i>Liability of Comodo and RegistryPro.....</i>	11
1.8	<i>Compliance with applicable standards.....</i>	11
1.9	<i>Digital Certificate Policy Overview</i>	12
1.10	<i>RegistryPro PKI Hierarchy.....</i>	12
1.11	<i>RegistryPro Certification Authority</i>	12
1.12	<i>Comodo PKI Hierarchy.....</i>	13
1.12.1	<i>Trial and 1 year certificates</i>	13
1.12.2	<i>2 and 3 year certificates</i>	13
1.13	<i>Comodo Certification Authority</i>	13
1.14	<i>RegistryPro Registration Authorities</i>	14
1.15	<i>Comodo Registration Authorities</i>	14
1.16	<i>Subscribers</i>	15
1.17	<i>Relying Parties</i>	15
2	Technology	15
2.1	<i>Comodo/RegistryPro CA Infrastructure.....</i>	15
2.1.1	<i>Root CA Signing Key Protection & Recovery</i>	15
2.1.2	<i>CA Root Signing Key Generation Process</i>	17
2.1.3	<i>CA Root Signing Key Archival.....</i>	18
2.1.4	<i>Procedures employed for CA Root Signing Key Changeover.....</i>	18
2.1.5	<i>CA Root Public Key Delivery to Subscribers.....</i>	18
2.1.6	<i>Physical CA Operations.....</i>	18
2.2	<i>Digital Certificate Management.....</i>	19
2.3	<i>Comodo Directories, Repository and Certificate Revocation List.....</i>	19
2.4	<i>RegistryPro Directories, Repository and Certificate Revocation List.....</i>	20
2.5	<i>Types of RegistryPro Certificates.....</i>	20
2.5.1	<i>RegistryPro Secure Server Certificate</i>	20
2.5.2	<i>RegistryPro Secure Email Certificates</i>	21
2.6	<i>Extensions and Naming</i>	21
2.6.1	<i>Digital Certificate Extensions.....</i>	21
2.6.2	<i>Incorporation by Reference for Extensions and Enhanced Naming</i>	21
2.7	<i>Subscriber Private Key Generation Process</i>	21
2.8	<i>Subscriber Private Key Protection and Backup</i>	21
2.9	<i>Subscriber Public Key Delivery to Comodo or RegistryPro</i>	22

2.10	<i>Delivery of Issued Subscriber Certificate to Subscriber</i>	22
2.10.1	Secure Server Certificate: ProSSL product type.....	22
2.10.2	Secure Email Certificate: ProCert product type.....	22
2.11	<i>RegistryPro Certificates Profile</i>	22
2.11.1	Key Usage extension field	22
2.11.2	Extension Criticality Field.....	23
2.11.3	Basic Constraints Extension	23
2.11.4	Certificate Policy (CP).....	23
2.12	<i>Comodo Certificates Profile</i>	25
2.12.1	Key Usage extension field	25
2.12.2	Extension Criticality Field.....	26
2.12.3	Basic Constraints Extension	26
2.12.4	Certificate Policy (CP).....	26
2.13	<i>RegistryPro Certificate Revocation List Profile</i>	32
2.14	<i>Comodo Certificate Revocation List Profile</i>	33
3	Organization	34
3.1	<i>Conformance to this CPS</i>	34
3.2	<i>Termination of CA Operations</i>	34
3.3	<i>Form of Records</i>	34
3.4	<i>Records Retention Period</i>	35
3.5	<i>Logs for Core Functions</i>	35
3.5.1	CA & Certificate Lifecycle Management.....	35
3.5.2	Security Related Events.....	36
3.5.3	Certificate Application Information.....	36
3.5.4	Log Retention Period.....	36
3.6	<i>Business Continuity Plans and Disaster Recovery</i>	36
3.7	<i>Availability of Revocation Data</i>	37
3.8	<i>Publication of Critical Information</i>	37
3.9	<i>Confidential Information</i>	37
3.9.1	Types of Information deemed as Confidential.....	37
3.9.2	Types of Information not deemed as Confidential.....	37
3.9.3	Access to Confidential Information.....	38
3.9.4	Release of Confidential Information.....	38
3.10	<i>Personnel Management and Practices</i>	38
3.11	<i>Privacy Policy</i>	38
3.12	<i>Publication of information</i>	39
4	Practices and Procedures	40
4.1	<i>Certificate Application Requirements</i>	40
4.1.1	RegistryPro Partner Certificate Applications.....	41
4.1.2	Methods of application	41
4.2	<i>Application Validation</i>	41
4.2.1	RegistryPro Secure Server Certificate Application	41

All .Pro applicants must provide their professional credentials to qualify for .Pro membership. Once the credentials are electronically verified against the professional governing body a postcard with a security code is mailed to the address on record..... 41

4.2.2 RegistryPro Secure Email Certificate Application 41

4.2.3 Secure Server Certificate Application Two-Step Validation Process 41

4.3 *Validation Information for RegistryPro Certificate Applications* 42

4.3.1 Application Information for Organizational Applicants 42

4.3.2 Supporting Documentation for Organizational Applicants..... 42

4.3.3 Application Information for Individual Applicants 42

4.3.4 Supporting Documentation for Individual Applicants..... 43

4.4 *Validation Requirements for RegistryPro Certificate Applications*..... 43

4.4.1 Third-Party Confirmation of Professional Entity Information..... 43

4.5 *Validation Information for Comodo Certificate Applications* 44

4.5.1 Application Information for Organizational Applicants 44

4.5.2 Supporting Documentation for Organizational Applicants..... 44

4.5.3 Application Information for Individual Applicants 45

4.5.4 Supporting Documentation for Individual Applicants..... 45

4.6 *Validation Requirements for Certificate Applications*..... 45

4.6.1 Third-Party Confirmation of Business Entity Information 46

4.6.2 Serial Number Assignment..... 46

4.7 *Time to Confirm Submitted Data*..... 46

4.8 *Approval and Rejection of Certificate Applications* 46

4.9 *Certificate Issuance and Subscriber Consent*..... 46

4.10 *Certificate Validity* 46

4.11 *Certificate Acceptance by Subscribers* 47

4.12 *Verification of Digital Signatures*..... 47

4.13 *Reliance on Digital Signatures*..... 47

4.14 *Certificate Suspension* 47

4.15 *Certificate Revocation* 47

4.15.1 Request for Revocation..... 48

4.15.2 Effect of Revocation..... 48

4.16 *Renewal* 48

4.17 *Notice Prior to Expiration*..... 49

5 Legal Conditions of Issuance **50**

5.1 *RegistryPro Representations* 50

5.2 *Comodo Representations*..... 50

5.3 *Information Incorporated by Reference into a RegistryPro Digital Certificate* 50

5.4 *Information Incorporated by Reference into a Comodo Digital Certificate*..... 50

5.5 *Displaying Liability Limitations, and Warranty Disclaimers - RegistryPro* 50

5.6 *Displaying Liability Limitations, and Warranty Disclaimers - Comodo*..... 51

5.7 *Publication of Certificate Revocation Data*..... 51

5.8 *Duty to Monitor the Accuracy of Submitted Information* 51

5.9	<i>Publication of Information</i>	51
5.10	<i>Interference with RegistryPro Implementation</i>	51
5.11	<i>Interference with Comodo Implementation</i>	51
5.12	<i>Standards</i>	52
5.13	<i>RegistryPro Partnerships Limitations</i>	52
5.14	<i>Comodo Partnerships Limitations</i>	52
5.15	<i>RegistryPro Limitation of Liability for a RegistryPro Partner</i>	52
5.16	<i>Comodo Limitation of Liability for a Comodo Partner</i>	52
5.17	<i>Choice of Cryptographic Methods</i>	52
5.18	<i>Reliance on Unverified Digital Signatures</i>	52
5.19	<i>Rejected Certificate Applications</i>	53
5.20	<i>Refusal to Issue a Certificate</i>	53
5.21	<i>Subscriber Obligations</i>	53
5.22	<i>Representations by Subscriber upon Acceptance</i>	54
5.23	<i>Indemnity by Subscriber</i>	54
5.24	<i>Obligations of RegistryPro Registration Authorities</i>	55
5.25	<i>Obligations of Comodo Registration Authorities</i>	55
5.26	<i>Obligations of a Relying Party</i>	55
5.27	<i>Legality of Information</i>	56
5.28	<i>Subscriber Liability to Relying Parties</i>	56
5.29	<i>Duty to Monitor Agents</i>	56
5.30	<i>Use of Agents</i>	56
5.31	<i>Conditions of usage of the RegistryPro Repository and Web site</i>	56
5.32	<i>Conditions of usage of the Comodo Repository and Web site</i>	56
5.33	<i>Accuracy of Information</i>	57
5.34	<i>Obligations of RegistryPro</i>	57
5.35	<i>Obligations of Comodo</i>	57
5.36	<i>Fitness for a Particular Purpose</i>	58
5.37	<i>Other Warranties</i>	58
5.38	<i>Non-Verified Subscriber Information</i>	59
5.39	<i>Exclusion of Certain Elements of Damages</i>	59
5.40	<i>Certificate Insurance Plan</i>	59
5.40.1	<i>ProSSL Certificate</i>	59
5.40.2	<i>InstantSSL Certificate</i>	59
5.40.3	<i>InstantSSL Pro Certificate</i>	59
5.40.4	<i>PremiumSSL Certificate</i>	60
5.40.5	<i>PremiumSSL Wildcard Certificate</i>	60
5.40.6	<i>Intranet SSL Certificate</i>	60
5.40.7	<i>Trial SSL Certificate</i>	60

