High Assurance SSL Sub CA Addendum to the Comodo Certification Practice Statement v.3.0

Comodo CA, Ltd.
High Assurance SSL Sub-CA Addendum to Version 3.0 Amendments
21 October 2008

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

Begining October 29, 2008 , Comodo CA Ltd. (“Comodo”) will begin to issue High Assurance SSL Certificates from its Comodo High Assurance Secure Server CA intermediary certificate. 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 the hierarchy and crl addresses for the certificate chain. 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

. . .

1.8 Comodo PKI Hierarchy

. . .

1.8.2 1-5 year certificates (InstantSSL and EnterpriseSSL)

Entrust Certificates

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

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

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

GTE Certificates

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

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

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

UTN/AddTrust certificates – InstantSSL and EnterpriseSSL CA

Visible on IE compatible browsers as follows:

UTN-USERFIRST-Hardware (*serial number = 44 be 0c 8b 50 00 24 b4 11 d3 36 2a fe 65 0a fd, expiry = 09 July 2019 19:19:22*)

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

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

AddTrust External CA Root (*serial number = 01, expiry = 30/05/2020 10:48:38*)

↳ UTN-USERFirst-Hardware (serial number = 48 4b ac f1 aa c7 d7 13 43 d1 a2 74 35 49 97 25, expiry = 30 May 2020 11:48:38)

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

Comodo *Certification Authority Certificates*

Visible on IE compatible browsers as follows:

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

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

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

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

AddTrust External CA Root (*serial number = 01, expiry = 30/05/2020 10:48:38*)

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

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

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

. .

1.8.5 Comodo SGC / Platinum SGC / Multi-Domain certificates

UTN Certificates

Visible on IE compatible browsers as follows:

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

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

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

AddTrust External CA Root (*serial number = 01, expiry = 30/05/2020 10:48:38*)

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

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

Comodo Certification Authority Certificates

Visible on IE compatible browsers as follows:

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

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

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

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

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

AddTrust External CA Root (*serial number = 01, expiry = 30/05/2020 10:48:38*)

↳ UTN - DATACorp SGC (*serial number = 53 7b 76 56 4f 29 7f 14 dc 69 43 e9 22 ad 2c 79, expiry = 30 May 2020 11:48:38*)

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

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

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

. . .

1.12 Relying Parties

. . .

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

. . .

2.1.1 Root CA Signing Key Protection and Recovery

. . .

90	Comodo Certification Authority	High Assurance SSL Certificates	31 Dec 2029	2048

. . .

153	Comodo High Assurance Secure Server CA	Intermediate for High Assurance SSL Certificates	31 Dec 2029	2048

. . .

2.3 Comodo Directories, Repository and Certificate Revocation Lists

Comodo manages and makes publicly available directories of revoked certificates using Certificate Revocation Lists (CRLs). All CRLs issued by Comodo are X.509v2 CRLs, in particular as profiled in RFC3280. Users and relying parties are strongly urged to consult the directories of revoked certificates at all times prior to relying on information featured in a certificate. Comodo updates and publishes a new CRL every 24 hours or more frequently under special circumstances. The CRL for end entity certificates can be accessed via the following URLs:

http://crl.comodo.net/Class3SecurityServices_3.crl
http://crl.comodoca.com/Class3SecurityServices 3.crl
http://crl.comodoca.com/ComodoHighAssuranceSecureServerCA.crl

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

. . .

2.12.4 Certificate Policy (CP)

. .

Comodo Secure Server Certificates – InstantSSL / ProSSL / PremiumSSL / PremiumSSL Wildcard / EliteSSL /GoldSSL / PlatinumSSL / PlatinumSSL Wildcard / PremiumSSL Legacy / PremiumSSL Legacy Wildcard / PlatinumSSL Legacy / PlatinumSSL Legacy Wildcard / PlatinumSSL SGC Legacy / PlatinumSSL SGC Legacy Wildcard / Comodo SGC SSL / Comodo SGC SSL Wildcard / Trial SSL / Intranet SSL / Other SSL Certificates		
Signature Algorithm	Sha1	
Issuer (option 1) **(not for any SGC type)**	CN	Comodo Class 3 Security Services CA
	OU	(c) 2002 Comodo Limited
	OU	Terms and Conditions of use: http://www.comodo.net/repository
	OU	Comodo Trust Network
	O	Comodo Limited
	C	GB
Issuer (option 2) **(not for any SGC type)**	CN	UTN-USERFIRST-Hardware
	OU	http://www.usertrust.com
	O	The USERTRUST Network
	L	Salt Lake City
	S	UT
	C	US
Issuer (option 3) **for SGC types only.**	CN	UTN - DATACorp SGC
	OU	http://www.usertrust.com
	O	The USERTRUST Network
	L	Salt Lake City
	S	UT
	C	US
Issuer (option 4) **(not for any SGC type)**	CN	Comodo Class 3 Security Services CA
	OU	(c) 2006 Comodo CA Limited
	OU	Terms and Conditions of use: http://www.comodo.com/repository
	OU	Comodo Trust Network
	O	Comodo CA Limited
	C	GB
Issuer (option 5)	CN	Comodo High Assurance Secure Server CA
	OU	© 2008 Comodo CA Limited

