ComSign Ltd.

Certification Practice Statement (CPS)

Procedures relating to issuing electronic certificates that comply with provisions of the Electronic Signature Law and its regulations.

Version 3.1.1

Publication Date: [April 26th 2015]

ComSign Ltd.

P.O.B. 58077, Kiryat Atidim, Tel Aviv 61580

This English version was translated by ComSign Ltd from the Hebrew version of ComSign's CPS.
Only the Hebrew version of the CPS was approved by the Israeli CA Registrar, and as such, only the Hebrew version is the binding version.

The Hebrew version of the current CPS can be found at: http://www.comsign.co.il/cps
The Israeli CA Registrar web site is:
http://www.justice.gov.il/MOJHeb/ILITA/HatimaElectronic/OdotRasamGormimMeaasrim.htm

Copyright Notice

Address of ComSign Ltd.

Mailing address: P.O.B. 58077, Kiryat Atidim, Tel Aviv 61580 Israel.

Office address: Building 4, Kiryat Atidim, Tel Aviv 61580 Israel.

Telephone: 972-3-648-5255, Facsimile: 972-3-647-4206

E-mail address: info@ComSign.co.il

Table of Contents

1. Introduction 7

1.1 General Explanation 7

1.2 Name and Identification of this Document 8

1.3 Parties Involved in Issuing Certificates 8

1.4 Use of the Certificate 9

1.5 Policy and Procedures 10

1.6 Definitions and Terminology 11

2. Publication and the Repository 15

2.1 The ComSign Repository 15

2.2 Publication via ComSign's Repository 15

2.3 Publishing Revoked Certificates in the Repository: Frequency and Time 15

2.4 Access to the ComSign Repository 16

3. Identification and Verification 17

3.1 Name of Certificate Owner 17

3.2 Identifying an Applicant 18

3.3 Validating Requests to Issue a Certificate 35

4. Process for Issuing an Electronic Certificate 37

4.1 Procedures for Handling a Request to Issue an Electronic Certificate 37

4.2 Handling a Certificate Application 40

4.3 Issuing a Certificate 41

4.4 Approval/Rejection of an Application to Issue a Certificate 42

4.5 Pair of Keys, their Safeguarding and Terms of Use of the Certificate 42

4.6 Relying Parties 46

4.7 Certificate Renewal 48

4.8 Revocation and Expiry of Certificates 50

4.9 Checking the Status of Certificates 52

4.10 Confirmation by ComSign after a Certificate has Expired 53

5. Physical, Personal and Records Security 54

5.1 Physical Security Controls 55

5.2 Security Policy 56
5.3 Senior Management Forum on Security 56
5.4 Procedures Related to Personnel Management 57
5.5 Documenting Actions using Records 60
5.6 Storage Period for Records, Documents and Information Received from Certificate Owners 62
5.7 Plans for Dealing with Unexpected Events and Disaster Response Plan 62
5.8 Termination or Interruption of ComSign's Activity 63
6. Logical Security 65
6.1 ComSign's Signature Device 65
6.2 Protecting the Signature Device – of the Certificate Owner and ComSign 66
6.3 Encryption 68
6.4 Security of Messages 68
6.5 The Reliability of the Systems 69
6.6 Synchronizing Critical Operations according to a Real-Time Clock 69
6.7 Date and Time Stamps 69
7. Certificate and CRL Profiles 71
7.1 Certificate Structure 71
7.2 Links (Pointers) to the CPS in a Certificate 85
7.3 Warnings, Liability and Responsibility Limitations in a Certificate 86
7.4 Structure of the CRL 87
8. Audits 88
9. Registration Agents 89
9.1 Introduction 89
9.2 An Application to act as a ComSign Registration Agent 89
9.3 The Address for Submitting an Application to Act as Registration Agent for ComSign 90
9.4 Responsibility for Actions of Registration Agents 90
10. Additional Legal and Business Issues 91
10.1 Payments 91
10.2 Financial Commitments 91
10.3 Confidential Information 91

10.4 Maintaining the privacy of information 92
10.5 Property Rights 92
10.6 Representations and Obligations 92
10.7 Limitations on the Liability of ComSign and its Representatives 94
10.8 Dangerous Activities 96
10.9 Force Majeure 96
10.10 Validity of the CPS 96
10.11 Notifications 97
10.12 Settling Disputes 97
10.13 Applicable Law 98
10.14 Subjection to Law 98
10.15 Conformity with WebTrust 98
11. Miscellaneous 105
11.1 Completeness of these Procedures 105
11.2 Assignment of Rights and Obligations 105
11.3 Waivers 105
11.4 Titles and Appendixes of these Procedures 105
11.5 Interpretation 105
11.6 Contradictory Instructions 105
11.7 Publication 106
11.8 Comments and Suggestions 106

1. Introduction

ComSign Ltd. is a Certification Authority as defined by The Electronic Signature Law 5761-2001. In this capacity, it is responsible to verify the identity of the applicant requesting a signature and for issuing the electronic certificate, which is an electronic confirmation of the validity of the signature and correctness of its details, according to law.

These procedures regulate ComSign's electronic certificate issuing services, which comply with the requirements of the Law, and their usage. It includes chapters on identification and verification [chapter 3], issuance, revocation and renewal of certificates [chapter 4], physical security [chapter 5], logical security [chapter 6], certificate profile and Certificate Revocation List (CRL) [chapter 7].

The agreement between ComSign and the applicant is dependent on signing a Subscription Agreement.

This document was inspected by the CA Registrar according to Israeli legislation only. ComSign declares that these CPS were formulated according to the ETSI TS 456 standard.

Unless specifically stated and noted otherwise, this English version was translated by ComSign Ltd from the Hebrew version of ComSign's CPS. Whenever noted otherwise, some procedures dealing with SSL Certificates, are not part of the Hebrew version, are not regulated under the Electronic Signature Law and are not subject to approval by the Registrar. However, these procedures comply with WebTrust Principles and Criteria for Certification Authorities Version 2.0 (WTCA), Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.1.6 and Network and Certificate Systems Security Requirements, v.1.0 and were audited, validated and approved as such.

Only the Hebrew version of the CPS was approved by the Israeli CA Registrar, and as such, only the Hebrew version is the binding version.

The Hebrew version of the current CPS can be found at: http://www.comsign.co.il/cps

The Israeli CA Registrar web site is:
http://www.justice.gov.il/MOJHeb/ILITA/HatimaElectronic/OdotRasamGormimMeaasrim.htm

1.1 General Explanation

The electronic certificate issuing services of ComSign are intended to support secure e-commerce and other electronic services, in order to provide a solution for the technical, business and personal needs of electronic signature technology-users. ComSign is registered as a Certification Authority (CA) by the Registrar of Certification Authorities, in accordance with the Law (as these terms are defined below) and serves as a trustworthy third party that issues, manages and revokes electronic certificates according to these procedures.

This CPS describes and regulates the process of issuing electronic certificates from beginning to end, and the processes and services related to the issuance and management of certificates. These procedures are implemented by ComSign and its representatives when issuing and managing electronic certificates.

ComSign acts as a third party that verifies the relationship between a particular electronic signature and the signer. This verification is accomplished using a certificate – an electronically signed message – that is issued by ComSign as a CA, confirming that the signature verification device (as defined below) belongs to the owner of the electronic certificate.

The certificate issuance services include application, proper identification of the applicant, issuing and revoking certificates, and documenting the actions taken by ComSign. Certificates will be revoked only in one of the situations listed in section 4.8.1 of this CPS, in accordance with the Law, regulations and instructions of the Registrar (as these terms are defined below).

This CPS applies only to electronic certificates, as defined by the Law, which comply with the requirements of the Law and its regulations (as defined below).

1.2 Name and Identification of this Document

This document will be referred to as "the procedures document" or "CPS of ComSign, Ltd." or "CPS," and thus it will appear on the certificate. This document may be read on the company's Internet site, http://www.comsign.co.il/cps.

1.3 Parties Involved in Issuing Certificates

1.3.1 Certification Authority:

ComSign is a Certification Authority (CA) as defined by the Electronic Signature Law and regulations pursuant thereto. The procedures followed by ComSign are based on Israeli law and regulations, international standards whenever they are in accord with the provisions of Israeli law, and with the instructions of the Registrar of Certification Authorities.

1.3.2 Registration Agents:

The certificate issuance services of ComSign are managed in a manner that allows the services related to applications for the issuance of electronic certificates, identification and registration of applicants to be handled by a Registration Agent who is authorized by the CA and approved by the Registrar of Certification Authorities, in accordance with the provisions of the Law and regulations. The Registration Agent is obligated to this CPS and instructions issued by the CA. The Registration Agent is hierarchically subordinated to the CA, and whilst

it bears the specific responsibilities defined in its authorization, this does not, in any way, relieve ComSign of its overall responsibility as defined by law. This ensures that the uniform quality of the certificate issuance services provided by the CA and its representatives is maintained.