5.41	<i>Financial Limitations on Certificate Usage</i>	60
5.42	<i>Damage and Loss Limitations</i>	60
5.43	<i>Conflict of Rules</i>	60
5.44	<i>RegistryPro Intellectual Property Rights</i>	60
5.45	<i>Comodo Intellectual Property Rights</i>	61
5.46	<i>Infringement and Other Damaging Material</i>	61
5.47	<i>Ownership</i>	61
5.48	<i>Governing Law</i>	61
5.49	<i>Jurisdiction</i>	61
5.50	<i>Dispute Resolution</i>	62
5.51	<i>Successors and Assigns</i>	62
5.52	<i>Severability</i>	62
5.53	<i>Interpretation</i>	62
5.54	<i>No Waiver</i>	62
5.55	<i>Notice</i>	63
5.56	<i>Fees</i>	63
5.57	<i>RegistryPro Reissue Policy</i>	63
5.58	<i>Comodo Reissue Policy</i>	64
5.59	<i>RegistryPro Refund Policy</i>	64
5.60	<i>Comodo Refund Policy</i>	64
6	General Issuance Procedure	64
6.1	<i>General - RegistryPro</i>	64
6.2	<i>General - Comodo</i>	65
6.3	<i>Certificates issued to Individuals and Organisations</i>	65
6.4	<i>Content</i>	65
6.4.1	<i>Secure Server Certificates</i>	65
6.4.2	<i>Secure Email Certificates</i>	66
6.5	<i>Time to Confirm Submitted Data</i>	66
6.6	<i>Issuing Procedure</i>	66
	Document Control	67

Terms and Acronyms Used in the CPS

Acronyms:

CA	Certificate Authority
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
EPKI	Enterprise Public Key Infrastructure Manager
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (based on X.509 Digital Certificates)
PKCS	Public Key Cryptography Standard
RA	Registration Authority
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 individual or entity applying for a Certificate.
Subscriber:	The Subscriber is an individual or entity that has been issued a Certificate.
Relying Party:	The Relying Party is an individual or entity that relies upon the information contained within the Certificate.
Subscriber Agreement:	The Subscriber Agreement is an agreement which 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 or www.registrypro.pro/support/repository .
Relying Party Agreement:	The Relying Party Agreement is an agreement which must be read and accepted by a Relying Party prior to validating, relying on or using a Certificate or accessing or using Comodo's Repository and is available for reference at www.comodogroup.com/repository or www.registrypro.pro/support/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) – incorporating the Registry Services Corporation (hereafter referred to as “RegistryPro” where applicable) Certification Practise Statement and outlines the legal, commercial and technical principles and practices that Comodo and RegistryPro 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 and RegistryPro’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 and the RegistryPro 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 and practices and CA infrastructure to issue Comodo digital certificates, or if appropriate, private labelled digital certificates.

1.2 Registry Services Corporation

Registry Services Corporation – hereafter referred to as “RegistryPro” where applicable - is a virtual Certification Authority that issues high quality and highly trusted certificates to .pro domain owners in accordance with the RegistryPro CPS; the .Pro domain extension is only available for certain self-certified professionals. In its role as a virtual CA, Registry Services Corporation 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 RegistryPro PKI. In delivering its PKI services RegistryPro 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.

RegistryPro extends, under agreement, membership of its PKI to approved third parties known as Registration Authorities. The international network of RegistryPro RAs share RegistryPro’s policies and practices and CA infrastructure to issue RegistryPro digital certificates.

1.3 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, Organisational, Practices and Legal.

This CPS, related agreements and Certificate policies referenced within this document are maintained by the Comodo Certificate Policy Authority. The Certificate Policy Authority may be contacted at the below address:

Certificate Policy Authority
New Court, Regents Place, Regent Road,
Manchester M5 4HB 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.

1.4 RegistryPro CPS

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

This CPS, related agreements and Certificate policies referenced within this document are maintained by the Comodo Certificate Policy Authority. The Certificate Policy Authority may be contacted at the below address:

Certificate Policy Authority
New Court, Regents Place, Regent Road,
Manchester M5 4HB 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.registrypro.pro/support/repository.

1.5 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 and www.registrypro.pro/support/repository), with thirty days notice given of upcoming changes and suitable incremental version numbering used to identify new editions.

Revisions not denoted "significant" shall be 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 – incorporating the RegistryPro CPS - is not amended and published without the prior authorisation of the Certificate Policy Authority.

1.6 Other Practice Statements & Agreements

The CPS is only one of a set of documents relevant to the provision of Certification Services by Comodo and Registry Services Corporation and that the list of documents contained in this clause are other documents which 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:

Document	Status	Location
Comodo Certification Practice Statement	Public	Comodo Repository: www.comodogroup.com/repository
Registry Services Corporation Certification Practice Statement	Public	RegistryPro Repository: www.registrypro.pro/support/repository
Secure Email Certificate Subscriber Agreement	Public	Comodo Repository: www.comodogroup.com/repository
Enterprise Public Key Infrastructure Manager Agreement	Confidential	Presented to partners accordingly
Web Host Reseller Agreement	Confidential	Presented to partners accordingly
Reseller Agreement	Confidential	Presented to partners accordingly
Powered SSL Partner Agreement	Confidential	Presented to partners accordingly
Enterprise Public Key Infrastructure Manager Guide	Confidential	Presented to partners accordingly
Web Host Reseller Guide	Confidential	Presented to partners accordingly
Reseller Guide	Confidential	Presented to partners accordingly
Powered SSL Partner Guide	Confidential	Presented to partners accordingly
Web Host Reseller Validation Guidelines	Confidential	Presented to partners accordingly

1.7 Liability of Comodo and RegistryPro

For legal liability of Comodo and RegistryPro under the provisions made in this CPS, please refer to Section 5: Legal Conditions of Issuance

1.8 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.

An annual 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

1.9 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.

As detailed in this CPS, Comodo and RegistryPro offer a range of distinct certificate types. The different certificate types have differing intended usages and differing policies.

Applicant	Certificate Type	Channels Available	Validation Levels ¹	Suggested Usage
Individual or Company; Authorized .pro domain owner.	Secure Server Certificate: <i>ProSSL</i>	- RegistryPro Website - RegistryPro Partner Network	Confirmation and cross verification of professional information and of right to use .pro domain	Establishes SSL / TLS session between the server housing the Secure Server Certificate and a client / customer / website visitor. The protocol is designed to authenticate a server to a client and provide confidentiality of data passed through the SSL / TLS session.
Individual or Company; Authorized .pro domain owner.	Secure Email Certificate: <i>ProCert</i>	- RegistryPro Website - RegistryPro Partner Network	Confirmation and cross verification of professional information and of right to use .pro domain. Email ownership automated challenge is conducted as part of the collection process.	Allows certificate owner to digitally sign email to prove corporate authorship, and for relying parties to verify a digitally signed email and to encrypt email for the certificate owner. May also be used for web based access control where prior validation of the certificate owner is deemed necessary.

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.

1.10 RegistryPro PKI Hierarchy

The following high-level representation of the RegistryPro PKI is used to illustrate the hierarchy utilised.

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

↳ RegistryPro CA (*serial number = 0200 029B, expiry = 23 February 2006*)

↳ End Entity SSL / End Entity Secure Email (*serial number = x, expiry = 1/2/3 year from issuance*)

1.11 RegistryPro Certification Authority

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

¹ Validation levels: Validation is conducted by Comodo, a Comodo Registration Authority (if the application is made through a Web Host Reseller or Powered SSL partner), RegistryPro or a RegistryPro Registration Authority under strict guidelines provided to the Registration Authority. Section 1.9 of this CPS identifies the Registration Authorities and outlines the roles and responsibilities of such entities.

- 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 RegistryPro repository (www.registrypro.pro/support/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 RegistryPro 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 RegistryPro issued certificate (for a period disclosed in this CPS)

1.12 Comodo PKI Hierarchy

Comodo partners with BeTrusted (www.betrusted.com - AICPA/CICA WebTrust Program for Certification Authorities approved security provider) for its Root CA Certificate. The partnership allows Comodo to issue highly trusted digital certificates by inheriting the trust level associated with BeTrusted root certificate (named GTE CyberTrust Root). The following high-level representation of the Comodo PKI is used to illustrate the hierarchy utilised.

1.12.1 Trial and 1 year certificates

GTE CyberTrust Global Root (*serial number = 01A3, expiry = 23 February 2006*)

- ↳ Comodo Class 3 Security Services CA (*serial number = 0200 029B, expiry = 23 February 2006*)
 - ↳ End Entity SSL / End Entity Secure Email (*serial number = x, expiry = 1 month/1 year from issuance*)

1.12.2 2 and 3 year certificates

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

- ↳ Comodo Class 3 Security Services CA (*serial number = 0200 029B, expiry = 27 August 2012*)
 - ↳ End Entity SSL / End Entity Secure Email (*serial number = x, expiry = 2 or 3 years from issuance*)

1.13 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)

1.14 RegistryPro Registration Authorities

RegistryPro 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. RegistryPro 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 RegistryPro validation guidelines documentation.
- Use official, notarised 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 RegistryPro validation guidelines documentation.