	OU	Terms and Conditions of use: http://www.comodo.com/repository
	OU	Comodo Trust Network
	O	Comodo CA Limited
	C	GB
Validity	1 year / 2 year / 3 year / 4 year / 5 year	
Subject	CN	Common Name
	OU	InstantSSL / ProSSL/PremiumSSL / PremiumSSL Wildcard / EliteSSL /GoldSSL / PlatinumSSL / PlatinumSSL Wildcard / PremiumSSL Legacy / PremiumSSL Legacy Wildcard / PlatinumSSL Legacy / PlatinumSSL Legacy Wildcard / PlatinumSSL SGC Legacy / PlatinumSSL SGC Legacy Wildcard / Comodo SGC SSL / Comodo SGC SSL Wildcard / *Other SSL Certificate name / Powered SSL product name*
	OU (0 or 1 of)	*Hosted by [Web Host Reseller Subscriber Name]* *Issued through [EPKI Manager Subscriber Name]* *Provided by [Powered SSL Subscriber Name]*
	OU (for Intranet SSL only)	INTRANET USE ONLY – NO WARRANTY ATTACHED – COMPANY NOT VALIDATED
	OU (for Trial SSL only)	TEST USE ONLY - NO WARRANTY ATTACHED
	O	Organization
	OU	Organization Unit
	L	Locality
	STREET	Street
	S	State
	PostalCode	Zip or Postal Code
	C	Country
Authority Key Identifier	KeyID only is specified.	
Key Usage (NonCritical)	Digital Signature, Key Encipherment(A0)	
Extended Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	
(Additional usages for SGC types only)	Microsoft SGC (1.3.6.1.4.1.311.10.3.3) Netscape SGC (2.16.840.1.113730.4.1)	
Netscape Certificate Type	SSL Client Authentication, SSL Server Authentication(c0)	
Basic Constraint	Subject Type = End Entity Path Length Constraint = None	
Certificate Policies	[1] Certificate Policy: PolicyIdentifier = 1.3.6.1.4.1.6449.1.2.1.3.4 [1,1]Policy Qualifier Info: Policy Qualifier Id = CPS Qualifier: https://secure.comodo.net/CPS	

CRL Distribution Policies	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=<Primary CDP URL> [2]CRL Distribution Point Distribution Point Name: Full Name: URL=<Secondary CDP URL>
(only when the Issuing CA is "Comodo Class 3 Security Services CA")	[3]CRL Distribution Point Distribution Point Name: Full Name: RFC822 Name=<CRL Request Email Address>
Authority Information Access (omitted when Issuing CA is "Comodo Class 3 Security Services CA") (non-critical)	*[1]Authority Info Access* *Access Method = id-ad-calssuers (1.3.6.1.5.5.7.48.2)* *URL=<Primary AIA URL>* *[2]Authority Info Access* *Access Method = id-ad-ocsp (1.3.6.1.5.5.7.48.1)* URL = http://ocsp.comodo.com
Thumbprint Algorithm	SHA1
Thumbprint	

. .

Comodo MDC		
Signature Algorithm	Sha1	
Issuer (Option 1)	CN	UTN - DATACorp SGC
	OU	http://www.usertrust.com
	O	The USERTRUST Network
	L	Salt Lake City
	S	UT
	C	US
Issuer (Option 2)	CN	Comodo High Assurance Secure Server CA
	OU	© 2008 Comodo CA Limited
	OU	Terms and Conditions of use: http://www.comodo.com/repository
	OU	Comodo Trust Network
	O	Comodo CA Limited
	C	GB
Validity	1 Year / 2 Year / 3 Year	
Subject	CN	Common Name [Name Windows displays as "Issued To" – Typically Entity Name like O field]
	OU	*Hosted by [Web Host Reseller Subscriber Name]* *Issued through [EPKI Manager Subscriber Name]* *Provided by [Powered SSL Subscriber Name]*
	O	*Organisation*
	OU	*Organisation Unit*
	L	*Locality*
	S	*Street*
	C	*Country*
	CN	*Domain Name 1*

