



**ComSign Ltd.™**

**Security Certificate Approval Regulations  
For SSL Websites (CPS)**

Version 1.2

Publication date: [14/12/2008 ]

Recommended effective date: [14/12/2008]

ComSign

Building 4, Kiryat Atidim, Tel Aviv

Copyrights © ComSign. 2007

All Rights Reserved

**ComSign – CPS © 2007 All Rights Reserved**

Without limiting the rights reserved above, and except for the license which will be granted as follows, no part of this publication may copied, stored or entered into a retrieval system, or broadcast and transferred in any form whatsoever (either electronically or mechanically, by photocopying or recording or any other way) without prior written permission from ComSign.

# Contents

<b>1. Introduction.....</b>	<b>4</b>
1.1 Executive summary.....	4
1.2 ComSign’s database.....	4
1.3 Publishing by ComSign’s database.....	4
<b>2. Regulations for handling requests to issue SSL certificates .....</b>	<b>4</b>
<b>3. Verification of certificate issuing requests .....</b>	<b>5</b>
3.1 Requirements regarding verifying requests to issue a certificate .....	5
3.2 Rejecting a request to issue a certificate .....	5
<b>4. Certificate revocation .....</b>	<b>6</b>
4.1 Reasons, in general, for revoking certificates .....	6
4.2 Notification and confirmation in case of revocation.....	6
<b>5. Certificate expiry .....</b>	<b>7</b>
5.1 Advance notification about certificate expiry.....	7
5.2 The outcome of certificate expiry regarding secrecy obligations.....	7
5.3 Certificate renewal .....	7
<b>6. The certificate authority and ComSign’s obligations, and the limitations on these obligations.....</b>	<b>7</b>
6.1 Policy regarding money refunds .....	7
6.2 Limited liability and other obligations.....	7
6.3 The certificate authority and ComSign’s liability repudiation and obligation limitation.....	8

6.4	Exclusion of certain fundamental damage .....	8
6.5	Limitations on loss and damage fees .....	9
6.6	The subscriber’s liability towards a reliant party.....	10
6.7	The absence of a trust relationship.....	10
6.8	Dangerous activities.....	10
<b>7. Miscellaneous provisions.....</b>		<b>10</b>
7.1	Contradictory instructions.....	10
7.2	Legal existence and export regulations.....	11
7.3	The applicable law .....	11
7.4	Interpretation and translation .....	11
7.5	Non-waiver .....	11
7.6	Notification .....	11

# 1. Introduction

## 1.1 Executive summary

This CPS details and regulate the **SSL** certificate issuing procedure **and does not refer to issuing private certificates.**

## 1.2 ComSign's database

ComSign's database is a collection of databases open to the public, which is meant for storing and retrieving certificates and other information connected to them. All certificate authorities must use ComSign's database as the main and official database for all ComSign certificate issuing services purposes. The database includes, among others, the following items: Certificates, a certificate revocation list (CRL) and other information about revoking certificates, current and previous versions of ComSign's CPS, and other information as will be decided periodically by ComSign.

## 1.3 Publication by ComSign's database

ComSign's database will act without delay to publish certificates, CPS amendments, and certificate revocation notifications (CRL). The CRL may be viewed at <http://crl.comsign.co.il/crl/ServerCA.crl>, as well as other information in a way which is in line with this CPS and the applicable law. ComSign's database may be accessed at <https://www.comsign.co.il/cps> and via other means of communication as determined periodically by ComSign.

# 2. Regulations for handling requests to issue SSL certificates

This paragraph describes the procedure for handling requests to issue SSL certificates. It includes the requirements regarding creating a pair of keys and their protection, and details the approvals required.

All organizations interested in a certificate must act in accordance with the following general regulations for every certificate request:

- Create a pair of keys on the server where the certificate needs to be installed.

- Provide ComSign with a confirmation of the organization's registration.
- Provide ComSign with the details of 2 of the organization's employees, who are authorized to request a certificate in the company's name and have the knowledge to use it correctly.

### **3. Verification of certificate issuing requests**

#### **3.1 Requirements regarding verifying requests to issue a certificate**

Upon receipt of a request to issue a security certificate, the following inspections are performed:

The certificate authority will confirm that:

- (a) The organization requesting the certificate is registered and the company still in operation by one of the following:
  - a. Checking the organization's registration in the D&B website.
  - b. Checking the organization's registration at the registrar of companies/fellowship societies.
  - c. Receiving an official document from the a certified authority confirming the organization's existence.
- (b) An investigation will be performed to confirm that the domain for which the certificate is requested is registered in the organization's name.
- (c) A telephone call will be made to the organization in order to verify the order and confirm the contact people's details as provided to ComSign.

Upon issuing a certificate, the certificate authority will not be obligated to continually monitor and investigate the accuracy of the information included in the certificate unless, in accordance with this CPS, the certificate authority is given notification concerning damage to this certificate.