A RegistryPro RA acts locally within their own context of geographical or business partnerships on approval and authorisation by RegistryPro in accordance with RegistryPro practices and procedures.

RAs are restricted to operating within the set validation guidelines published by RegistryPro 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.

1.15 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, notarised 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 authorisation 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.

1.16 Subscribers

Subscribers of Comodo and RegistryPro services are individuals or companies that use PKI in relation with Comodo/RegistryPro supported transactions and communications. Subscribers are parties that are identified in a certificate and hold the private key corresponding to the public key that is listed in a subscriber certificate. Prior to verification of identity and issuance of a certificate a subscriber is an applicant for the services of Comodo/RegistryPro.

1.17 Relying Parties

Relying parties use PKI services in relation with Comodo/RegistryPro certificates and reasonably rely on such certificates and/or digital signatures verifiable with reference to a public key listed in a subscriber certificate.

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

2 Technology

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

2.1 Comodo/RegistryPro CA Infrastructure

The Comodo CA and RegistryPro CA Infrastructures use 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

Protection of the CA Root signing key pairs is ensured with the use of IBM 4578 crypto processor 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 using the RSA algorithm.

Key Number	CA Number	Description	Usage	Lifetime	Size
2	2	Class 1 Public Primary CA	Self signed root certificate for Class1 intermediates	20 years	2048
3	3	Class 2 Public Primary CA	Self signed root certificate for Class2 intermediates (not commercially active)	20 years	2048
4	4	Class 3 Public Primary CA	Self signed root certificate for Class3 intermediates	20 years	2048

5	5	Class 4 Public Primary CA	Self signed root certificate for Class4 intermediates (not commercially active)	20 years	2048
6	6	Comodo Class 1 TTB Intermediate CA	Intermediate certificate for IdAuthority Website Certificates	10 years	2048
7	7	Comodo Class 3 TTB/Verification Engine Intermediate CA	Intermediate certificate for IdAuthority Premium, Card Payment, & Verification Engine Certificates	10 years	2048
8	8	Comodo Class 1 Individual Subscriber CA – Persona Not Validated	Intermediate certificate for Class 1 email certificates	10 years	2048
9	9	Comodo Class 3 Secure Server CA	Intermediate certificate for SSL certificates (not commercially active)	10 years	2048
10	10	Comodo Class 3 Software Developer CA	Intermediate certificate for code signing certificates (not commercially active)	10 years	2048
11	11	'GlobalSigned' Class 3 Security Services CA	Intermediate certificate for SSL certificates	To 28-jan-2014	2048
16	11	'BeTrustedSigned' Class 3 Security Services CA (2018)	Intermediate certificate for code signing	To 2018	2048
17	11	'BeTrustedSigned' Class 3 Security Services CA (2006)	Intermediate certificate for SSL certificates, Class 1 & 3 email certificates	To 23-feb-2006	2048
18	12	Comodo Certified Delivery Plug-in CA	Intermediate certificate for "Certified Delivery Plug-in" certificates (not commercially active)	10 years	2048
19	13	Comodo Certified	Intermediate	10 years	2048

		Delivery Manager CA	certificate for “Certified Delivery Manager” certificates (not commercially active)		
20	14	Comodo Certified Delivery Authority CA	Intermediate certificate for “certified delivery authority” certificates (not commercially active)	10 years	2048
22	16	AAA Certificate Services	TBC	25 years	2048
23	17	Secure Certificate Services	TBC	25 years	2048
24	18	Trusted Certificate Services	TBC	25 years	2048
27	22	RegistryPro CA	Intermediate certificate for SSL certificates, Class 1 & 3 email certificates	2018	2048

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 2 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.

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).

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 unauthorised usage of it.

Comodo securely generates and protects RegistryPro’s 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 unauthorised usage of it.

The Comodo CA Root key and RegistryPro CA Root key were generated in accordance with the guidelines detailed in the Root Key Generation Ceremony Reference. The activities undergone and the personnel involved in the Root Key Generation Ceremony are recorded for audit

purposes. Subsequent Root Key Generation Ceremonies are to follow the documented reference guide also.

2.1.3 CA Root Signing Key Archival

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

2.1.4 Procedures employed for CA Root Signing Key Changeover

Towards the end of any 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

All CA Root Certificates are available in online repositories at www.comodogroup.com/repository and www.registrypro.pro/support/repository. The GTE CyberTrust Root certificate is present in Internet Explorer 5.00 and above, Netscape 4.x and above and Opera 5.0 and above and is made available to relying parties through these browsers.

Comodo and RegistryPro provide the full certificate chain (see section **Error! Reference source not found.** 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 through the use of physical access control and is only accessible to appropriately authorised 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.

2.1.6.2 RegistryPro

Access to the secure part of RegistryPro facilities is limited through the use of physical access control and is only accessible to appropriately authorised 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.

RegistryPro 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

RegistryPro 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.

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

- Verification of the identity of an applicant of a certificate.
- Authorising the issuance of certificates.
- Issuance of certificates.
- Revocation of certificates.
- De-commissioning of the corresponding private keys through a process involving the revocation of certificates.
- Listing of certificates.
- Distributing certificates.
- Publishing certificates.
- Storing certificates.
- Retrieving certificates in accordance with their particular intended use.

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.

RegistryPro conducts the overall certification management within the RegistryPro PKI; either directly or through a RegistryPro approved RA. RegistryPro 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 List

Comodo manages and makes publicly available directories of revoked certificates through the use of 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 issued and revoked certificates at all times prior to relying on information featured on a certificate. Comodo updates and publishes a new CRL daily at 06:05 or more frequently under special circumstances. The CRL for end entity certificates can be accessed via the following URLs:

<http://crl.comodo.net/Class3SecurityServices.crl>
http://crl.comodo.net/Class3SecurityServices_3.crl

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

<http://crl.comodoca.com/Class3SecurityServices.crl>
<http://crl.comodoca.com/Class3SecurityServices 3.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 RegistryPro Directories, Repository and Certificate Revocation List

RegistryPro manages and makes publicly available directories of revoked certificates through the use of Certificate Revocation Lists (CRLs). All CRLs issued by RegistryPro are X.509v2 CRLs, in particular as profiled in RFC3280. Users and relying parties are strongly urged to consult the directories of issued and revoked certificates at all times prior to relying on information featured on a certificate. RegistryPro updates and publishes a new CRL daily at 06:05 or more frequently under special circumstances. The CRL for end entity certificates can be accessed via the following URLs:

<http://crl.registrypro.com/RegistryProCA1.crl>

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

<http://crl2.registrypro.com/RegistryProCA1.crl>

RegistryPro 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 RegistryPro legal repository may be accessed at <http://www.registrypro.pro/support/repository>.

2.5 Types of RegistryPro Certificates

RegistryPro currently offers one type of digital certificate 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.

RegistryPro 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 RegistryPro products creates no claims by any third party. Upon the inclusion of a new certificate product in the RegistryPro hierarchy, an amended version of this CPS will be made public within two days on the official RegistryPro and Comodo websites.

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

2.5.1 RegistryPro Secure Server Certificate

RegistryPro makes available a Secure Server Certificate that in combination with a Secure Socket Layer (SSL) web server attests the public server's identity providing full authentication and enables secure communication with corporate customers and corporate business partners. RegistryPro Secure Server Certificate is offered as a ProSSL certificate. Pricing for the certificates are made available on the relevant official RegistryPro websites.

2.5.2 RegistryPro Secure Email Certificates

RegistryPro 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 RegistryPro websites. From time to time RegistryPro reserves the right to make available promotional offers that may affect the standard price card.

2.6 Extensions and Naming

2.6.1 Digital Certificate Extensions

Comodo and RegistryPro use the standard X.509, version 3 to construct digital certificates for use within the Comodo and RegistryPro PKI. X.509v3 allows a CA to add certain certificate extensions to the basic certificate structure. Comodo and RegistryPro use 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.

2.6.2 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 organisational unit field is also included in the Certificate Policy extension that Comodo and RegistryPro may use.

2.7 Subscriber Private Key Generation Process

The Subscriber is solely responsible for the generation of the private key used in the certificate request. Comodo and RegistryPro do not provide key generation, escrow, recovery or backup facilities.

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

Typically, Secure Server Certificate requests are generated using the key generation facilities available in the Subscriber's webserver software. Typically, Secure Email Certificate requests are generated using the FIPS 140-1 Level 1 cryptographic service provider module software present in popular browsers.

2.8 Subscriber Private Key Protection and Backup

The Subscriber is solely responsible for protection of their private keys. Comodo and Registry Pro maintain no involvement in the generation, protection or distribution of such keys.

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

2.9 Subscriber Public Key Delivery to Comodo or RegistryPro

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

2.10 Delivery of Issued Subscriber Certificate to Subscriber

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

2.10.1 Secure Server Certificate: ProSSL product type

ProSSL are delivered via email to the Subscriber through the use of the administrator contact email address provided during the application process.

2.10.2 Secure Email Certificate: ProCert product type

Upon issuance of the ProCert 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.