1.3.3 ComSign Registration and Verification Clerks:

Representatives of ComSign who are responsible for receiving certificate applicants, completing the form containing details of certificate applicants, confirming and verifying the identity of the certificate applicants, actually implementing the process of issuing the certificate and, after issuance, verifying that it functions properly. Subsequently, they receive payment and issue the invoice and receipt. If the certificate is to be revoked, they confirm the identity of the person requesting the revocation, and actually revoke the certificate.

1.3.4 Certificate Owner:

As defined below.

1.3.5 Representative of the Applicant:

The applicant requesting an individual certificate or the authorized representative of an individual or the authorized representative of a corporation, when the application is for issuing an individual certificate in the name of a corporation.

The identity of the authorized representative must be verified in accordance with the procedures described below.

1.3.6 Relying Party:

As defined below.

1.4 Use of the Certificate

1.4.1 Type of Certificate:

An electronic certificate issued in accordance with this CPS, the Law and regulations is an electronic certificate as defined by law: "An electronic message issued by a Certification Authority under the provisions of Chapter 4, confirming that a certain signature verification device belongs to a certain person."

1.4.2 Authorized Signatures on the Electronic Certificate when a Signature is Required by Law:

Section 2(a) of the Law states, "For any legislation requiring the signature of a person on a document, the said requirement may be fulfilled, in respect of an electronic message, by use of an electronic signature, provided that it is a certified electronic signature (certified with an electronic signature). Section 2(b) of the Law states, "The provisions of subsection (a) will not apply to legislations that the Minister, following approval of the Constitution, Legislation and Law Committee, sets forth in the First Schedule." The First Schedule to the Law contains a list of laws to which section 2(a) does not apply.

1.4.3 Legal Status:

Section 3 and Section 4 of the Law state a presumption according to which an electronic message signed with an electronic signature certified by an electronic certificate is acceptable as *prima facie* evidence in any legal proceeding that (a) the signature belongs to the owner of the electronic signature; (b) the electronic message is the one that was signed by the owner of the electronic signature.

1.4.4 Limitations on Use of the Certificate:

Additional or other limitations on certificates usages according to section 19(8) of the law, may be placed by ComSign in accordance with Section 21(b) of the Law, as per the provisions of any law, or at the request of the owner of the certificate. These limitations will appear on the certificate.

Limitations on certificate usages will be executed only according the certificate owner's specific request. The form of the request will be formulated subject to the approval by the Registrar.

1.5 Policy and Procedures

1.5.1 Responsibility for Implementation of Policy and Procedures:

The party at ComSign who is responsible for implementation of policy and procedures is the Security Officer. E-mail address: security@comsign.co.il. Mailing address: 11th floor, Building 4, P.O.B. 58007, Kiryat Atidim, Tel Aviv 61580 Israel. Tel. 972-3-644-3620, Fax. 972-3-649-1092.

1.5.2 Support and Customer Service:

Information regarding certified electronic signatures and support may be obtained from ComSign by writing to support@comsign.co.il. Additional assistance may be obtained from ComSign's customer service representatives by e-mail: customer_services@comsign.co.il, Tel. 972-3-644-3620, Fax. 972-3-649-1092.

1.5.3 Approval of Procedures:

These procedures were formulated in accordance with the Electronic Signature Law and regulations and approved, as required by law, by the Registrar of Certification Authorities, which is the regulatory agency for this matter, within the Ministry of Justice of the State of Israel, in accordance with Section 10 of the Electronic Signature Regulations (Certification Authority) (for definitions, see below).

Additional details and contact information for the Registrar may be found at the following address:

http://www.justice.gov.il/MOJHeb/ILITA/HatimaElectronic/OdotRasamGormimMeaasrim.htm

1.6 Definitions and Terminology

In these procedures, the terms listed below will have the meanings stated beside them:

Signature device	Unique software, object or information required for creating a secure electronic signature. A signature device is used to produce a certified electronic signature. A signature device is unique to its owner, kept confidential by its owner, and is also known as a "private key" in the public key encryption system.
Signature verification device	Unique software, object or information required for verifying that a secure electronic signature was created using a specific signature device. A signature verification device has a single value correspondence with the signature device, and is also known as a "public key" in the public key encryption system. A particular signature verification device is used to identify a secure electronic signature as one produced by a particular signature device. It is possible to make the signature verification device available to the public for the purpose of this process.
Certificate owner	An applicant to whom an electronic certificate was issued.

Application	The process by which the applicant (as defined below) requests that an electronic certificate be issued.
The Law	The Electronic Signature Law 5761-2001
Device or hardware device	Smart card, token, HSM or any other hardware component used to create and secure the signature device.
Electronic signature or Certified electronic signature	Certified electronic signature as defined by the Law (as defined above).
Comsign Repository	The ComSign database that contains publicly-accessible information including, but not limited to, this CPS and the list of revoked electronic certificates, as published on the ComSign Internet site. The ComSign Repository also includes additional information that is not accessible to the general public, for example, the list of valid certificates.
Applicant	A person or a corporation or a public institution that submits a request for issuing an electronic certificate, as described in chapter 4, below.
Relying party	A third party who receives a message signed with a certified electronic signature and who takes or refrains from action on the basis of the certified electronic signature and/or on information found in ComSign's Repository.
Key (private, public) or pair of keys	A private key and its associated public key which are connected by a single-value correspondence in accordance with accepted methods of encryption, as required by the Law, as part of the public key method of encryption.
The procedures or these procedures	The procedures described below that regulate the activities of ComSign as a Certification Authority, according to the Law (as defined above) and its regulations. These procedures apply only to the certificates (as defined below).

Representative of Comsign	A party external to ComSign that was appointed by ComSign as a Registration Agent, with the approval of the Registrar of Certification Authorities, for the purpose of registering and identifying applicants and handling applications for the issuance of electronic certificates, and whose appointment was approved by the Registrar of Certification Authorities.
The parties	ComSign, its representatives and users of its certificates, meaning the owner of the certificate and the relying party.
The Registrar or Registrar of Certification Authorities	Registrar of Certification Authorities who was appointed to office according to the Law and its regulations.
Certificates or electronic certificates	Electronic certificates, as defined by Law, issued by ComSign and complying with the requirements of the Law and regulations. It should be noted that ComSign issues other certificates for other purposes that do not comply with the requirements of the Law and regulations but are suitable for other uses and purposes. These procedures apply only to certificates as defined above. Other procedures apply to the other certificates issued by ComSign. Those procedures may be viewed at http://www.comsign.co.il/cps. Requests for additional information may be addressed to ComSign.
Revoked certificate	A certificate that appears on the Certificates Revocation List (CRL) in the ComSign Repository.
Valid certificate	A certificate that appears on the list of valid certificates in the ComSign Repository.
Regulations	Regulations promulgated pursuant to the Law.
Electronic signature Regulations (Hardware and Software Systems)	Electronic Signature Regulations (Hardware and Software Systems and Request Verification), 5761-2001.

Electronic Signature Regulations (Certification Authority)	Electronic Signature Regulations (Registration and Management of Certification Authorities), 5761-2001.
Securities Regulations (Certification Authority)	Regulations which are part of the securities Act and its regulations which determine the action of the Certification Authority, regarding a certified electronic signature on documents and reports to the Magna System belonging to the ISA who offers its services to public companies. The ISA demands that these public companies report to the authority using the system and a certified electronic signature.

Terms defined in the Law and its regulations will be interpreted according to the Law and its regulations**.**

2. Publication and the Repository

The purpose of this chapter is to review the ways in which ComSign publishes relevant information to the general public, to relying parties, certificate owners and applicants, as applicable. This chapter relates to the types of information published, the frequency of publication, and ways of accessing the ComSign Repository.

2.1 The ComSign Repository

For purposes of conducting its activity in compliance with the law, ComSign manages a collection of databases designed for storage and retrieval certificate and other relevant information. Together they are known as the "Repository." ComSign's Repository includes, *inter alia*, the following sub-collections: database of valid electronic certificates (including ComSign's certificates), a database of revoked certificates, additional information regarding the revocation of certificates and lists of revoked certificates, and other information as decided by ComSign from time to time, subject to instructions issued by the Registrar.

Only part of the information published in ComSign's Repository is accessible for the general public to view. The list of revoked certificates containing their serial number and date of revocation is accessible for controlled viewing.

ComSign's databases are registered with the Registrar of Databases in accordance with the Protection of Privacy Law, 5741-1981, and ComSign will act in accordance with and subject to this law.

2.2 Publication via ComSign's Repository

As part of the ComSign Repository, ComSign will publish a list of revoked certificates, updates to procedures that have been approved by the Registrar, and other information in a manner consistent with the CPS and applicable law.

The aforementioned information will be publicized conspicuously on the Internet site. Partial updates of the procedures will include the date that the changes take effect.