#### **3.2 Rejecting a request to issue a certificate**

In cases where the verification fails, the relevant certificate authority will send the client an email detailing the approvals missing for approving the certificate.

If the client does not present the approvals required, their request will be rejected and the certificate cannot be approved until the required approvals are presented.

## **4. Certificate revocation**

### **4.1 Reasons, in general, for revoking certificates**

A certificate will be revoked if:

- The security certificate's personal key, which was issued for a website, has been stolen, lost, changed or revealed without authorization, or if any other damage was caused to it.
- A senior representative on behalf of the organization (or another authorized representative on its behalf) legally requests it.

### **4.2 Notification and confirmation in case of revocation**

If a certificate is revoked, the certificate authority must publish a notification in ComSign's database regarding the revocation.

A certificate authority is entitled to publish one or more of the following notifications:

- The certificate revocation list which can be accessed via a secure channel <http://crl1.comsign.co.il/crl/ServerCA.crl>.
- The certificate revocation list (CRL) will be published once every 24 hours.

Certificate authorities are also entitled to provide the following services for delivering revocation notifications according to request and after payment of commission by the requester.

- Provide an "expediting service" to deliver notifications from the certificate authority to the revocation requester of certain certificates.

## **5. Certificate expiry**

### **5.1 Advance notification about certificate expiry**

The certificate authorities must make reasonable efforts to notify subscribers, via email, that the expiry date of their certificates is drawing near. This notification is meant only for the subscriber's convenience in the re-registration or renewal process, as applicable.

### **5.2 The outcome of certificate expiry regarding secrecy obligations**

The certificate expiry will not affect the validity of the contractual secrecy obligations created or granted in accordance with this CPS.

### **5.3 Certificate renewal**

Certificate renewal will be implemented in the same way as a new order.

## **6. The certificate authority and ComSign's obligations, and the limitations on these obligations.**

### **6.1 Policy regarding money refunds**

ComSign adheres to and supports stringent regulations and policies in performing actions connected to certificates and issuing them. However, if, for any reason, subscribers are not completely satisfied with the certificate issued to them, they are entitled to ask ComSign to cancel it within 30 days from the date of issue and receive a refund. After the initial 30 day period, the subscriber is entitled to ask ComSign to cancel the certificate and receive a refund if ComSign has significantly violated its responsibility or other obligations, according to this CPS, in connection with the subscriber or his/her certificate.

### **6.2 Limited liability and other obligations**

The certificate authority (and ComSign, to the extent set in the mentioned paragraphs of the CPS) undertakes:

- To perform the verification regulations of the requests for the specified certificate level, as detailed in paragraph 3 of the CPS (verification of certificate issuing requests).
- To publish legally admissible certificates in accordance with paragraph 5 of the CPS.

- To revoke certificates as required in paragraph 5 of the CPS (certificate revocation).
- To handle certificate expiry, re-registration and renewal as determined in paragraph 5 of the CPS (certificate expiry). In addition, the certificate authority and ComSign guarantee that their personal keys will not be affected, unless otherwise notified via ComSign's database.

**ComSign is not liable for any other responsibility whatsoever in accordance with this CPS.**

**6.3 The certificate authority and ComSign's liability repudiation and obligation limitation**

Except as determined explicitly above (paragraph 6 of the CPS), ComSign repudiates any liability and obligations of any kind, including any negotiability, for matching a specific objective and the accuracy of information given, and in addition, repudiates any liability for negligence, failure to provide a warning and failure to take reasonable caution.

Except as determined explicitly in paragraph 6 of the CPS above, ComSign:

- Is not responsible for the accuracy, truth, reliability, completeness, updating, negotiability or suitability of any information included in certificates or of information transferred, published or distributed in any other way by ComSign.
- Will not bear responsibility for presentation of information included in a certificate, and provided that, in essence, the certificate contents matches this CPS.
- Does not promise Non-Repudiation regarding any certificate or message whatsoever (since non-repudiation is determined exclusively in accordance with the law and the relevant mechanism to settle disputes), and –
- Is not responsible for any software whatsoever.

**6.4 Exclusion of certain fundamental damage**

Under no circumstances will ComSign be responsible for any indirect, special, accompanying or consequential damage or for profit loss, data loss or indirect or other

consequential damage or for punitive damage fees, whether they could have been reasonably anticipated or not, resulting from, or connected to the use, delivery, transfer under license, performance or non-performance of transactions or services regarding certificates or electronic signatures or other transactions or services offered or discussed in this CPS, also if ComSign was notified about the possibility of damages as mentioned.

**6.5 Limitations on loss and damage fees**

Under no circumstances will ComSign’s aggregate responsibility towards any parties (including, among others, a subscriber, request submitter, recipient or reliant party) exceed the relevant liability ceiling concerning a certificate as said, as detailed in table 14 below.