2.11 RegistryPro Certificates Profile

A Certificate profile contains fields as specified below:

2.11.1 Key Usage extension field

RegistryPro certificates are general purpose and may be used without restriction on geographical area. In order to use and rely on a RegistryPro certificate the relying party must use X.509v3 compliant software. RegistryPro certificates include key usage extension fields to specify the purposes for which the certificate may be used and also 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 RegistryPro.

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 non-repudiation 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

2.11.2 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.

2.11.3 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 certificate. Reliance on basic constraints extension field is dependent on correct software implementations of the X.509v3 standard and is outside of the control of RegistryPro.

2.11.4 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 RegistryPro certificate profiles are as per the tables below:

RegistryPro Secure Server Certificate		
Signature Algorithm	Sha1	
Issuer	CN	Registry Pro CA
	OU	(c)2004 Registry Services Corporation
	OU	Terms and Conditions: http://www.registrypro.pro/support/repository
	O	Registry Services Corporation
	C	US
Validity	1 Year / 2 Year / 3 Year	
Subject	CN	Common Name
	OU	Registry Pro SSL Certificate

	O	Organization
	OU	Organization Unit
	L	Locality
	S	Street
	C	Country
Authority Key Identifier	KeyID=[aka literal value]	
Key Usage (NonCritical)	Digital Signature , Key Encipherment(A0)	
Netscape Certificate Type	SSL Server Authentication(40)	
Basic Constraint	Subject Type=End Entity Path Length Constraint=None	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.registrypro.com/RegistryProCA1.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl2.registrypro.com/RegistryProCA1.crl [3]CRL Distribution Point Distribution Point Name: Full Name: RFC822 Name=RegistryProCA1@crl. registrypro.com	
Thumbprint Algorithm	SHA1	
Thumbprint		

Registry Pro Secure Email Certificate		
Signature Algorithm	Sha1	
Issuer	CN	Registry Pro CA
	OU	(c)2004 Registry Services Corporation
	OU	Terms and Conditions: http://www.registrypro.pro/support/repository
	O	Registry Services Corporation
	C	US
Validity	1 Year	
Subject	E	Email address
	CN	Common Name (name of subscriber)
	OU	OU = (c)2004 Registry Pro Inc
	OU	OU = Terms and Conditions: http://www.registrypro.pro/support/repository
	OU	Registry Pro - PERSONA NOT VALIDATED
Authority Key Identifier	KeyID=[aka literal value]	

Key Usage (NonCritical)	Secure Email(1.3.6.1.5.5.7.3.4) Client Authentication(1.3.6.1.5.5.7.3.2) Smart Card Logon(1.3.6.1.4.1.311.20.2.2) Certified Delivery Service Rx (1.3.6.1.4.1.6449.1.3.5.2)
Netscape Certificate Type	SSL Client Authentication , SMIME(A0)
Basic Constraint	Subject Type=End Entity Path Length Constraint=None
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.registrypro.com/RegistryProCA1.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl2.registrypro.com/RegistryProCA1.crl [3]CRL Distribution Point Distribution Point Name: Full Name: RFC822 Name= RegistryProCA1@crl. registrypro.com
Thumbprint Algorithm	SHA1
Thumbprint	

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 also 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:

- j) 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
- k) Non-repudiation, for verifying digital signatures used in providing a non-repudiation service which protects against the signing entity falsely denying some action (excluding certificate or CRL signing, as in f) or g) below)
- l) Key encipherment, for enciphering keys or other security information, e.g. for key transport

- m) Data encipherment, for enciphering user data, but not keys or other security information as in c) above
- n) Key agreement, for use as a public key agreement key
- o) Key certificate signing, for verifying a CA's signature on certificates, used in CA-certificates only
- p) CRL signing, for verifying a CA's signature on CRLs
- q) Encipher only, public key agreement key for use only in enciphering data when used with key agreement
- r) 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 certificate. 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 Certificate – InstantSSL / InstantSSL Pro / PremiumSSL / PremiumSSL Wildcard		
Signature Algorithm	Sha1	
Issuer	CN	Comodo Class 3 Security Services CA
	OU	(c) 2002 Comodo CA Limited
	OU	Terms and Conditions of use: http://www.comodogroup.com/repository
	OU	Comodo Trust Network
	O	Comodo CA Limited
	C	GB
Validity	1 Year / 2 Year / 3 Year	
Subject	CN	Common Name
	OU	InstantSSL / InstantSSL Pro / PremiumSSL / <i>Powered SSL Product Name*</i>

	OU	<i>Hosted by [Web Host Reseller Subscriber Name] Issued through [EPKI Manager Subscriber Name] Provided by [Powered SSL Subscriber Name]</i>
	O	Organization
	OU	Organization Unit
	L	Locality
	S	Street
	C	Country
Authority Key Identifier		KeyID=7E7E 8DC4 5055 B52E D34F 59D9 6559 A1F1 5A0C EAB1
Key Usage (NonCritical)		Digital Signature , Key Encipherment(A0)
Netscape Certificate Type		SSL Server Authentication(40)
Basic Constraint		Subject Type=End Entity Path Length Constraint=None
Certificate Policies		[1]Certificate Policy: PolicyIdentifier=1.3.6.1.4.1.6449.1.2.1.3.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.comodogroup.com/repository
CRL Distribution Points		[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.comodo.net/Class3SecurityServices.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.comodoca.com/Class3SecurityServices.crl [3]CRL Distribution Point Distribution Point Name: Full Name: RFC822 Name=Class3SecurityServices@crl.comodo.net [1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.comodo.net/Class3SecurityServices 3.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.comodoca.com/Class3SecurityServices 3.crl [3]CRL Distribution Point Distribution Point Name: Full Name: RFC822 Name= Class3SecurityServices 3@crl.comodo.net
Subject Alternate Name		DNS Name
NetscapeSSLServerName		

Thumbprint Algorithm	SHA1
Thumbprint	

Comodo Secure Server Certificate – Intranet SSL	
Signature Algorithm	Sha1
Issuer	CN Comodo Class 3 Security Services CA
	OU (c) 2002 Comodo CA Limited
	OU Terms and Conditions of use: http://www.comodogroup.com/repository
	OU Comodo Trust Network
	O Comodo CA Limited
	C GB
Validity	1 Year / 2 Year / 3 Year
Subject	CN Common Name
	OU Intranet SSL ²
	OU INTRANET USE ONLY - NO WARRANTY ATTACHED - COMPANY NOT VALIDATED
	OU <i>Hosted by [Web Host Reseller Subscriber Name] Issued through [EPKI Manager Subscriber Name] Provided by [Powered SSL Subscriber Name]</i>
	O Organization
	OU Organization Unit
	L Locality
	S Street
	C Country
Authority Key Identifier	KeyID=7E7E 8DC4 5055 B52E D34F 59D9 6559 A1F1 5A0C EAB1
Key Usage (NonCritical)	Digital Signature , Key Encipherment(A0)
Netscape Certificate Type	SSL Server Authentication(40)
Basic Constraint	Subject Type=End Entity
	Path Length Constraint=None
Certificate Policies	[1]Certificate Policy: PolicyIdentifier=1.3.6.1.4.1.6449.1.2.1.3.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.comodogroup.com/repository

² Subscribers to the Powered SSL service have the opportunity to rebrand an InstantSSL Certificate, InstantSSL Pro Certificate, PremiumSSL Certificate, PremiumSSL Wildcard Certificate, Intranet SSL Certificate or Trial SSL Certificate with their own product naming.

CRL Distribution Points	<p>[[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.comodo.net/Class3SecurityServices.crl</p> <p>[2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.comodoca.com/Class3SecurityServices.crl</p> <p>[3]CRL Distribution Point Distribution Point Name: Full Name: RFC822 Name=Class3SecurityServices@crl.comodo.net</p> <p>[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.comodo.net/Class3SecurityServices 3.crl</p> <p>[2]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.comodoca.com/Class3SecurityServices 3.crl</p> <p>[3]CRL Distribution Point Distribution Point Name: Full Name: RFC822 Name= Class3SecurityServices 3@crl.comodo.net</p>
Subject Alternate Name	DNS Name
NetscapeSSLServerName	
Thumbprint Algorithm	SHA1
Thumbprint	

Comodo Secure Server Certificate – Trial SSL	
Signature Algorithm	Sha1
Issuer	CN Comodo Class 3 Security Services CA
	OU (c) 2002 Comodo CA Limited
	OU Terms and Conditions of use: http://www.comodogroup.com/repository
	OU Comodo Trust Network
	O Comodo CA Limited
	C GB
Validity	1 Year / 2 Year / 3 Year
Subject	CN Common Name
	OU Trial SSL ³
	OU TEST USE ONLY - NO WARRANTY ATTACHED

³ Subscribers to the Powered SSL service have the opportunity to rebrand an InstantSSL Certificate, InstantSSL Pro Certificate, PremiumSSL Certificate, PremiumSSL Wildcard Certificate Intranet SSL Certificate or Trial SSL Certificate with their own product naming.