2.3 Publishing Revoked Certificates in the Repository: Frequency and Time

ComSign will publish a new list of revoked certificates no later than every 12 hours or immediately after a certificate is revoked, whichever is earlier. The published list of revoked certificates is valid for 24 hours.

Exception for users of the Electronic Full Disclosure System ("*Magna*"): A new list of revoked certificates is published every 2 hours (pushed into the Magna servers) and the published list of revoked certificates is valid for 24 hours.

In order to remove any doubt, the updated and valid list of revoked certificates is the one that appears in the ComSign Repository. A relying party must conduct a new, online check of the database of revoked certificates every time that it wishes to the rely on a certificate in order to ensure that he/she is checking the certificate against the most recently updated list of revoked certificates.

2.4 Access to the ComSign Repository

There is free access to the ComSign Repository of revoked certificates on the Internet at: http://fedir.comsign.co.il/crl, at the address appearing on the certificate and using other methods of communication, as determined by ComSign from time to time.

3. Identification and Verification

The purpose of this chapter is to review the requirement for physical presence, the process of identifying and verifying the identity of the person applying for a certificate, the documents that the applicant must present, verification of the application, cases in which the application will be refused, and the process for identifying the owner of the certificate for purposes of revocation or re-issuance.

3.1 Name of Certificate Owner

ComSign does not issue anonymous certificates and/or certificates that identify the certificate's owner using a nickname or pseudonym. The name of the owner is specified on the certificate in accordance with the X.509 standard. It is possible to issue several certificates for **different** authorized signatories of the same applicant corporation and/or public institution, as long as they are issued in accordance with this CPS, the Law and regulations. It is possible to issue several electronic certificates to the same applicant, according to his/her various positions (for example, Mr. John Doe will receive one certificate as a person who reports to the Electronic Full Disclosure System, one as a supplier to the Ministry of Defense and one as a user of the Ministry of Finance's *Merkava* system).

Applicants and certificate owners warrant to ComSign and/or its representatives that their use of the details that appear on the application for issuance of a certificate do not impair or violate the rights of any third party, in any jurisdiction, in respect of their trademarks, service marks, trade names or any other intellectual property, and that they are not attempting to use any of the details appearing on the certificate application for any illegal purpose including, but not limited to, causing a breach of contract, or other illegal intervention in contractual relationships, unfair competition, damage to the reputation of another and misleading any person, corporation or legal entity.

ComSign and its representatives shall not be responsible for the information that a certificate owner provided to ComSign, to a representative of ComSign, or to ComSign's Repository or provided in another manner for insertion into a certificate and that's very provision might be in violation of the law.

The certificate owners will be solely responsible for the legality of the information they provide, for the use of the certificates issued according to this CPS, in any jurisdiction where the content of the certificate may be used or viewed. Therefore, applicants and certificate owners must be aware of the existence of various laws regarding data transfer, and especially encrypted data or data that includes encryption algorithms, and that these laws may be significantly different in different countries and states. Furthermore, in most cases it is not possible to limit the distribution of content

via the Internet or certain other networks based on the location of the user/viewer, which may require applicants and certificate owners to obey the laws of any jurisdiction where the content may be viewed or used.

3.2 Identifying an Applicant

All of the procedures in this subsection are in accordance with the Electronic Signature Regulations (Hardware and Software Systems).

3.2.1 Identifying a Single Applicant for the First Issuance of a Certificate:

The identification of an applicant as described in this subsection will be accomplished by two ComSign registration clerks, solely on the basis of face to face identification, as described below.

3.2.1.1. An individual applicant who is a resident of Israel – on the basis of an identity card (including the addendum) with the addition of one of the following documents (two different documents, both with a photograph, are required for the identification process):

1) A valid Israeli passport; or

2) A valid Israeli drivers license containing a photo; or

3) A laissez-passer, as defined by the Passports Law, 5712-1952; or

4) An identifying document issued by the State to a State employee or to someone employed by the State or fulfilling a function on its behalf or who functions in accordance with law in order to fill the said function or position, provided that this document bears the photograph and identity number of the applicant. For the purpose of this section, the term "State employee" includes a soldier, policeman, prison warden or any other official or functionary according to law in any institution of the State; or

5) An identifying document of another type issued by a public authority in accordance with the law, which is approved by the Registrar for this purpose, provided that this document bears the photograph of the applicant and his/her identity number; or

6) An identifying document of another type that is approved by the Registrar, provided that this document bears the photograph of the applicant and his/her identity number; or

7) In the case that the applicant does not have one of the documents listed in subsections (1)-(5) – an affidavit on the lack of any one of the documents listed in subsections (1)-(5) above and, in addition, a statement from an attorney confirming the applicant's identity and that he/she knows the applicant personally, accompanied by a picture of the applicant signed by the attorney, in a form approved by the Registrar.

In addition to inspecting the documents, the details will be verified on the basis of information received from the Population Registrar of the Ministry of the Interior (hereinafter, "the population registry") that contains the following details: identity number of applicant, surname and previous surname if any, first name, father's name, mother's name, year of birth, date the most recent identity card was issued, reason for the card was issued, current address and, if relevant, death status and date of death.

3.2.1.2. An individual applicant who is not a resident of Israel – on the basis of a foreign passport, a travel document or an identity card, together with another identifying document containing the applicant's photograph and his/her identifying details and those of the entity that issued the additional document. (Two different documents, both with a photograph, are required for the identification process).

3.2.2 <u>Identifying an Authorized Signatory of a Corporation and/or Public Institution for the First Issuance of a Certificate:</u>

3.2.2.1. A corporation registered in Israel – on the basis of the incorporation certificate, an attorney's statement confirming the existence of the corporation, its name and registration number, or instead of the specified attorney's statement – by verification in the appropriate registries and on the basis of a certified copy of a resolution passed by the authorized bodies of the corporation regarding the authorized signatories on behalf of the corporation, or an attorney's statement regarding the identity of the said authorized signatory, using the text published on the Internet site of ComSign from time to time, as approved by the Registrar.

3.2.2.2. A corporation not registered in Israel – on the basis of a certified copy of a document confirming that the corporation is incorporated, the statement of an attorney confirming the existence of the corporation, its name and registration number, or instead of the specified attorney's statement – by verification in the appropriate registries and on the basis of a certified copy of a resolution passed by the authorized bodies of the corporation regarding the authorized signatories on behalf of the

corporation, or an attorney's statement regarding the identity of the said authorized signatory, using the text published on the Internet site of ComSign from time to time, as approved by the Registrar.

3.2.2.3. A public institution – on the basis of an affidavit of the applicant signed by an authorized signatory, using the text published on the Internet site of ComSign, from time to time, in accordance with the position of the authorized signatory, after the CA is convinced by the document that the authorized signatory is indeed authorized to act on behalf of the public institution; for purposes of this subsection, a "public institution" is a government ministry, local authority, and also any authority, corporation or other institution established in Israelby law.

3.2.2.4. Regarding corporations (whether or not they are registered in Israel) and public institutions – The CA will identify the authorized signatory in the same manner that it identifies individual applicants either residents of Israel or non-residents, as applicable, as described in section 3.2.1 above.

3.2.2.5. Regarding corporations that are not registered in Israel and public institutions – If a "certified copy" is required, the intention is a copy "true to the original" that is authenticated by one of the following:

3.2.2.5.1 The authority that issued the original document;

3.2.2.5.2 An attorney licensed to practice law in Israel;

3.2.2.5.3 An Israeli diplomatic or consular representative overseas.

3.2.2.6. Certificate applicants are required to present an ISA approval which was issued to them by the ISA and on behalf of their organization. This approval will be authenticated by Comsign on each issuing of a new certificate to the ISA. The authentication will be based on an identical approval sent to Comsign beforehand.

3.2.3 Identifying an Authorized Signatory of an Individual for the First Issuance of a Certificate:

3.2.3.1. At the request of an individual applicant who has authorized an authorized signatory to act in his/her name and on his/her behalf, and with an attorney's confirmation of the said authorized signatory, using the text published on the Internet site of ComSign from time to time, as approved by the Registrar.

3.2.3.2. The CA will identify the authorized signatory in the same manner that it identifies individual applicants either residents of Israel or non-resident, as applicable, as described in section 3.2.1 above.

3.2.4 Identifying an Applicant for Issuance as Part of an Automatic Signature System:

A certificate that is part of an automatic signature system will be issued only for an applicant who is a corporation or public institution.

ComSign will identify the applicant in accordance with the process described in sections 3.2.1 and 3.2.2, above, as applicable. In addition, the applicant will provide ComSign with signed affidavit and commitment forms, according to the text approved by the Registrar.

On these forms the applicant declares that it was warned regarding the risks inherent in using automatic signature systems, and is implementing IT security and access control measures. In addition, it must submit a declaration by an authorized signatory on its behalf that the corporation will be responsible for all uses of the certificate and cannot deny a document signed using the automatic signature system.