ComSign’s combined aggregate responsibility towards any person regarding a specific certificate will be limited to a sum which does not exceed that mentioned below for all transactions connected to the same certificate:

	Liability ceiling
Level 1	[a sum in NIS equal to US\$100.00]
Level 2	[a sum in NIS equal to US\$5,000.00]
Level 3	[a sum in NIS equal to US\$100,00.00]

**Table 14 – Liability Ceiling**

The limitation of damages and the damage fee as mentioned above applies to any kind of loss and damage, including, without limitation, direct damages; damage compensation fee; indirect, special, or consequential damages; damage fees for example or accompanying damages, caused to any person, including, without limitation, a subscriber, request submitter, recipient or reliant party, and which were caused because of relying on a certificate, or use of a certificate, which ComSign issues or manages, uses or revokes, or because of relying on an expired certificate or using an expired certificate. This limitation of damages and damage fee applies also to contractual or damage liability and any other liability claim. The liability ceiling for any certificate will be identical, without reference to number, the transaction or the claims regarding the same certificate. In case

the claim sum exceeds the liability ceiling, the existing liability ceiling will be allocated at first for the earlier claims in order to reach a final settlement of the dispute, unless an authorized court rules otherwise. Under no circumstances will ComSign be obligated to pay a sum exceeding the combined liability ceiling regarding any certificate, without relating to the liability ceiling allocation method between a few claimants.

#### **6.6 The subscriber's liability towards a reliant party**

Without limiting the subscribers' other obligations as set in this CPS, subscribers are liable for any false presentation which was given by them in certificates to third parties who, after verifying a certificate, rely within reason on the presentations included therein.

#### **6.7 The absence of a trust relationship**

ComSign is not the subscribers or reliant parties' messenger, trustee or other representative. The relationship between ComSign and the subscribers, and between ConSign and the reliant parties, is not a messenger-sender relationship. The subscribers and reliant parties are not authorized to coerce ComSign into any obligations whatsoever, through a contract or any other way. ComSign will not provide any other stand opposing this, whether explicitly, implied, ostensibly or any other way.

#### **6.8 Dangerous activities**

ComSign's certificate issuing services are not designed, meant or permitted to be used or resold as control equipment under dangerous circumstances or usage requiring foolproof performance, such as operating nuclear facilities, navigating aircraft or communications systems, air traffic control systems, or arms control systems, a place where failure is likely to lead directly to death or bodily harm or cause serious environmental damage.

## **7. Miscellaneous provisions**

### **7.1 Contradictory provisions**

In case of a contradiction between this CPS and other regulations, directives or contracts, the subscriber will be obligated to this CPS, except for other contracts which (i) bear an earlier date to the first publication date of this CPS or (ii) explicitly cancel this CPS, for

which the said contracts will apply towards its parties, and except in case this CPS's directives are forbidden according to the law.

## **7.2 Legal existence and export regulations**

Exporting certain software which is in use in combination with ComSign's certificate issuing services is liable to require approval of the relevant authorities. The parties must uphold the applicable export laws and regulations.

## **7.3 The applicable law**

The State of Israel's laws will apply to enforcement, interpretation and validity of this CPS, without reference to the provisions of contract law or other laws concerning choice of law and without requiring proof of trade relations in Israel. The choice of law is determined in order to ensure uniform regulations and interpretation for all users, without reference to their place of residence or where they use their certificates.

## **7.4 Interpretation and translation**

Unless otherwise determined, this CPS will be interpreted in a way which is in line with fair commercial under the same circumstances. In interpreting this CPS, its scope and international application must be referred to, as well as the advantages concealed in encouraging uniformity in its application and maintaining good faith.

The English translation of this CPS can be found at <https://www.comsign.co.il/cps>. In case of a contradiction between the English version and the non-English version, and for interpretation purposes, this English version will prevail.

## **7.5 Non-waiver**

Failure of a person to enforce any provision of this CPS will not be considered a waiver of future enforcement of the same provision or any other provision whatsoever.

## **7.6 Notification**

Any time that any party to this CPS is interested or required to send a notification, demand or request concerning this CPS, the said message must be provided by using electronically signed messages in a way which is in line with the requirements of this CPS, or in writing. Electronic messages will be valid when the sender receives a valid

confirmation of receipt from the recipient signed by electronic signature. The said confirmation of receipt must be received within five (5) days, otherwise written notification must be sent. Written messages must be delivered via a courier service which confirms delivering the message or via prepaid registered mail with a request to receive a delivery confirmation to the following address:

To ComSign:

ComSign

[Building 4, Kiryat Atidim, Tel Aviv]

From ComSign or CA to another person:

To the most current address registered in the file at ComSign.