	OU	<i>Hosted by [Web Host Reseller Subscriber Name] Issued through [EPKI Manager Subscriber Name] Provided by [Powered SSL Subscriber Name]</i>
	O	Organization
	OU	Organization Unit
	L	Locality
	S	Street
	C	Country
Authority Key Identifier	KeyID=7E7E 8DC4 5055 B52E D34F 59D9 6559 A1F1 5A0C EAB1	
Key Usage (NonCritical)	Digital Signature , Key Encipherment(A0)	
Netscape Certificate Type	SSL Server Authentication(40)	
Basic Constraint	Subject Type=End Entity Path Length Constraint=None	
Certificate Policies	[1]Certificate Policy: PolicyIdentifier=1.3.6.1.4.1.6449.1.2.1.3.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.comodogroup.com/repository	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.comodo.net/Class3SecurityServices.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.comodoca.com/Class3SecurityServices.crl [3]CRL Distribution Point Distribution Point Name: Full Name: RFC822 Name=Class3SecurityServices@crl.comodo.net	
Subject Alternate Name	DNS Name	
NetscapeSSLServerName		
Thumbprint Algorithm	SHA1	
Thumbprint		

Comodo Secure Server Certificate – Secure Email Certificate (Free Version)		
Signature Algorithm	Sha1	
Issuer	CN	Comodo Class 3 Security Services CA
	OU	(c)2002 Comodo CA Limited
	OU	Terms and Conditions of use: http://www.comodogroup.com/repository
	OU	Comodo Trust Network
	O	Comodo CA Limited
	C	GB
Validity	1 Year	
Subject	E	Email address
	CN	Common Name (name of subscriber)

	OU	OU = (c)2001 Comodo CA Limited
	OU	OU = Terms and Conditions of use: http://www.comodogroup.com/repository
	OU	Comodo Trust Network - PERSONA NOT VALIDATED
Authority Key Identifier	KeyID=F652 2217 1513 0803 59BF 1895 9F48 B4B9 E9FE F866	
Key Usage (NonCritical)	Secure Email(1.3.6.1.5.5.7.3.4) Unknown Key Usage(1.3.6.1.4.1.6449.1.3.5.2) ⁴	
Netscape Certificate Type	SMIME(20)	
Basic Constraint	Subject Type=End Entity Path Length Constraint=None	
Certificate Policies	[1]Certificate Policy: PolicyIdentifier=1.3.6.1.4.1.6449.1.2.1.3.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.comodogroup.com/repository	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.comodo.net/Class3SecurityServices_2.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.comodoca.com/Class3SecurityServices_2.crl [3]CRL Distribution Point Distribution Point Name: Full Name: RFC822 Name=Class3SecurityServices_2@crl.comodo.net	
Subject Alternate Name	RFC822 Name= email address	
Thumbprint Algorithm	SHA1	
Thumbprint		

Comodo Secure Server Certificate – Secure Email Certificate (Corporate Version)		
Signature Algorithm	Sha1	
Issuer	CN	Comodo Class 3 Security Services CA
	OU	(c)2002 Comodo CA Limited
	OU	Terms and Conditions of use: http://www.comodogroup.com/repository
	OU	Comodo Trust Network
	O	Comodo CA Limited
	C	GB
Validity	1 Year	
Subject	E	Email address
	CN	Common Name (name of subscriber)
	OU	OU = (c)2001 Comodo CA Limited

⁴ Used for the Comodo Certified Delivery Service receive facility. Certified Delivery Service is not covered in this CPS.

	OU	OU = Terms and Conditions of use: http://www.comodogroup.com/repository
	OU	Comodo Trust Network - PERSONA NOT VALIDATED
Authority Key Identifier	KeyID=F652 2217 1513 0803 59BF 1895 9F48 B4B9 E9FE F866	
Key Usage (NonCritical)	Secure Email(1.3.6.1.5.5.7.3.4) Client Authentication(1.3.6.1.5.5.7.3.2) Smart Card Logon(1.3.6.1.4.1.311.20.2.2) Unknown Key Usage(1.3.6.1.4.1.6449.1.3.5.2) ⁵	
Netscape Certificate Type	SSL Client Authentication , SMIME(A0)	
Basic Constraint	Subject Type=End Entity Path Length Constraint=None	
Certificate Policies	[1]Certificate Policy: PolicyIdentifier=1.3.6.1.4.1.6449.1.2.1.3.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.comodogroup.com/repository	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.comodo.net/Class3SecurityServices_2.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.comodoca.com/Class3SecurityServices_2.crl [3]CRL Distribution Point Distribution Point Name: Full Name: RFC822 Name=Class3SecurityServices_2@crl.comodo.net	
Subject Alternate Name	RFC822 Name= email address	
Thumbprint Algorithm	SHA1	
Thumbprint		

2.13 RegistryPro Certificate Revocation List Profile

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

Version	[Version 1]
----------------	-------------

⁵ Used for the Comodo Certified Delivery Service receive facility. Certified Delivery Service is not covered in this CPS.

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 + 2 hours]	
Revoked Certificates	<i>CRL Entries</i>	
	Certificate Serial Number	[Certificate Serial Number]
	Date and Time of Revocation	[Date and Time of Revocation]

2.14 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 + 2 hours]	
Revoked Certificates	<i>CRL Entries</i>	
	Certificate Serial Number	[Certificate Serial Number]
	Date and Time of Revocation	[Date and Time of Revocation]

3 Organization

Comodo operates within the United Kingdom, 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.

RegistryPro operates within the United States of America. The site operates 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.

RegistryPro 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/RegistryPro will provide timely notice and transfer of responsibilities to succeeding entities, maintenance of records, and remedies. Before terminating its own CA activities, Comodo/RegistryPro will where possible take the following steps:

- 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 and RegistryPro each retains records in electronic or in paper-based format for a period detailed in section 3.4 of this CPS. Comodo and RegistryPro may each 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 its 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.

RegistryPro Registration Authorities are required to submit appropriate documentation as detailed in the pertinent agreement, and prior to being validated and successfully accepted as an approved RegistryPro Registration Authority.

In its role as a RegistryPro 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 RegistryPro and as stated in this CPS.

3.4 Records Retention Period

Comodo and RegistryPro each retains the records of Comodo/RegistryPro digital certificates and the associated documentation for a term of no less than 7 years. 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 format, in paper-based format or any other format that Comodo or RegistryPro 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 and RegistryPro maintain 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 or RegistryPro 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 offsite 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, 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/RegistryPro 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

3.5.4 Log Retention Period

Comodo and RegistryPro each maintains logs for a period not less than 7 years, or as necessary to comply with applicable laws.

3.6 Business Continuity Plans and Disaster Recovery

To maintain the integrity of its services Comodo and RegistryPro each 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 and RegistryPro each 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) within 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 two sites, with Salford, Greater Manchester, UK being the primary operations site and Bradford West Yorkshire, UK being the secondary site. Both sites offer facilities to manage the lifecycle of a certificate, including but not limited to the application, issuance, revocation and renewal of such certificates.
- RegistryPro operations are situated on one site in Chicago, Illinois, USA. This site offers 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 and RegistryPro each 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 and RegistryPro will each endeavour to minimise interruptions to its CA operations.

3.7 Availability of Revocation Data

Comodo and RegistryPro each publishes Certificate Revocation Lists (CRLs) to allow relying parties to verify a digital signature made using a Comodo or RegistryPro issued digital certificate. Each CRL contains entries for all revoked un-expired certificates issued and is valid for 24 hours. Comodo and RegistryPro each issues a new CRL at 06:05 prior to the expiry of the current CRL and includes a monotonically increasing sequence number for each CRL issued. Under special circumstances Comodo and RegistryPro may each 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. Neither Comodo nor RegistryPro supports OCSP (Online Certificate Status Protocol).

3.8 Publication of Critical Information

Comodo and RegistryPro each publishes any revocation data on issued digital certificates, 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 and the official RegistryPro repository <http://www.registrypro.pro/support/repository>. The Comodo and RegistryPro repositories are maintained by the Comodo Certificate Policy Authority and all updates, amendments and legal promotions are logged in accordance with the logging procedures referenced in section 3.5 this CPS.

3.9 Confidential Information

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

3.9.1 Types of Information deemed as Confidential

Comodo and RegistryPro each 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 which may be published at the discretion of Comodo/RegistryPro.
- Contingency plans and disaster recovery plans.
- Internal tracks and records on the operations of Comodo/RegistryPro 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 and RegistryPro CAs is public information and is periodically published every 24 hours at the Comodo and RegistryPro repositories. 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 **Error! Reference source not found.** 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

Neither Comodo nor RegistryPro is required to release any confidential information, unless as otherwise required by law, without an authenticated, reasonably specific request by an authorised party specifying:

- The party to whom Comodo or RegistryPro 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 and RegistryPro each 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.

Trusted roles – Not applicable to RegistryPro

Trusted roles relate to access to the Comodo account management system, with functional permissions applied on an individual basis. Permissions are decided by senior members of the management team, 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 both a password and digital certificate.

Personnel controls

All trusted personnel have background checks before access is granted to Comodo's and RegistryPro's respective 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 is in compliance with this CPS. The Comodo privacy policy is published at the Comodo repository at www.comodogroup.com/repository.

RegistryPro has implemented a privacy policy, which is in compliance with this CPS. The RegistryPro privacy policy is published at <http://www.registrypro.pro/support/privacy.php>.

