Private Key Escrow Addendum to the Comodo Certification Practice Statement v.3.0

Comodo CA, Ltd.
Private Key Escrow Addendum to Version 3.0 Amendments
1 March 2010

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

Beginning March 9, 2010, Comodo CA Ltd. ("Comodo") will offer private key escrow services for its certificates. The private key escrow services will be available through special Comodo software operated on Comodo servers. 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 Comodo's private key escrow services will function. All provisions of the CPS not specifically amended or added herein remain in full force and effect. 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.

2.2 Digital Certificate Management

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

- Verification of the identity of an applicant of a certificate.
- Authorizing the issuance of certificates.
- Issuance of certificates.
- Revocation of certificates.
- Listing of certificates.
- Distributing certificates.
- Publishing certificates.
- Storing certificates.
- Storing private keys

[• Escrowing private keys]

- Generating, issuing, decommissioning, and destruction of key pairs
- Retrieving certificates in accordance with their particular intended use.
- Verification of the domain of an applicant of a certificate.

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

2.6 Subscriber Private Key Generation Process

The Subscriber is solely responsible for the generation of the private key used in the certificate request. However, for certain products, Comodo does provide the option of key generation, escrow, recovery, and backup facilities for private keys. Keys generated by Comodo are generated during the order process for the certificate. Where keys are backed-up or escrowed, the keys are generated on Comodo's servers and then delivered to the subscriber over an encrypted communication. At the request of certain qualifying subscribers, Comodo will escrow the private keys it generates by encrypting the private key and storing it on a Comodo server.

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

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

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

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

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

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

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

2.7 Subscriber Private Key Protection and Backup

Generally, the Subscriber is solely responsible for protection of their private keys. However, Comodo offers certain subscribers the optional feature of having Comodo back up the private keys Comodo generates on their behalf. Comodo protects these keys by having an agent or agents of the Certificate Manager Subscriber (typically, the employer of the individual receiving the client certificate) encrypt a PKCS#12 format that contains the keys before they are stored on a secure server. Keys stored by Comodo can only be decrypted using the keys held by the selected agents of the Certificate Manager Subscriber. Encrypted keys are sent via a secure connection and decrypted by the agent of the Certificate Manager Subscriber on their own computers.

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

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

Comodo strongly urges Subscribers to use a strong password or authentication method of equivalent or greater strength than the key being protected to prevent unauthorized access and use of the Subscriber private key.

. . .

Document Control
This document is the Private Key Escrow Addendum to Comodo CPS Version 3.0, created on 1 October 2009 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
Copyright Comodo CA Limited 2009. 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
3rd Floor, Office Village, Exchange Quay, Trafford Road,
Salford, Manchester, M5 3EQ, United Kingdom