3.2.5 Identifying an Applicant for Renewal of a Certificate without Creating a New Signatory Device, for an Applicants with an Unexpired Certificate:

ComSign will offer remote certificate renewal for owners of unexpired certificates, at the request of the certificate owner. This service will be offered only after it is approved by the Registrar.

The certificate owner must enter ComSign's site and identify himself using a valid electronic certificate (prior to expiration). In addition, the certificate owner must identify himself to the device on which the certificate is installed and follow the instructions on the site. If the remote certificate renewal process fails or does not operate for any reason, until the expiration date of the certificate being replaced, a new certificate will be issued using the complete, ordinary identification process, including identification of the applicant as when an electronic certificate is issued for the first time.

3.2.6 Identifying an Applicant when Revoking a Certificate:

3.2.6.1. ComSign will revoke a certificate at the request of the owner of the certificate immediately upon receipt of the request and verification that the person requesting the revocation is indeed the owner of the certificate. The act of revoking a certificate

will be implemented by two or more clerks. The owner of the certificate who is requesting its revocation will be identified in one of the following ways:

3.2.6.1.1 Using the cancellation code created by the certificate owner when the application for issuing the certificate was submitted. A representative of ComSign will verify the correctness of the cancellation code by entering it into the relevant systems and receiving a correct/incorrect signal.

3.2.6.1.2 If the certificate owner did not create a cancellation code or does not remember it, a representative of ComSign and/or someone on its behalf will call the telephone number that the certificate owner entered on the certificate application for purposes of ascertaining that the owner of the certificate is indeed the one requesting to its revocation and confirm the details of the person making the revocation request by using the personal details that were entered in the application for the certificate, including answers to identifying questions that were given by the certificate owner when it was issued.

3.2.6.2. ComSign will revoke a certificate issued to the authorized signatory of a corporation or public institution or a member of an organization or other institutional body or an authorized signatory on behalf of an individual, at the request of the corporation, public institution, organization or institutional body and/or individual, in the case of an authorized signatory of an individual and/or in accordance with the arrangements made in the subscription agreement and on the application forms for issuing the certificate.

3.2.7 Verifying the Applicant's e-mail address:

3.2.7.1. As part of the identification process, a unique secret code (the "Secret Code" will be mailed by Comsign to the Applicant's e-mail address. The Secret Code will be mailed during the coordination stage preceding the Applicant's personal appearance for the identification process. The Applicant will provide the Secret Code to the coordination clerk during the telephone conversation coordinating the Applicant's personal appearance. If the provided Secret Code is correct, the coordination clerk will transfer it to the identification clerk together with all other data pertaining to the applicant (including the applicant's e-mail address).

3.2.7.2. In the event of a non-coordinated visit to Comsign offices (as well as in any other event) the identification clerk will mail the Secret Code during the identification process (Comsign will provide the Applicant with internet access).

3.2.7.3. The Applicant must provide the Secret Code in the application form. The identification clerk will verify the matching of the Secret Code in the application form with the one reported by the coordination clerk (or by the applicant himself in a non-coordinated visit to Comsign offices) as well as the matching of the e-mail address in the application form with the address reported by the coordination clerk. Alternatively, the identification clerk will verify the matching of the Secret Code in the application form to the one mailed by the identification clerk to the e-mail address provided by the Applicant in the application form.

3.2.7.4. Only the e-mail address to which the verified Secret Code was mailed will appear in the electronic certificate issued by Comsign to the Applicant.

NOTE: **The procedures in this sub-section 3.2.8 are not regulated under the Electronic Signature Law and are not subject to approval by the Registrar. However, these procedures comply with WebTrust Principles and Criteria for Certification Authorities Version 2.0 (WTCA), Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.1.6 and Network and Certificate Systems Security Requirements, v.1.0 and were audited, validated and approved as such.**

3.2.8 Authentication Process for SSL certificates

All authentication and verification procedures in this sub-section will be performed either directly by ComSign's personnel (RAOs) or by ComSign's authorized representatives.

3.2.8.1. Verifying the Applicant's domain name

For issuing certificates to organizations requesting SSL certificates, Comsign performs domain name owner verification to detect cases of homographic spoofing of IDNs. Comsign employs an automated or manual process that searches-various 'whois' services to find the owner of a particular domain. A search failure result is flagged and the RA rejects the Certificate Request. Additionally, the RA rejects any domain name that visually appears to be made up of multiple scripts within one hostname label.

Note: Orders for major corporations, well known trademarks and financial institutions may be queued for further security reviews prior to issuance.

In the event an order is queued for review the administrative contact must be a full time employee of the company for successful issuance. A verification telephone call with the administrative contact may be required.

- Verification methods include one of the following:

3.2.8.1.1 EMail-based DCV

An email is sent to an administrative contact for the required domain. The email will contain a unique validation code and link. Clicking the link and entering the code will prove domain control.

Valid email addresses are:

Any email address listed in the "whois" records.

The following generic admin type email addresses AT the domain for which the certificate is being applied:

admin@

administrator@

postmaster@

hostmaster@

webmaster@

3.2.8.1.2 DNS-based DCV

The CSR that Comsign receives from the Applicant will be hashed. The hash values are provided to the Applicant, and it must be entered as a DNS TXT record OR a DNS CNAME record for the domain.

The hashes are to be entered in DNS RR as follows:

CNAME Example:

<Value of hash of CSR>.domainname.com CNAME <value of hash of CSR>.comsign.co.uk.

TXT Example:

DCV TXT <value of hash of CSR>

3.2.8.1.3 HTTP(S)-based DCV

The CSR that Comsign receives from the Applicant will be hashed. The hash values are provided to you and you must create a simple plain-text file and place this in the root of your webserver and served over HTTP-only!

The file and its content should be as follows:

http://domainname.com/<Upper case value of hash of CSR>.txt

OR

http://domainname.com/<Upper case value of hash of CSR>.html

Content (as a plain text file):

<Value of hash of CSR>

Comsign

3.2.8.2. Authentication of Organization identity

Before issuing SSL certificate and whenever a certificate contains an organization name, the identity of the organization and other enrolment information provided by Certificate Applicants (except for Non-verified Subscriber Information) is confirmed in accordance with the procedures set forth in ComSign's documented validation procedures. Comsign shall:

Determine that the organization exists by using at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable government agency or competent authority that confirms the existence of the

organization or an authorised lawyer that confirm the existence of the organisation according to local laws, confirm by telephone, confirmatory postal mail, or comparable procedure to the SSL certificate applicant certain information about the organization, that the organization has authorized the certificate application request, and that the person submitting the Certificate Application request on behalf of the certificate applicant is authorized to do so.

Where a domain name is included in the SSL certificate - Comsign authenticates the organization's right to use that specific domain name as a fully qualified domain name.

- Verification methods include ALL of the following:

3.2.8.2.1 Verify Identity and Address

Individuals

Comsign MUST obtain ALL of the following:

A. Copy of a valid driver's license, passport or government issued ID certificate of the Applicant.

B. Copy of a recent major utility bill (i.e. power bill, water bill, etc.) or bank statement or credit card statement that displays address and phone number of the Applicant, dated within the last 6 months

Organizations

Comsign MUST verify Identity through one of the following (these may also be used to verify address if it's included):

A. Government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition.

B. A third party database that is periodically updated and considered a Reliable Data Source, for example:

www.dnb.com
www.hoovers.com
UK - http://www.companieshouse.gov.uk

C. A site visit by the CA or a third party who is acting as an agent for the CA, OR:

D. An Attestation Letter.

Comsign MAY use the following to verify address provided that identity has been verified as required above:

A. Articles of Incorporation (with address)

B. Government Issued Business License (with address)

C. Copy of a recent company bank statement (you may blacken out the Account Number)

D. Copy of a recent company phone bill

E. Copy of a recent major utility bill of the company (i.e. power bill, water bill, etc.) or current lease agreement for the company

3.2.8.2.2 WhoIs Verification (Registrant company name and address)

Comsign will verify the following details trough a whois service:

A. Company name.

B. Address.

C. Phone number.

D. Contact person's name.

E. Contact person's e-mail.

3.2.8.2.3 Domain Control Validation:

Comsign will validate Domain control as it was explained chapter 3.2.8.1.

3.2.8.2.4 Callback to a Verified Telephone Number (to verify applicant)

The phone number MUST be verified via one of the following:

A. Government database
B. Other third party database
C. Verified legal opinion or accountant letter.

3.2.8.3. Authentication of Extended Validation Certificates

This is the highest level of authentication available with an SSL Certificate.