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

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

- On the web: www.registrypro.pro
- By email from legal@registrypro.pro
- and by mail from:
Registry Services Corporation
One North State Street, Suite 1200, Chicago, Illinois, United States of America
Tel: + 1 312 994 7652
Fax: + 1 312 236 1958
Email: legal@registrypro.pro

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 includes:

- Generate a RSA key pair and demonstrate to Comodo/RegistryPro ownership of the private key half of the key pair through the submission of a valid PKCS#10 Certificate Signing Request (CSR)
- Make all reasonable efforts to protect the integrity the private key half of the key pair
- Submit to Comodo/RegistryPro 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/RegistryPro during the enrolment process

Certificate applications are submitted to either Comodo, a Comodo approved RA, RegistryPro or a RegistryPro 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 – RegistryPro ProSSL	End Entity Subscriber	RegistryPro	Comodo
Secure Email Certificate – RegistryPro ProCert	End Entity Subscriber	RegistryPro	Comodo
Secure Server Certificate – RegistryPro ProSSL	RegistryPro RA on behalf of End Entity Subscriber	RegistryPro	Comodo
Secure Email Certificate – RegistryPro ProCert	RegistryPro RA on behalf of End Entity Subscriber	RegistryPro	Comodo
Secure Server Certificate – <i>all types as per section Error! Reference source not found. of this CPS</i>	End Entity Subscriber	Comodo	Comodo
Secure Server Certificate – <i>all types as per section Error! Reference source not found. of this CPS</i>	Web Host Reseller on behalf of End Entity Subscriber	Web Host Reseller	Comodo
Secure Email Certificate – <i>free version as per Error! Reference source not found. of this CPS</i>	End Entity Subscriber	Comodo	Comodo
Secure Email Certificate – <i>Corporate version as per Error! Reference source not found. of this CPS</i>	End Entity Subscriber	EPKI Manager Account Holder	Comodo

4.1.1 RegistryPro Partner Certificate Applications

Authorised RegistryPro 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 partner 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 Methods of application

Generally, applicants will complete the online forms made available by Comodo or RegistryPro 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 RegistryPro 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 Comodo and RegistryPro each 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 RegistryPro Secure Server Certificate Application

All .Pro applicants must provide their professional credentials to qualify for .Pro membership. Once the credentials are electronically verified against the professional governing body a postcard with a security code is mailed to the address on record.

4.2.2 RegistryPro Secure Email Certificate Application

All .Pro applicants must provide their professional credentials to qualify for .Pro membership. In accordance with section **Error! Reference source not found.** (Validation Practices) of this CPS, and through the use of an email ownership validation check, RegistryPro asserts that the subscriber owns, or has direct access to, the email address stated within the Secure Email Certificates.

4.2.3 Secure Server Certificate Application Two-Step Validation Process

Comodo utilises a two-step validation process prior to the issuance of a secure server certificate.

This process involves Comodo, automatically or manually, reviewing the application information provided by the applicant (as per section 4.3 of this CPS) in order to check that:

1. The applicant has the right to use the domain name used in the application
 - Validated by reviewing domain name ownership records available publicly through Internet or approved global domain name registrars
 - Validation may be supplemented through the use of the administrator contact associated with the domain name register record for communication with Comodo validation staff or for automated email challenges

- Validation may be supplemented through the use of generic emails which ordinarily are only available to the person(s) controlling the domain name administration, for example webmaster@..., postmaster@..., admin@...
2. The applicant is an accountable legal entity, whether an organization or an individual.
 - Validated by requesting official company documentation, such as Business License, Articles of Incorporate, Sales License or other relevant documents. For non-corporate applications, documentation such as bank statement, copy of passport, copy of driving license or other relevant documents.

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

4.3 Validation Information for RegistryPro Certificate Applications

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

From time to time, RegistryPro may modify the requirements related to application information for individuals to respond to own RegistryPro requirements, the business context of the usage of a digital certificate, or as it may be prescribed by law.

4.3.1 Application Information for Organizational Applicants

The following elements are critical information elements for a RegistryPro 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)
- Organisational 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 professional 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 are the following:

- Professional Credentials

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

4.3.3 Application Information for Individual Applicants

The following elements are critical information elements for a RegistryPro certificate issued to an individual. 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 Individual (PUBLIC)
- Organisational 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 professional status of the Individual
- Subscriber agreement, signed (if applying out of bands)

4.3.4 Supporting Documentation for Individual Applicants

Documentation requirements for Individual applicants are the following:

- Professional Credentials

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

4.4 Validation Requirements for RegistryPro Certificate Applications

Upon receipt of an application for a digital certificate and based on the submitted information, RegistryPro will confirm 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 authorised to do so.

In all types of RegistryPro certificates the Subscriber has a continuous obligation to monitor the accuracy of the submitted information and notify RegistryPro 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 not yet paid under the Subscriber Agreement.

4.4.1 Third-Party Confirmation of Professional Entity Information

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

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

4.5 Validation Information for Comodo 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 own Comodo requirements, the business context of the usage of a digital certificate, or as it may be prescribed by law.

4.5.1 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)
- Organisational 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)

4.5.2 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 authorised 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.

4.5.3 Application Information for Individual Applicants

The following elements are critical information elements for a Comodo certificate issued to an individual. 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 Individual (PUBLIC)
- Organisational 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)

4.5.4 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.

4.6 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 authorised 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 not yet paid under the Subscriber Agreement.

4.6.1 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 organisations, other third party databases and government entities.

Comodo controls 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.

4.6.2 Serial Number Assignment

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

4.7 Time to Confirm Submitted Data

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

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

4.8 Approval and Rejection of Certificate Applications

Following successful completion of all required validations of a certificate application Comodo and/or RegistryPro will approve an application for a digital certificate.

If the validation of a certificate application fails, Comodo and/or RegistryPro will reject the certificate application.

Comodo and RegistryPro each 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 names of Comodo or RegistryPro might get tarnished, diminished or have either of their 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.

4.9 Certificate Issuance and Subscriber Consent

Comodo and RegistryPro each 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 4.11 of this CPS). Issuing a digital certificate means that Comodo and RegistryPro each accepts a certificate application.

4.10 Certificate Validity

Certificates are valid upon issuance by Comodo and RegistryPro and acceptance by the Subscriber. Generally the certificate validity period will be 1, 2 or 3 years, however Comodo and

RegistryPro each reserves the right to offer validity periods outside of this standard validity period.

4.11 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.
- 30 days pass from the date of the issuance of a certificate.

4.12 Verification of Digital Signatures

Verification of a digital signature is used to determine that:

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

4.13 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.

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.

4.14 Certificate Suspension

Neither Comodo nor RegistryPro utilizes certificate suspension.

4.15 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 and RegistryPro will each revoke a digital certificate if:

- There has been loss, theft, modification, unauthorised disclosure, or other compromise of the private key associated with the certificate.
- The Subscriber, Comodo or RegistryPro has breached a material obligation under this CPS.
- Either the Subscriber's, Comodo's or RegistryPro's obligations under this CPS 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.

4.15.1 Request for Revocation

The Subscriber or other appropriately authorised parties such as RAs can request revocation of a certificate. Prior to the revocation of a certificate Comodo and RegistryPro 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 and RegistryPro each employs the following procedure for authenticating a revocation request:

- The revocation request must be received by the Administrator contact associated with the certificate application. Comodo and RegistryPro may each, if necessary, also request that the revocation request be made by either the organizational contact or the billing contact.
- Upon receipt of the revocation request Comodo and RegistryPro will each request confirmation from the known administrator out of bands contact details, either by telephone or fax.
- Comodo and RegistryPro 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.

4.15.2 Effect of Revocation

Upon revocation of a certificate, the operational period of that certificate is immediately considered terminated. The serial number of the revoked certificate will be placed within the Certificate Revocation List (CRL) and remains on the CRL until some time after the end of the certificate's validity period. An updated CRL is published on the Comodo and RegistryPro websites every 24 hours; however under special circumstances the CRL may be published more frequently.

4.16 Renewal

Depending on the option selected during application, the validity period of Comodo and RegistryPro certificates is one year (365 days), two years (730 days) or three years (1095 days) from the date of issuance and is detailed in the relevant field within the certificate.

Renewal fees are detailed on the official Comodo and RegistryPro 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.

4.17 Notice Prior to Expiration

Comodo and RegistryPro shall each 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 each of Comodo's and RegistryPro's digital certificates.

5.1 RegistryPro Representations

Except as expressly stated in this CPS, RegistryPro makes no representations or warranties regarding its public service. RegistryPro reserves its right to modify such representations as it sees fit, at its sole discretion, or as required by law.

5.2 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.

5.3 Information Incorporated by Reference into a RegistryPro Digital Certificate

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

- Terms and conditions of the digital certificate.
- The Certificate Policy and any other applicable certificate policy as may be stated on an issued RegistryPro certificate, including the location of this CPS.
- The mandatory elements of the standard X.509v3.
- Any non-mandatory but customised 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.

5.4 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 customised 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.

5.5 Displaying Liability Limitations, and Warranty Disclaimers - RegistryPro

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

- An organisational unit attribute.
- A RegistryPro standard resource qualifier to a certificate policy.

- Proprietary or other vendors' registered extensions.

5.6 Displaying Liability Limitations, and Warranty Disclaimers - Comodo

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

5.7 Publication of Certificate Revocation Data

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

5.8 Duty to Monitor the Accuracy of Submitted Information

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

5.9 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.

