Dual Use Certificate Addendum to the Comodo Certification Practice Statement v.3.0

Beginning April 1, 2008, Comodo CA Ltd. ("Comodo") will offer a new type of certificate called Dual Use Certificates. These certificates are high assurance identification certificates will be issued by Comodo and its RA's through the Comodo Certificate Manager software to Subscribers. The purpose of this Addendum to the Comodo Certification Practice Statement ("ACPS") is to amend version 3.0 of the Comodo Certification Practice Statement ("CPS") to include information and details on how these certificates will work, the purposes of the new program, and the validation procedures behind the certificates issued using the Certificate Manager. All provisions of the CPS not specifically amended or added herein remain in full force and effect and where applicable shall apply to the new product offerings. Only the amended portions in this ACPS are included herein. Nothing in the CPS shall be deemed omitted, deleted or amended unless expressly stated in this ACPS. Headings from the CPS are included to identify the location of the Amended information, and are not intended to be duplicative.

1 General

. . .

1.4 Other Practice Statements

. . .

Comodo Dual Use Certificate Subscriber Agreement	Public	Comodo Repository

. . .

1.8 Comodo PKI Hierarchy

. . .

1.8.12 Dual Use Certificates

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

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

. . .

2.4 Types of Comodo Certificates

e) Comodo Dual Use Certificates

Comodo Dual Use Certificates are high assurance certificates used as email and identification certificates that are issued through the Certificate Manager software to the end users of the Certificate Manager subscriber. These certificates are used for secure remote access to the subscriber's computer networks by its employees, agents, and contractors as well as providing these individuals with secure email services.

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

. . .

2.6 Subscriber Private Key Generation Process

. . .

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

. . .

2.9.7 Comodo Dual Use Certificates

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

. . .

2.12.4 Certificate Policy (CP)

. . .

Comodo Secure Server Certificate – Secure Email Certificate (Free Version) / Secure Email Certificate (Corporate Version) / Custom Client Certificates / Comodo TF / Dual Use Certificates		
Signature Algorithm	Sha1	
Issuer (option 1)	CN	Comodo Class 3 Security Services CA
	OU	(c) 2002 Comodo CA Limited
	OU	Terms and Conditions of use: http://www.comodo.net/repository
	OU	Comodo Trust Network
	O	Comodo Limited
	C	GB
Issuer (option 2)	CN	UTN-USERFirst-Client Authentication and Email
	OU	http://www.usertrust.com
	O	The USERTRUST Network
	L	Salt Lake City
	S	UT
	C	US
Issuer (option 3)	CN	Comodo Class 3 Security Services CA
	OU	(c) 2006 Comodo CA Limited
	OU	Terms and Conditions of use: http://www.comodo.com/repository
	OU	Comodo Trust Network
	O	Comodo CA Limited
	C	GB
Validity	1 year / 2 year / 3 year	
Subject (for Free version)	E	*Email address*
	CN	*Common Name (name of subscriber)*
	OU	(c)2003 Comodo Limited
	OU	*Terms and Conditions of use: http://www.comodo.net/repository*

	OU	Comodo Trust Network - PERSONA NOT VALIDATED
Subject (for Corporate version)	E	Email address
	CN	Common Name (name of subscriber)
	OU	Corporate Secure Email
	OU (0 or 1 of)	Hosted by [Web Host Reseller Subscriber Name] Issued through [EPKI Manager Subscriber Name] Provided by [Powered SSL Subscriber Name]
	O	Organization
	OU	Organization Unit
	L	Locality
	STREET	Street
	S	State
	PostalCode	Zip or Postal Code
	C	Country
Subject (for Custom Client. Comodo TF version, and Dual Use Certificates)	All fields are customizable on a per-certificate basis.	
Authority Key Identifier	KeyID only is specified.	
Key Usage (NonCritical) (Free Version Only)	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)	
Key Usage (NonCritical) (Corporate and Custom Client versions)	Secure Email (1.3.6.1.5.5.7.3.4) Client Authentication (1.3.6.1.5.5.7.3.2)	
Netscape Certificate Type (Corporate Version Only)	SSL Client Authentication, SMIME (a0)	
Netscape Certificate Type (Free and Custom Client versions)	SMIME(20)	
Basic Constraint	Subject Type = End Entity Path Length Constraint = None	
Certificate Policies	[1] Certificate Policy: PolicyIdentifier = 1.3.6.1.4.1.6449.1.2.1.3.5 [1,1]Policy Qualifier Info: Policy Qualifier Id = CPS Qualifier: https://secure.comodo.net/CPS	
CRL Distribution Policies	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=<Primary CDP URL> [2]CRL Distribution Point Distribution Point Name: Full Name: URL=<Secondary CDP URL>	
(Only for certificates issued by "Comodo Class 3 Security Services CA")	[3]CRL Distribution Point Distribution Point Name: Full Name: RFC822 Name=<CRL Request Email Address>	

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

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

. . .

4.1 Certificate Application Requirements

. . .

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

- Generate a RSA key pair and demonstrate to Comodo ownership of the private key half of the key pair through the submission of a valid PKCS#10 Certificate Signing Request (CSR) (or SPKAC request for certain Comodo TF or Dual Use certificates)
- Make all reasonable efforts to protect the integrity the private key half of the key pair
- Submit to Comodo a certificate application, including application information as detailed in this CPS, a public key half of a key pair, and agree to the terms of the relevant subscriber agreement
- Provide proof of identity through the submission of official documentation as requested by Comodo during the enrolment process

. . .

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

. . .

4.2.12 Comodo Dual Use Certificates

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

. . .

5.31 Certificate Insurance Plan

. . .

Comodo Dual Use Certificate	$0	$0

. . .

Document Control

This document is the Dual Use Certificate Addendum to Comodo CPS Version 3.0, created on 25 March 2008 and signed off by the Comodo Certificate Policy Authority.

Comodo CA Limited
3rd Floor, Office Village, Exchange Quay, Trafford Road,
Salford, Manchester, M5 3EQ, United Kingdom
URL: http://www.comodogroup.com

Email: legal@comodogroup.com

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