<table>
<tr><td rowspan="3"></td><td>CN</td><td><em>Domain Name 2</em></td></tr>
<tr><td>CN</td><td><em>Domain Name 3 (etc to Domain Name 100)</em></td></tr>
<tr><td>CN</td><td>Common Name [Name Windows displays as “Issued To” – Typically Entity Name like O field]</td></tr>
<tr><td>Enhanced Key Usage</td><td colspan="2">Server Authentication (1.3.6.1.5.5.7.3.1)
Client Authentication (1.3.6.1.5.5.7.3.2)
Microsoft SGC (1.3.6.1.4.1.311.10.3.3)
Netscape SGC (2.16.840.1.113730.4.1)</td></tr>
<tr><td>Key Usage (NonCritical)</td><td colspan="2">Digital Signature , Key Encipherment(A0)</td></tr>
<tr><td>Netscape Certificate Type</td><td colspan="2">SSL Client Authentication, SSL Server Authentication(c0)</td></tr>
<tr><td>Basic Constraint</td><td colspan="2">Subject Type=End Entity
Path Length Constraint=None</td></tr>
<tr><td>Certificate Policies</td><td colspan="2">[1]Certificate Policy:
Policy Identifier=1.3.6.1.4.1.6449.1.2.1.3.4
[1,1]Policy Qualifier Info:
Policy Qualifier Id=CPS
Qualifier:
https://secure.comodo.net/CPS</td></tr>
<tr><td>CRL Distribution Points</td><td colspan="2">[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&gt;</td></tr>
<tr><td>Authority Information Access
(non-critical)</td><td colspan="2"><em>[1]Authority Info Access
Access Method = id-ad-caIssuers (1.3.6.1.5.5.7.48.2)
URL=<Primary AIA URL>
[2]Authority Info Access
Access Method = id-ad-ocsp (1.3.6.1.5.5.7.48.1)
URL = http://ocsp.comodo.com</em></td></tr>
<tr><td>Subject Alternate Name</td><td colspan="2"><em>DNS Name=Domain Name 1
DNS Name=Domain Name 2
DNS Name=Domain Name 3
….up to
DNS Name=Domain Name 100</em></td></tr>
<tr><td>Thumbprint Algorithm</td><td colspan="2">SHA1</td></tr>
<tr><td>Thumbprint</td><td colspan="2"></td></tr>
</table>

. .

4.13.2 Effect of Revocation

Upon revocation of a certificate, the operational period of that certificate is immediately considered terminated. The serial number of the revoked certificate will be placed within the Certificate Revocation List (CRL) and remains on the CRL until some time after the end of the certificate’s validity period. An updated CRL is published on the Comodo website every 24 hours; however, under special circumstances the CRL may be published more frequently. In addition, Comodo’s systems are configured to pre-generate OCSP responses using the private key of the certificate. This provides real-time information regarding the validity of the Certificate making the revocation information immediately available through the OCSP.

. .

5.12 Reliance on Unverified Digital Signatures

Parties relying on a digital certificate must verify a digital signature at all times by checking the validity of a digital certificate against the relevant CRL published by Comodo or using the Comodo OCSP responder. Relying parties are alerted that an unverified digital signature cannot be assigned as a valid signature of the subscriber.

. .

5.19 Obligations of a Relying Party

A party relying on a Comodo certificate accepts that in order to reasonably rely on a Comodo certificate they must:

- Minimize the risk of relying on a digital signature created by an invalid, revoked, expired or rejected certificate; the relying party must have reasonably made the effort to acquire sufficient knowledge on using digital certificates and PKI.
- Study the limitations to the usage of digital certificates and be aware through the Relying Party agreement the maximum value of the transactions that can be made using a Comodo digital certificate.
- Read and agree with the terms of the Comodo CPS and relying party agreement.
- Verify a Comodo certificate by referring to the relevant CRL and the CRLs of intermediate CA and root CA or by checking the OCSP response using the Comodo OCSP responder.
- Trust a Comodo certificate only if it is valid and has not been revoked or has expired.
- Rely on a Comodo certificate, only as may be reasonable under the circumstances listed in this section and other relevant sections of this CPS.

. .

Document Control
This document is the High Assurance SSL Sub-CA Addendum to Comodo CPS Version 3.0, created on 16 October 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

Copyright Notice

Salford, Manchester, M5 3EQ, United Kingdom