5.10 Interference with RegistryPro Implementation

Subscribers, Relying Parties and any other parties shall not interfere with, or reverse engineer the technical implementation of RegistryPro 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 RegistryPro. Failure to comply with this 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 not yet paid under the Subscriber Agreement. Failure to comply with this will also result in the termination of the Relying Party Agreement with the Relying Party, the removal of permission to use or access the RegistryPro repository and any Digital Certificate or Service provided by RegistryPro.

5.11 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 not yet 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.

5.12 Standards

Comodo and RegistryPro each 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. Neither Comodo nor RegistryPro warrants that such user software will support and enforce controls required by Comodo or RegistryPro, whilst the user should seek appropriate advice.

5.13 RegistryPro Partnerships Limitations

Partners of the RegistryPro network shall not undertake any actions that might imperil, put in doubt or reduce the trust associated with the RegistryPro products and services. RegistryPro 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 Relying Party Agreement with the Relying Party, the removal of permission to use or access the RegistryPro repository and any Digital Certificate or Service provided by RegistryPro.

5.14 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.

5.15 RegistryPro Limitation of Liability for a RegistryPro Partner

As the RegistryPro network includes RAs that operate under RegistryPro practices and procedures RegistryPro warrants the integrity of any certificate specifically issued under its own root within the limits of the RegistryPro insurance policy.

5.16 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.

5.17 Choice of Cryptographic Methods

Parties are solely responsible for and have exercised independent judgement 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.

5.18 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 and by RegistryPro. 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 to risks that the Relying Party assumes in whole, and neither Comodo nor RegistryPro assumes in any way.

By means of this CPS Comodo and RegistryPro has each 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 <http://www.registrypro.pro/support/repository> or by contacting via out of bands means via the contact address as specified in the Document Control section of this CPS.

5.19 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

5.20 Refusal to Issue a Certificate

Comodo/RegistryPro 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/RegistryPro reserves the right not to disclose reasons for such a refusal.

5.21 Subscriber Obligations

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

- To minimise 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, a Comodo RA, RegistryPro or a RegistryPro RA.
- Ensure that the public key submitted to Comodo, a Comodo RA, RegistryPro or a RegistryPro RA corresponds with the private key used.
- Ensure that the public key submitted to Comodo, a Comodo RA, RegistryPro or a RegistryPro RA is the correct one.
- Provide correct and accurate information in its communications with Comodo, a Comodo RA, RegistryPro or a RegistryPro RA.
- Alert Comodo, a Comodo RA, RegistryPro or a RegistryPro RA if at any stage whilst the certificate is valid, any information originally submitted has changed since it had been submitted to Comodo and RegistryPro.
- Generate a new, secure key pair to be used in association with a certificate that it requests from Comodo, a Comodo RA, RegistryPro or a RegistryPro RA.
- Read, understand and agree with all terms and conditions in this Comodo/RegistryPro CPS and associated policies published in the Comodo Repository at www.comodogroup.com/repository and the RegistryPro Repository at <http://www.registrypro.pro/support/repository>.
- Refrain from tampering with a Comodo or RegistryPro certificate.
- Use Comodo and RegistryPro certificates for legal and authorised purposes in accordance with this suggested usages and practices CPS.
- Cease using Comodo and RegistryPro certificates if any information in any of them becomes misleading obsolete or invalid.
- Cease using Comodo and RegistryPro certificates if any of such certificates 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 or RegistryPro issued certificate to issue end-entity digital certificate or subordinate CAs.
- Make reasonable efforts to prevent the compromise, loss, disclosure, modification, or otherwise unauthorised use of the private key corresponding to the public key published in a Comodo or RegistryPro certificate.
- Request the revocation of a certificate in case of an occurrence that materially affects the integrity of a Comodo or RegistryPro certificate.
- For acts and omissions of partners and agents they use to generate, retain, escrow, or destroy their private keys.

5.22 Representations by Subscriber upon Acceptance

Upon accepting a certificate the Subscriber represents to Comodo and RegistryPro 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 unauthorised person has ever had access to the Subscriber's private key.
- All representations made by the Subscriber to Comodo or RegistryPro 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 and RegistryPro of any material inaccuracies in such information.
- The certificate is used exclusively for authorised and legal purposes, consistent with this CPS.
- It will use Comodo and RegistryPro certificates only in conjunction with the entity named in the organization field of a digital certificate (if applicable).
- The Subscriber retains control of the Subscriber's private key, use a trustworthy system, and take reasonable precautions to prevent its loss, disclosure, modification, or unauthorised 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 each of Comodo and RegistryPro.
- The Subscriber agrees with the terms and conditions of this CPS and other agreements and policy statements of each of Comodo and RegistryPro.
- 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.

5.23 Indemnity by Subscriber

By accepting a certificate, the Subscriber agrees to indemnify and hold Comodo and RegistryPro, as well as their respective parent companies, subsidiaries, directors, officers, employees, agents, 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/or RegistryPro, and/or 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 its agent(s).
- Any failure of the Subscriber to disclose a material fact, including, but not limited to, if the misrepresentation or omission was made negligently or with intent to deceive the CA, Comodo, RegistryPro, or any person receiving or relying on the certificate.
- Failure to protect the Subscriber's confidential data including the Subscriber's private key, or failure to take reasonable precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorised use of the Subscriber's confidential data.
- Breaking any applicable laws (including, but not limited to, the laws applicable in his/her country or territory and those related to intellectual property protection, viruses, accessing computer systems, etc.).

5.24 Obligations of RegistryPro Registration Authorities

A RegistryPro RA operates under the policies and practices detailed in this CPS and also the associated partner agreement.

The RA is bound under contract to:

- Receive applications for RegistryPro certificates in accordance with this CPS.
- Perform all verification actions prescribed by the RegistryPro validation procedures and this CPS.
- Receive, verify and relay to RegistryPro all requests for revocation of a RegistryPro certificate in accordance with the RegistryPro revocation procedures and the CPS.
- Act according to all applicable laws and regulations.

5.25 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.

5.26 Obligations of a Relying Party

A Relying Party accepts that in order to reasonably rely on a Comodo and/or RegistryPro certificate the Relying Party must:

- Minimise 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 and RegistryPro CPS and Relying Party Agreement.
- Verify the Comodo and RegistryPro certificates by referring to the relevant CRL and also the CRLs of intermediate CA and root CA as available in each of the Comodo and RegistryPro repositories.

- Trust a Comodo or RegistryPro certificate only if it is valid and has not been revoked or has expired.
- Rely on a Comodo or RegistryPro certificate, only as may be reasonable under the circumstances listed in this section and other relevant sections of this CPS.

5.27 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.

5.28 Subscriber Liability to Relying Parties

Without limiting other Subscriber obligations stated in this CPS, Subscribers are solely 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.

5.29 Duty to Monitor Agents

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

5.30 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 and hold harmless Comodo, RegistryPro, and their parent companies, subsidiaries, directors, officers, employees, agents, and contractors.

5.31 Conditions of usage of the RegistryPro Repository and Web site

Parties (including Subscribers and Relying Parties) accessing the RegistryPro Repository (<http://www.registrypro.pro/support/repository>) and official web site(s) agree with the provisions of this CPS and any other conditions of usage that RegistryPro may make available.

Parties demonstrate acceptance of the conditions of usage of the CPS by using a RegistryPro issued certificate.

Failure to comply with the conditions of usage of the RegistryPro Repositories and web site may result in termination of the relationship between RegistryPro and the party, at RegistryPro's sole discretion.

5.32 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.

5.33 Accuracy of Information

Each of Comodo and RegistryPro, recognising its trusted position, makes all reasonable efforts to ensure that parties accessing its Repositories receive accurate, updated and correct information. Comodo and RegistryPro, however, do not accept any liability beyond the limits set in this CPS and the Comodo and RegistryPro insurance policies.

Failure to comply with the conditions of usage of the Comodo and RegistryPro Repositories and web sites may result in termination of the relationship between Comodo/RegistryPro and the party.

5.34 Obligations of RegistryPro

Only to the extent specified in the relevant sections of the CPS, RegistryPro 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 RegistryPro 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 fulfil its obligations presented herein.
- Upon receipt of a request from an RA operating within the RegistryPro network act promptly to issue a RegistryPro certificate in accordance with the RegistryPro CPS.
- Upon receipt of a request for revocation from an RA operating within the RegistryPro network act promptly to revoke a RegistryPro certificate in accordance with the RegistryPro 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 RegistryPro has no further obligations under this CPS.

5.35 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 fulfil 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.

5.36 Fitness for a Particular Purpose

Comodo and RegistryPro each 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.

5.37 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, neither Comodo nor RegistryPro:

- Warrants 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 and/or RegistryPro except as it may be stated in the relevant product description below in this CPS and in the Comodo and RegistryPro insurance policies.
- Warrants the accuracy, authenticity, completeness or fitness of any information contained in Comodo and/or RegistryPro Personal certificates class 1, free, trial or demo certificates.
- Shall incur liability for representations of information contained in a certificate except as it may be stated in the relevant product description below in this CPS.
- Warrants the quality, functions or performance of any software or hardware device.
- Shall be liable if it cannot execute the revocation of a certificate for reasons outside its own control.
- Warrants the validity, completeness or availability of directories of certificates issued by a third party (including an agent) unless that is specifically stated by Comodo and/or RegistryPro.