The CA/Browser Forum, a consortium of certificate authorities and browser manufacturers, developed this category of Web site authentication as an industry-wide standard. In order to be authorized to issue EV SSL certificates, a CA must pass regular third-party audits confirming that it meets the requirements set out in this standard for validating the identity of

certificate requesters. More information on the CA/Browser Forum and the EV standard is available at www.cabforum.org.

These are the standard methods of identity verification used to validate organizations for EV SSL certificates, however, documentation requirements may vary depending on the information available on various approved online databases.

ComSign requires a signed acknowledgement of agreement from the corporate contact listed on any order for an EV SSL Certificate.

A company registration document may also be required if the we are unable to confirm the organization's details through a government database. A legal opinion letter may also be requested to confirm the following details about the organization applying for the Extended Validation SSL Certificate:

• Physical address of place of operation of the organisation requesting the SSL certificate

• Telephone number of the organisation

• Confirmation of exclusive right of the organisation to use the domain

• Additional confirmation of the organization's existence (if less than 3 years old), and verification of the corporate contact's employment.

3.2.8.4. EV SSL certificates Authentication process

For supplying SSL Certificates with this level – ComSign requires authentication verification of an organization's existence through a government issued business credential.

With EV Certificate, Comsign ensures that all Subject organization information to be included in the EV Certificate are validated with these specifications:

3.2.8.4.1 Verify Applicant's existence and identity, including:

3.2.8.4.1.1. Verify the Applicant's legal existence and identity

1) Private Organization Subjects
   a) Legal Existence: Verify that the Applicant is a legally recognized entity, in existence and validly formed (e.g., incorporated) with the Incorporating or Registration Agency in the Applicant's Jurisdiction of Incorporation or Registration, and not designated on the records of the Incorporating or Registration Agency by labels such as "inactive", "invalid", "not current", or the equivalent.

b) Organization Name: Verify that the Applicant's formal legal name as recorded with the Incorporating or Registration Agency in the Applicant's Jurisdiction of Incorporation or Registration matches the Applicant's name in the EV Certificate Request.

c) Registration Number: Obtain the specific Registration Number assigned to the Applicant by the Incorporating or Registration Agency in the Applicant's Jurisdiction of Incorporation or Registration. Where the Incorporating or Registration Agency does not assign a Registration Number, the Comsign will obtain the Applicant's date of Incorporation or Registration.

d) Registered Agent: Obtain the identity and address of the Applicant's Registered Agent or Registered Office (as applicable in the Applicant's Jurisdiction of Incorporation or Registration).

2) Government Entity Subjects

a) Legal Existence: Verify that the Applicant is a legally recognized Government Entity, in existence in the political subdivision in which such Government Entity operates.

b) Entity Name: Verify that the Applicant's formal legal name matches the Applicant's name in the EV Certificate Request.

c) Registration Number: Comsign will attempt to obtain the Applicant's date of incorporation, registration, or formation, or the identifier for the legislative act that created the Government Entity. In circumstances where this information is not available, Comsign enter appropriate language to indicate that the Subject is a Government Entity.

3) Business Entity Subjects

a) Legal Existence: Verify that the Applicant is engaged in business under the name submitted by the Applicant in the Application.

b) Organization Name: Verify that the Applicant's formal legal name as recognized by the Registration Authority in the Applicant's Jurisdiction of Registration matches the Applicant's name in the EV Certificate Request.

c) Registration Number: Attempt to obtain the specific unique Registration Number assigned to the Applicant by the Registration Agency in the Applicant's

Jurisdiction of Registration. Where the Registration Agency does not assign a Registration Number, Comsign will obtain the Applicant's date of Registration.

d) Principal Individual: Verify the identity of the identified Principal Individual.

4) Non-Commercial Entity Subjects (International Organizations)

a) Legal Existence: Verify that the Applicant is a legally recognized International Organization Entity.

b) Entity Name: Verify that the Applicant's formal legal name matches the Applicant's name in the EV Certificate Request.

c) Registration Number: Comsign will attempt to obtain the Applicant's date of formation, or the identifier for the legislative act that created the International Organization Entity. In circumstances where this information is not available, the Comsign will enter appropriate language to indicate that the Subject is an International Organization Entity.

3.2.8.4.1.2. Verify the Applicant's physical existence (business presence at a physical address)

1) Check the current version of either at least one Qualified Government Information Source (other than that used to verify legal existence) or Qualified Independent Information Source.

OR

By obtaining documentation of a site visit to the business address, which MUST be performed by a reliable individual or firm. The documentation of the site visit MUST:

(a) Verify that the Applicant's business is located at the exact address stated in the EV Certificate Request

(b) Identify the type of facility (e.g., office in a commercial building, private residence, storefront, etc.) and whether it appears to be a permanent business location,

(c) Indicate whether there is a permanent sign (that cannot be moved) that identifies the Applicant,

(d) Indicate whether there is evidence that the Applicant is conducting ongoing business activities at the site (not that it is just, for example, a mail drop, P.O. Box, etc.)

(e) Include one or more photos of (i) the exterior of the site (showing signage indicating the Applicant's name, if present, and showing the street address if possible), and (ii) the interior reception area or workspace.

2) Comsign may alternatively rely on a Verified Legal Opinion or a Verified Accountant Letter that indicates the address of the Applicant's or a Parent/Subsidiary Company's Place of Business and that business operations are conducted there.

3.2.8.4.1.3. Verify the Applicant's Operational Existence – Comsign will verify that the Applicant has the ability to engage in business:

1) Verifying that the Applicant, Affiliate, Parent Company, or Subsidiary Company has been in existence for at least three years, as indicated by the records of an Incorporating Agency or Registration Agency;

2) Verify that the Applicant, Affiliate, Parent Company, or Subsidiary Company is listed in either a current Qualified Government Information Source, Qualified Independent Information Source.

3) Verify that the Applicant, Affiliate, Parent Company, or Subsidiary Company has an active current Demand Deposit Account with a Regulated Financial Institution by receiving authenticated documentation of the Applicant's, Affiliate's, Parent Company, or Subsidiary Company's Demand Deposit Account directly from a Regulated Financial Institution.

OR

Relying on a Verified Legal Opinion or a Verified Accountant Letter to the effect that the Applicant has an active current Demand Deposit Account with a Regulated Financial Institution.

3.2.8.4.2 Verify the Applicant is a registered holder, or has control, of the Domain Name(s) to be included in the EV Certificate:

As specified in section 3.2.8.1.

3.2.8.4.3 Verify a reliable means of communication with the entity to be named as the Subject in the Certificate

A telephone number, fax number, email address, or postal delivery address as a Verified Method of Communication with the Applicant.

3.2.8.4.3.1. Verify that the Verified Method of Communication belongs to the Applicant, or a Parent/Subsidiary or Affiliate of the Applicant, by matching it with one of the Applicant's Parent/Subsidiary or Affiliate's Places of Business in records provided by the applicable phone company, Qualified Government Information Source, Qualified Independent Information Source or a Verified Legal Opinion or Verified Accountant Letter.

3.2.8.4.3.2. Confirm the Verified Method of Communication by using it to obtain an affirmative response sufficient to enable a reasonable person to conclude that the Applicant, or a Parent/Subsidiary or Affiliate of Applicant, can be contacted reliably by using the Verified Method of Communication

3.2.9 Authentication Process for Code Signing certificates

Before issuing a Code Signing certificate, the identity of the organization and other enrolment information provided by Certificate Applicants (except for Non-verified Subscriber Information) is confirmed in accordance with the procedures set forth in ComSign's documented validation procedures. ComSign shall:

Determine that the organization exists by using at least one third party identity proofing service or database, or alternatively, organizational documentations issued by or filed with the applicable government agency or a competent authority that confirm the existence of the organization or a qualified lawyer that confirms the existence of the organisation according to local laws.

ComSign shall further confirm, by telephone, confirmatory postal mail or comparable procedure, that the organization has authorized the certificate application request and that the person submitting the Certificate Application request on behalf of the certificate applicant is authorized to do so.

- Verification methods include ALL of the following:

3.2.9.1. Verify Identity and Address

Individuals

ComSign MUST obtain the following:

A. Copy of a valid driver's license, passport or government issued ID certificate of the Applicant.

B. If the certificate is required to include an address, state or country information, ComSign will obtain a copy of a recent major utility bill (i.e. power bill, water bill, etc.) or bank statement or credit card statement that displays address and phone number of the Applicant, dated within the last 6 months

Organizations

ComSign MUST verify identity through one of the following (these may also be used to verify address if included):

A. A government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition.

B. A third party database that is periodically updated and considered a Reliable Data Source. For example:

www.dnb.com
www.hoovers.com
UK - http://www.companieshouse.gov.uk

C. A site visit by the CA or a third party who is acting as an agent for the CA, OR:

D. An Attestation Letter.

ComSign MAY use the following to verify address, provided that identity has been verified as required above:

A. Articles of Incorporation (with address)

B. Government Issued Business License (with address)

C. Copy of a recent company bank statement (Applicant may blacken out the Account Number)

D. Copy of a recent company phone bill

E. Copy of a recent major utility bill of the company (i.e. power bill, water bill, etc.) or current lease agreement for the company

3.2.9.2. Organization representative validation

If the request is on behalf of an organization, then the authority of the individual to make that request must be verified by a signed document from that organization, which authorizes the individual to request certificates on its behalf.

