Validation and Code Signing Certificate Addendum (Revised) to the Comodo Certification Practice Statement v.3.0

Comodo CA, Ltd.
Code Signing Certificate Addendum to Version 3.0 Amendments
July 29, 2011

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

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 additional information regarding Code Signing Certificates and the validation process of Certificates. 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.

. . . .

4.8 Certificate Validity

Certificates are valid upon issuance by Comodo and acceptance by the subscriber. Generally, the certificates validity period will be from 1 to 10 years, however, Comodo reserves the right to offer validity periods outside of this standard validity period. Comodo verifies all information that is included in SSL certificates at time intervals of thirty-nine months or less.

. . . .

1.13 Comodo Time-Stamping Authority

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

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

. . . .

3.7 Availability of Revocation Data

Comodo publishes Certificate Revocation Lists (CRLs) to allow relying parties to verify a digital signature made using a Comodo issued digital certificate. Each CRL contains entries for all revoked un-expired certificates issued and is valid for 24 hours. Comodo issues a new CRL every 24 hours and includes a monotonically increasing sequence number for each CRL issued. Under special circumstances, Comodo may publish new CRLs prior to the expiry of the current CRL. All expired CRLs are archived (as described in section 3.4 of this CPS) for a period of 7 years or longer if applicable. For Code Signing Certificates revoked due to key compromise or that have been issued to unauthorized persons, Comodo will maintain certificate information on CRLs for at least 20 years.

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

. . . .

4.2.1 Secure Server and Code Signing Certificates Validation Process

Comodo utilizes a two-step validation process prior to the issuance of a Secure Server Certificate and a Code Signing Certificate. Comodo may at its discretion require addition steps to validate.

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

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

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

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

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

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

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

. . . .

4.2.8 Code Signing Certificate / Time Stamping Certificate

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

Document Control
This document is the Code Signing Certificate Addendum (Revised) to the Comodo CPS Version 3.0, created on July 18, 2010 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