5.38 Non-Verified Subscriber Information

Notwithstanding limitation warranties under the product section of this CPS, neither Comodo nor RegistryPro shall be responsible for non-verified Subscriber information submitted to Comodo and/or RegistryPro, or the Comodo and/or RegistryPro directories 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.

5.39 Exclusion of Certain Elements of Damages

In no event and under no circumstances (except for fraud or wilful misconduct) shall Comodo and/or RegistryPro be liable for any or all of the following and the results thereof:

- Any indirect, incidental or consequential damages.
- Any costs, expenses, or loss of profits.
- Any death or personal injury.
- 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, or 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 wilful 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.

5.40 Certificate Insurance Plan

Except to the extent of wilful misconduct, the cumulative maximum liability of Comodo and RegistryPro, whether jointly or severally as the case may be, for the issuance of a certificate containing invalid information pertaining to the certificate Subscriber that has been validated using the methods appropriate for the certificate class and/or type is laid out below:

5.40.1 ProSSL Certificate

Shall not exceed \$50.00 (fifty US dollars).

5.40.2 InstantSSL Certificate

Shall not exceed \$50.00 (fifty US dollars).

5.40.3 InstantSSL Pro Certificate

Shall not exceed \$2500.00 (two thousand five hundred US dollars).

5.40.4 PremiumSSL Certificate

Shall not exceed \$10,000.00 (ten thousand US dollars).

5.40.5 PremiumSSL Wildcard Certificate

Shall not exceed \$10,000.00 (ten thousand US dollars).

5.40.6 Intranet SSL Certificate

There is no liability of either Comodo or RegistryPro or both to anyone (including, but not limited to, applicants, Subscribers and Relying Parties).

5.40.7 Trial SSL Certificate

There is no liability of either Comodo or RegistryPro or both to anyone (including, but not limited to, applicants, Subscribers and Relying Parties).

5.41 Financial Limitations on Certificate Usage

Comodo and RegistryPro certificates may only be used in connection with data transfer and transactions having a US dollar (US\$) value no greater than the level of warranty associated with the certificate and detailed in section 5.40 of this CPS.

5.42 Damage and Loss Limitations

In no event and under no circumstances (except for fraud or wilful misconduct) will the aggregate liability of Comodo and RegistryPro, whether jointly or severally, 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 applicable liability cap for such certificate as stated in the Comodo and RegistryPro insurance plans detailed section 5.40 of this CPS.

5.43 Conflict of Rules

- If/when this CPS conflicts with other rules, guidelines, or contracts, this CPS, dated 7 May 2004, shall prevail and bind the Subscriber and other parties. If there is any conflict between the sections of this CPS (and/or any other document) that relate to Comodo and the section of this CPS (and/or any other document) that relate to RegistryPro, then the sections benefiting RegistryPro and preserving RegistryPro's best interest, at RegistryPro's sole determination, shall prevail and bind the applicable parties.

5.44 RegistryPro Intellectual Property Rights

RegistryPro, its partners, and its associates each own all their respective intellectual property rights associated with their databases, web sites, RegistryPro digital certificates and any other publication originating from RegistryPro including the CPS.

5.45 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.

5.46 Infringement and Other Damaging Material

Comodo and RegistryPro subscribers represent and warrant that when submitting to Comodo and RegistryPro 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.

Certificate Subscribers shall defend, indemnify, and hold Comodo and RegistryPro 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 and RegistryPro whether jointly or severally.

5.47 Ownership

Certificates are the exclusive property of RegistryPro. RegistryPro gives permission to reproduce and distribute certificates on a non-exclusive, royalty-free basis, provided that they are reproduced and distributed in full. RegistryPro reserves the right to revoke the certificate at any time and at its sole discretion.

Private and public keys are the property of the Subscribers who rightfully issue and hold them.

All secret shares (distributed elements) of the Comodo and RegistryPro private keys remain the respective property of Comodo and RegistryPro.

5.48 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 and/or RegistryPro digital certificates or other products and services. English law applies in all of Comodo and/or RegistryPro commercial or contractual relationships in which this CPS may apply or quoted implicitly or explicitly in relation to Comodo and/or RegistryPro products and services where Comodo and/or RegistryPro acts as a provider, supplier, beneficiary receiver or otherwise.

5.49 Jurisdiction

Each party, including Comodo and RegistryPro 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 and RegistryPro PKI services.

5.50 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) the parties agree to notify Comodo and RegistryPro of the dispute with a view to seek dispute resolution.

5.51 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 that this CPS applies to. 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.

5.52 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 remain in full force and effect and shall be interpreted in such manner as to implement the original intention of the parties to the fullest extent possible.

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. **[Comment: What is the purpose of this and how does this further that purpose?]**

5.53 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 the parties shall also take into account the international scope and application of the services and products of Comodo, RegistryPro and their international networks of Registration 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.

5.54 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.

5.55 Notice

Comodo and RegistryPro each 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 or RegistryPro or both, as the case may be, 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
New Court
Regents Place
Regent Road
Salford
Greater Manchester
M5 4HB
United Kingdom

Attention: Legal Practices

Email: legal@comodogroup.com

[Comment: What about RegistryPro's contact information for notices?]

This CPS, related agreements and Certificate policies referenced within this document are available online at www.comodogroup.com/repository and <http://www.registrypro.pro/support/repository>.

5.56 Fees

Comodo and RegistryPro charges Subscriber fees for some of the certificate services it offers, including issuance, renewal and reissues (in accordance with the Comodo and RegistryPro Reissue Policies stated in 5.57 of this CPS). Such fees are detailed on the official Comodo websites (www.comodogroup.com and www.instantssl.com) and RegistryPro web site (www.registrypro.pro)

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

RegistryPro retains its right to affect changes to such fees. RegistryPro partners, will be suitably advised of price amendments as detailed in the relevant partner agreements.

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.

5.57 RegistryPro Reissue Policy

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

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

5.58 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.

5.59 RegistryPro Refund Policy

RegistryPro 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.

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

5.60 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.

5.61 Independent Contractors

The parties hereto, including, but not limited to, Comodo and RegistryPro are independent contractors in relation to each other at all times and will have no right or authority to create any obligation on behalf of any of the other parties, except as may be expressly provided in this CPS.

6 General Issuance Procedure

6.1 General - RegistryPro

RegistryPro 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 RegistryPro will validate an application in accordance with this CPS which may involve the applicant providing RegistryPro with relevant official documentation supporting the application.

RegistryPro certificates are issued to professional organizations or individuals.

The validity period of RegistryPro certificates varies dependent on the certificate type, but typically a certificate will be valid for either 1 year, 2 years or 3 years. RegistryPro reserves the right to, at its sole discretion, issue certificates that may fall outside of these set periods.

6.2 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.

6.3 Certificates issued to Individuals and Organisations

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

On-line: Via the Web (<https> **[Comment: What's the URL?]**). The certificate applicant submits an application via a secure on-line link according to a procedure provided by Comodo or RegistryPro, as the case may be. Additional documentation in support of the application may be required so that Comodo or RegistryPro verifies the identity of the applicant. The applicant submits to Comodo or RegistryPro such additional documentation. Upon verification of identity, Comodo or RegistryPro 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 or RegistryPro or both, as the case may be, 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 and/or RegistryPro may at its sole discretion accept or reject applications via email.

6.4 Content

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

6.4.1 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/RegistryPro).
- Applicant's public key.
- Comodo digital signature. **[Comment: RegistryPro digital signature? (Just making sure if applicable or not.)]**
- Type of algorithm.
- Validity period of the digital certificate.
- Serial number of the digital certificate.

6.4.2 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/RegistryPro).
- Comodo digital signature. **[Comment: RegistryPro digital signature? (Just making sure if applicable or not.)]**
- Type of algorithm.
- Validity period of the digital certificate.
- Serial number of the digital certificate.

6.5 Time to Confirm Submitted Data

Comodo and RegistryPro each makes reasonable efforts to confirm certificate application information and issue a digital certificate within 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 and RegistryPro each aims to confirm submitted application data and to complete the validation process and issue or reject a certificate application within 2 working days.

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

6.6 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 or RegistryPro's web site and the applicant submits the required information: Certificate Signing Request (CSR), e-mail address, common name, organisational 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/RegistryPro.
- d) The applicant pays the certificate fees.
- e) Comodo/RegistryPro verifies the submitted information using third party databases and Government records
- f) Upon successful validation of the application information, Comodo/RegistryPro may issue the certificate to the applicant or should the application be rejected, Comodo/RegistryPro 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/RegistryPro websites.
- h) Revocation is conducted as per the procedures outlined in this CPS.

Document Control

This document is version 2.2 of the Comodo CPS incorporating Registry Services Corporation CPS, created on 7 May 2004 and signed off by the Comodo Certificate Policy Authority

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

URL: <http://www.comodogroup.com>

E-mail: legal@comodogroup.com

Tel: +44 (0) 161 874 7070

Fax: +44 (0) 161 877 1767

Copyright Notice

Copyright Comodo CA Limited 2004. 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 Limited
New Court,
Regents Place,
Regent Road,
Manchester
M5 4HB
United Kingdom

The trademarks "Comodo" and "TrustToolbar" are registered trademarks of Comodo CA Limited.

The trademarks "RegistryPro", "ProSSL" and "ProCert" are registered trademarks of Registry Services Corporation