3.2.9.3. Callback to a Verified Telephone Number (to verify applicant)

The phone number MUST be verified via one of the following:

A. Government database
B. Other third party database
C. Verified legal opinion or accountant letter.

3.3 Validating Requests to Issue a Certificate

The procedure described in this chapter is subject to change from time to time, in accordance with requirements of the Law and regulations, and with the prior approval of the Registrar.

3.3.1 Procedure for Verifying Applications for Issuing an Electronic Certificate:

When an application to issue a certificate is received, ComSign will implement all of the required verification checks as a prior requirement for issuing the certificate. ComSign and/or one of its representatives will check that:

3.3.1.1. The applicant has signed the subscription agreement and application form;

3.3.1.2. The applicant is the person, corporation or public institution that is identified on the application (in case of a corporation and/or public institution, see the detailed identification method in section 3.2.2 above; for an authorized signatory of an individual, see 3.2.3, above);

3.3.1.3. The information to be registered in the certificate is accurate, in accordance with the details provided by the applicant;

3.3.1.4. Authorized signatories applying for a certificate on behalf of a corporation and/or public institution and/or an individual are legally permitted to submit such an application (see the method for identifying a corporation or public institution described in section 3.2.2 above, and the method for identifying an authorized signatory of an individual described in section 3.2.3, above);

3.3.1.5. Verification of the details of the person applying for the certificate with the Population Registrar.

3.3.2 Responsibility of ComSign for Details on the Certificate:

All information included in the certificate is verified by ComSign and is accurate as of the date the certificate was issued. It is the duty of ComSign to revoke a certificate immediately upon being informed that any of the details appearing on the certificate is incorrect.

3.3.3 Personal Presence:

To ensure identification of the certificate applicant and verify the relationship between the applicant and his/her public key (signatory verification device), Regulation 10 of the Electronic Signature Regulations (Hardware and Software Systems) states that individuals and/or authorized signatories of corporations who submit an application for an electronic certificate must appear in person in front of ComSign and/or one of its representatives.

3.3.4 Rejecting an Application to Issue a Certificate:

If the verification of the identification or authorization, as described in Chapter 3, fails, or if, at ComSign's discretion, a reasonable doubt arises regarding the identity of the applicant or his/her authorization and/or if the certificate is to be issued and/or the device generating and/or storing the signatory device does not comply with instructions in chapter 4 of this CPS, ComSign will reject the application to issue a certificate and will notify the applicant of this without delay, stating the reason why the verification failed or for its inability to issue the certificate. If the failure is caused by information contained in third party data bases such as: the Companies Registrar or the Population Registry, ComSign will provide the applicant with the details of the third party. An applicant whose application was rejected may submit a new application at a later date.

4. Process for Issuing an Electronic Certificate

The purpose of this chapter is to describe the process for issuing a certificate, from the stage of presenting the application and the required documents, through the process of logical issuance and concluding with the issuance of the certificate. In addition, this chapter includes an explanation of the process for renewing and revoking certificates, including who is entitled to request renewal or revocation. The chapter also describes the obligations imposed on the owner of an electronic certificate.

The process for issuing an electronic certificate will be accomplished by at least two clerks of the CA.

4.1 Procedures for Handling a Request to Issue an Electronic Certificate

4.1.1 Submitting an Application for an Electronic Certificate:

4.1.1.1. The applicant must come to an office of ComSign or one of its representatives, where the application will be handled by two clerks, a verification clerk and an identification clerk. The division of responsibility between them is described below, and intended to ensure the propriety of the process.

4.1.1.2. An identification clerk will identify the applicant according to the Law and its regulations as described in chapter 3 of this CPS.

4.1.1.3. The verification clerk will present the applicant with an information and warning form approved by the Registrar, regarding the risks inherent in using automatic signature systems and the obligations imposed upon him/her. The applicant will sign a declaration that he/she was warned as stated above, in accordance with Regulation 11(c)(3) of the Electronic Signature Regulations (Certificate Authority).

4.1.1.4. The applicant shall complete his/her details on the application for issuing a certificate and on the personal details form, in accordance with ComSign's requirements and create a user code for revoking the certificate, if necessary. The representative of ComSign will enter this code into a system that does not allow reconstruction of the code but gives only a "correct" or "incorrect" signal when the code is entered, see section 3.2.6, above. He/she will also set a code for remote renewal of the certificate, see section 3.2.5, above.

4.1.1.5. The identification clerk will have the applicant sign the application for issuing a certificate and the subscriber agreement.

4.1.1.6. The device used to create and store the electronic signature: The verification clerk will offer the applicant a device approved by ComSign. If the applicant wishes to use

a device not supplied by ComSign, he/she may do so, as explained in section 4.1.1.7 and 4.5.2, below.

4.1.1.7. If the device for creating and safeguarding the electronic signature is not supplied by ComSign, ComSign will check that the applicant possesses a secure device for creating an electronic signature and that the signature device and the signature verification device that identifies the said signature device comply with the provisions of Regulation 8 of the Electronic Signature Regulations (Hardware and Software Systems). For this purpose, the applicant will be required to submit the following details and documentation to ComSign:

- Name of the manufacturer
- Name of the product/model
- Copy of the approval certificate for the device issued by NIST and/or Common Criteria.

In order to comply with the provisions of Regulation 8(1)(b) and (c) of the Electronic Signature Regulations (Hardware and Software Systems), ComSign may rely on a declaration made by the applicant. This declaration will be made in accordance with the instructions issued by the Registrar. In accordance with the Registrar's instructions, in the event that ComSign has received such a declaration, ComSign will not be responsible for any additional inspection of the signature device or its routine operation, subject to the manner in which the private key is generated, as described in section 4.5.2, below.

4.1.2 Information Required on an Application for Issuing a Certificate:

The information to be included in the application for issuing a certificate is listed in Table 1, below. It has been determined in accordance with the Law, Regulations and instructions of the Registrar. Not all of the information listed below will be included in the certificate. [Note: All of the information provided will be kept confidential (see section 10.3 of this CPS).]

Table 1 – Information and Documents Required for a Certificate Application

Individuals:

The information required (regarding documents, see section 3.2.1, above):

1) Applicant name, as listed in the identification documents (first name, family name and previous family name, if any).
2) Identity number, issue date and reason of issue.
3) Name of father and mother.
4) Date of birth.
5) Drivers license details (if applicable) or passport.
6) Address: street, city, state, postal code, country (residence).
7) Telephone numbers (residence).
8) E-mail address.
9) A signed subscriber agreement.
10) Additional information as defined by the Registrar and/or required by Law and regulations.

Corporations and Public Institution:

The information required (regarding documents, see section 3.2.2, above):

1) Name of the corporation or public institution making the application.
2) Registration number of the corporation or public institution.
3) Registered office address: street, city, state, postal code, country.
4) Documents attesting to the existence and registration of the corporation as required by the Electronic Signature Regulations (Hardware and Software Systems) [certificate of incorporation, an attorney's written statement confirming the corporation existence, name and registration number or instead of the said statement, verification of the above in the appropriate registries].
5) Documents attesting to authorized signatories on behalf of the corporation or public institution or on the authority of the signatory to act on behalf of the corporation or public institution as required by the Electronic Signature Regulations (Hardware and Software Systems) [certified copy of the resolution passed by the authorized body in the corporation or public institution appointing the signatory or written confirmation of the signatory's authority from an attorney, all in accordance with the provisions of the Law and its regulations and as required by ComSign].
6) Organizational unit (if applicable).
7) Telephone numbers (of the registered office).
8) E-mail address
9) Details of the signatory as listed in items 1-8 in the previous list for single certificate applicants, plus details of his/her position in the corporation or public institution.
10) A signed subscriber agreement.
11) Additional information as defined by the Registrar and/or required by Law and regulations.

Authorized Signatories: Corporations, individuals and public institutions may submit a request using an authorized signatory.

4.2 Handling a Certificate Application

The identification clerks will verify that the applicant has all of the required documents and that there is no other reason in the Law, regulations or this CPS not to issue the certificate.

When all of the required documents have been received, the process of issuing a certificate will begin without delay.

4.3 Issuing a Certificate

The verification clerk will operate the registration terminal. The process will be implemented in the presence of the applicant.

The verification clerk will initialize the hardware component installed on the device, according to the type of device.

The verification clerk will issue the certificate:

- The verification clerk will enter the applicant's details in the system, according to the application form.
- The verification clerk will connect the signature device to the issuing computer (token, card, HSM)
- At this stage, the applicant will enter his/her password for creating the signature device (private key) and the means for verifying the signature (public key) directly into the hardware device without exposing the password and signature device to the verification clerk.
- The verification clerk will verify that the certificates and the keys are in place on the device by using the device management software and entering the device (it is likely that the applicant will have to enter his/her password).
- The verification clerk will check the certificates against the relevant systems, if possible.
- The verification clerk will transfer the device to the Applicant's possession and explain to the Applicant about his/her obligation to keep it under his/her control.
- The verification clerk will explain to the Applicant about the importance of securing the device and the importance of keeping the password and/or access element to the device in secure, safe places.
- The verification clerk will describe the certificate revocation procedure to the Applicant.
- If necessary, the verification clerk will verify the Applicant's signature on the required declarations.

4.4 Approval/Rejection of an Application to Issue a Certificate

4.4.1 Approval of an Application to Issue a Certificate:

ComSign will issue an electronic certificate to the applicant only after his/her application is approved. An electronic certificate represents a complete and final approval by ComSign of the application for issuing an electronic certificate.

When the certificate is issued, ComSign will record details of the certificate on the list of valid certificates in the ComSign Repository and other databases, in accordance with the Law and regulations, and subject to the instructions of the Registrar. Certificate owners may publicize their certificates in additional databases.

4.4.2 Rejection of an Application to Issue a Certificate:

ComSign may refuse to issue a certificate to any applicant for reasonable reasons, such as a suspicion of incorrect identity, noncompliance of the signature device with the hardware and software regulations and/or instructions of the Registrar, or nonpayment for the service, and subject to the provisions of any law, without bearing any responsibility or liability for losses or other results of this refusal. If ComSign refuses to issue the certificate, Comsign will return the application fee, if any, that the applicant paid for the certificate without delay.

4.5 Pair of Keys, their Safeguarding and Terms of Use of the Certificate

4.5.1 Pair of Keys:

The key pair created by the applicant must conform to Regulation 8 of the Electronic Signatures Regulations (Hardware and Software Systems) as follows: "The electronic signature is produced using a key based on an accepted standard which uses one of the following: (1) RSA or DSA key that is at least 1024 bits long, (2) an elliptic curve DSA key which is at least 160 bits long." ComSign issues its Applicants RSA keys that are 2048 bits long.

The device that creates and secures the signature device may be provided either by ComSign or by the Applicant.

4.5.2 Safeguarding the Signature Device:

The hardware device containing the signature device (the private key of the key pair) must be safeguarded in accordance with regulation 8 of the aforementioned regulations: "To operate or access the signature device, use of unique physical or crypto-logical measures that

conform to Security Level 1 of the FIPS 140-2 standard, with a security level of at least Common Criteria EAL2 standard is required."

If the applicant did not purchase from ComSign the hardware device on which the signature device is to be installed, ComSign will not issue an electronic certificate until receiving the applicant's declaration stating that he/she has provided ComSign with accurate details, to the best of his/her knowledge, regarding the signature device, the manner of its operation and access. ComSign will not issue the applicant an electronic certificate for a signature verification device that does not comply with the Law, its regulations and the instructions of the Registrar, as described in section 4.1.17, above. ComSign will ensure that the keys will be created during the issuing process and will not allow a situation in which an applicant arrives for issuing a certificate with a signature device that was created in any prior process. This is in order to prevent the possibility that keys belonging to another identity can infiltrate the device. During the verification process, the applicant's signature device will not be exposed.

4.5.3 Applicant's Control of the Access to the Signature Device:

The creation of the signatory device will be carried out, as detailed in section 4.3 in a secured process using a reliable physical device or a reliable system.

Every certificate applicant and certificate owner is required to confirm and declare in the subscription agreement that after the certificate is issued, he/she, him/her/herself, and not ComSign (or its representative), is solely responsible for safeguarding the signature device from damage, loss, exposure, modification or unauthorized use.

Furthermore, the subscription agreement obligates certificate owners not to copy, reproduce, or reverse-engineer the technology that ComSign uses to issue the certificates.

4.5.4 Certificate Validity:

All certificates will be valid from the date and time that they are issued by ComSign. The certificate will be valid for the period of time that is stated in the subscription agreement, unless revoked earlier ("validity period").

4.5.5 Releasing a Locked Device:

Hardware devices include security mechanisms that make access to the signature device dependent on entering a password. In accordance with instructions issued by the Registrar,

the hardware will lock after a specified number of unsuccessful attempts to enter the password

ComSign will offer certificate owners a service for releasing a locked card without ComSign having access to the signature device, by using a special mechanism that **will be approved by the Registrar**.

4.5.6 Responsibility of the Certificate Owner:

Upon receipt of the certificate, the subscriber will verify that all of the details listed in it are correct, in accordance with section 4.3, above. If an error is found, the certificate owner is required, by the subscriber agreement, to notify ComSign as soon as the error is discovered and request the revocation of the certificate, in accordance with the procedure for revocation at the certificate owner's request (section 3.2.6). If the information does not conform with the information provided by the certificate owner before the certificate was issued (either in the application form and/or the personal details form and/or the subscription agreement), ComSign will revoke the certificate and issue the certificate owner a new certificate free of charge. In any other case, the certificate will be revoked and the certificate owner will be charged the full price for issuing a new certificate.

4.5.7 Obligations of the Certificate Owner:

The owner of the certificate confirms and undertakes (unless he/she gives notice to the contrary) that:

- Throughout the entire period of the certificate is valid, to take all reasonable measures for the safe keeping of his/her signature device and to prevent its unauthorized use;
- Throughout the entire period that the certificate is valid, to inform ComSign immediately upon learning that his/her control of the signature device has been impaired;
- To the best of his/her knowledge, all representations made by the owner to ComSign regarding the information contained in the certificate are correct;
- To the best of his/her knowledge, all information about himself contained in the certificate is complete and correct;
- He/she will use the certificate in a manner consistent with this CPS and the Law.

4.5.8 Obligation of the Certificate Owner to Safeguard His/Her Signature Device and Prevent Unauthorized Use:

The certificate owner is duty-bound to know that it is his/her obligation, under section 7(a)(1) of the Law, to take all reasonable measures to safeguard his/her signature device and prevent its unauthorized use, *inter alia*, as stated in sections 4.5.1 and 4.5.2, above.

Hazards Inherent in using Electronic Signatures

The applicant and/or certificate owner is hereby warned that not safeguarding the certificate owner's signature device may make it possible for an unauthorized person to use of the certificate owner's electronic signature to incur undertakings in the name of the certificate owner, complete transactions and make representations on behalf of the certificate owner or take any other action that can be done using the electronic signature in a way that might cause extensive damages to the certificate owner and/or those relying on the certificate. Therefore, it is very important that the signature device be safeguarded and protected according to the directions detailed in these procedures, in the Law and its regulations.

4.5.9 Permissible Use of a Certificate on behalf of a Corporation or by an Authorized Signatory on behalf of an Individual:

The owner of a signature device who is an authorized signatory on behalf of a corporation or an individual may only use the certificate in the context of the authority granted him/her by the corporation or individual in the name of which the owner was authorized, and not in any other way.

Limitations on certificate usages will be executed only according the certificate owner's specific request. The form of the request will be formulated subject to the approval by the Registrar.

4.6 Relying Parties

4.6.1 Checking the Validity of an Electronic Signature:

Checking the validity of an electronic signature on an electronic message is a process that the relying party must carry out if he/she wishes to ensure (a) that ComSign confirms, with a valid certificate, that the electronic signature was created by the signatory whose name appears on the electronic certificate; (b) that the signed electronic message was not changed after the electronic signature was created; and (c) what limitations, if any, there are on the permitted use of the certificate.

4.6.2 Checking the List of Revoked Certificates in the ComSign Repository:

The recipient must check if a certificate has been revoked because a revoked certificate is not valid and not to be relied upon. It is possible to check the most up-to-date status of a certificate (if it has been revoked) by submitting an inquiry to the ComSign Repository using the link included in the certificate.

In accordance with the Law, regulations and instructions of the Registrar, ComSign publishes on its Internet site at www.comsign.co.il, a list of its signature verification devices that are used to issue certificates, as well as a list of revoked certificates related to these signature devices.

A relying party who does not verify the validity of a certificate as described above and below, risks relying on an invalid electronic certificate and may be held legally responsible for any damage that might be caused as a result of not checking the validity of the electronic certificate. ComSign will not bear any responsibility for any damage caused by relying on a revoked certificate if it is proven that it took all reasonable measures to fulfill its obligations according to Law and this CPS.

Regarding publicizing revoked certificates in the ComSign Repository, see chapter 2 above, including the exclusion concerning the publication of revoked certificates belonging to Magna users according to the securities act.

4.6.3 Checking the Permitted Uses of a Certificate:

The owner of a certificate and ComSign are permitted to limit the permitted uses of a certificate in accordance with the provisions of section 19(8) of the Law. These limitations are specified in the certificate or included in it by reference and provide a means for warning the certificate owner and relying parties regarding the permitted uses of the certificate and

limitations, if any, on its valid uses. ComSign will not be responsible for damage caused due to uses that violate these limitations. It is advised that users of electronic certificates issued by ComSign examine the content of the certificate and look for these warnings and limitations.

In addition, ComSign may limit its responsibility and note the limitation on certificates, as stated in section 21(b) of the Law and as provided by section 10.7, below.

Limitations on certificate usages will be executed only according the certificate owner's specific request. The form of the request will be formulated subject to the approval by the Registrar.

A certificate issued to a corporation or public institution or authorized signatory of an individual confirms that the person listed is an authorized signatory of the specified corporation or public institution or individual and authorized to act on its behalf. However, the certificate does not serve as evidence that the listed person is authorized to take a specific action on behalf of the corporation or public institution or individual. Persons relying on messages signed with an authorized electronic signature are solely responsible for conducting a due diligence check and using reasonable discretion as required when checking ordinary, handwritten signatures prior to relying on the content of those messages. A certificate serves as a warranty by ComSign only to the extent specifically stated in the Law, regulations and this CPS.

Limitations on certificate usages imposed at the request of the owner of the certificate will be executed only according the certificate owner's specific request. The form of the request will be formulated subject to the approval by the Registrar.

4.6.4 Responsibility of a Relying Party if an Electronic Certificate cannot be Verified:

A person, who chooses to rely on a revoked electronic certificate for a legal action taken after revocation of the certificate or on an electronic certificate that cannot be verified according to these procedures, may be held responsible for all risks that might be caused by relying on an electronic certificate whose validity he/she did not verify. An attempt to verify the validity of a revoked certificate whose revocation was published on the CRL and/or a verification check done when ComSign's database of revoked certificates and/or the computer of the relying party are not on-line will produce a reply indicating that the certificate is invalid

and/or that its validity cannot be verified. In this case, the relying party should not rely on the certificate. If he/she does so, it is at his/her sole responsibility.

Nothing in this section detracts from the obligation of ComSign to take all reasonable steps to fulfill its obligations according to the Law and this CPS.

4.7 Certificate Renewal

A certificate that is still valid can be renewed as described in section 3.2.5, subject to availability of the service and approval of the Registrar.

If the aforementioned renewal procedure is not available and/or if the certificate owner's electronic certificate is revoked or expired, or if the certificate owner did not set a password or does not remember it, renewal will require the complete regular application procedure, including identification of the applicant according to the same process used when the certificate was first issued.

ComSign reserves the right to amend or update the procedure for renewing certificates, subject to approval of the Registrar. Updated renewal procedures will be available (after their publication) on the Internet, as part of an amended version of the CPS, at: http://www.comsign.co.il/cps/.

4.7.1 Notifying the Certificate Owner of the Expiration Date:

No more than 45 days and no fewer than 30 days prior to the expiration date of a certificate, ComSign and/or it representative will notify the subscriber by e-mail (with a request for a return receipt) that the certificate in his/her possession will expire soon and specify the expiration date. If the subscriber does not make contact to renew his/her certificate and/or the read-receipt for the notification is not returned within 15 days after the notice was sent, a representative of ComSign will send daily e-mails (with requests for a return receipt) informing the subscriber that the certificate in his/her possession will expire and specifying the expiration date. A link to the appropriate site for renewing the certificate will be attached to the e-mail notification. The notice will explain that if the certificate owner wishes to the extent the validity of the certificate in his/her possession, he/she must click on the link. Renewal of certificate via a link will be possible after the approval of the Registrar is received.

In order to prevent fraud, the system will allow the certificate owner to enter the site associated with the link only via the electronic certificate in his/her possession, which will verify the identity of the applicant.

If no renewal request is made 15 days prior to the expiration of a certificate, ComSign will do its outmost to contact the certificate owner by telephone, using the details that he/she provided when applying for the certificate, in order to notify him/her of its expiry.

If certificate owner tries to follow the renewal link after the expiration date has passed and the certificate has expired, he/she will be notified that the certificate in his/her possession has expired and he/she can no longer extend its validity. If he/she wishes to have a new certificate issued, he/she must apply, in person, at the application site.

The owner of the certificate is solely responsible for its renewal. The aforementioned notifications are for the convenience of the certificate owner in the renewal process. Nothing in their delivery or non-delivery to the certificate owner obligates ComSign and/or imposes any liability and/or responsibility of any type on ComSign, either derived from and/or related to the expiration of the certificate and/or its non-renewal.

4.7.2 Renewal of a Certificate:

The owner of the certificate will click on the link in the notification that his/her certificate is expiring and use the valid electronic certificate in his/her possession to enter the site, and follow the instructions on the site. When the process is completed correctly, the validity of the electronic certificate in his/her possession will be extended for another identical period, subject to the conditions in the subscription agreement.

The certificate owner's key pair will remain unchanged during the period for which the certificate's validity is extended.

ComSign's servers are automatically upgraded with the certificate renewal.

Notification of the expiration date of a renewed certificate will be sent to the subscriber as described in section 4.7.1.

4.7.3 Expiry of a Certificate:

It is not possible to extend the validity of a electronic certificate that has expired.

If the owner of the certificate did not renew the certificate in his/her possession, it is revoked and he/she must apply for a new certificate as described in chapter 3 of this CPS.

The new certificate can be issued using the existing signatory device.

A new certificate may be issued in every active application station in accordance with instructions issued to the applicant by ComSign or its representative.

4.7.4 Key Pair Remains Unchanged upon Renewal:

The key pair for an electronic certificate will never be changed when a valid certificate is renewed.

The key pair for an electronic certificate will be changed when the owner of the certificate asks to extend the validity of an expired certificate. In this case, the certificate owner's electronic certificate is replaced with a new certificate and a new key pair.

4.8 Revocation and Expiry of Certificates

This section describes the circumstances in which a certificate may – or must – be revoked, the procedures for revoking certificates and the procedures related to the expiry of certificates.

4.8.1 Grounds for Certificate Revocation:

- A certificate will be revoked if ComSign has been notified by the certificate owner or learns in another way that a theft, loss, change, unauthorized use, defect or another harm to the certificate owner's control in the signatory device has occurred.
- The certificate owner or his/her agent or another third party explicitly authorized in the subscriber agreement,requests its revocation.
- A request from a Registration Agent that ComSign revoke a certificate that was issued by that Registration Agent, on the condition that this possibility exists and the reason that the Registration Agent is making the request was brought to the certificate owner's attention prior to issuance and is included in the subscription agreement with the certificate owner.
- As soon as ComSign learns that any detail on the certificate is incorrect, or that the reliability of the certificate has been compromised in another way.
- As soon as ComSign learns of a defect in its secured electronic signature or signature device, or in its software and hardware systems, or the data security of these systems in a way that might harm the reliability of its signature or the reliability of the electronic certificates that it issues.
- As soon as ComSign finds out that the certificate owner has died (if a person), or if a liquidation order has been issued (if a corporation) on the condition that ComSign is convinced that the notification is reliable.

- If it is required of ComSign in order to comply with the operational requirements listed in this CPS.
- If a substantive fault was found in the process for issuing the certificate, whether the source of the fault was ComSign or the applicant or any other party involved in the issuance process.

4.8.2 Request to Revoke a Certificate:

A request to revoke a certificate will be submitted by the owner of the certificate or his/her emissary or another third party whose appointment is explicitly noted in the subscription agreement. In the case of a certificate for a corporation and/or authorized signatory of a corporation or public institution, ComSign will revoke the certificate at the request of the corporation, public institution, organization or institution and/or in accordance with the provisions made in the subscription agreement and the application forms submitted when the certificate was issued.

4.8.3 Procedure for Submitting a Request to Revoke a Certificate:

- The owner of the certificate or his/her emissary or another third party whose appointment is explicitly noted in the subscription agreement will contact ComSign by telephone or in writing.
- The Applicant will be referred to a ComSign identification clerk who will handle the request.
- The ComSign identification clerk or the owner of the certificate will complete the revocation form.
- The ComSign identification clerk will verify the identity of the person requesting the revocation, in accordance with the procedure stated in section 3.2.6, above.
- If the verification is successful, the certificate will be revoked by the registration supervisor at ComSign. In any other case, the certificate will be suspended pending final clarification of the matter, subject to the internal procedures of ComSign.
- The revocation process will be in the control of more than one person.

4.8.4 Notification to the Certificate Owner of the Certificate's Revocation:

ComSign will notify the owner of the certificate that his/her certificate has been revoked, by sending a message to his/her e-mail address.

4.8.5 Destroyed Signature Device:

If a signature device is destroyed, the certificate must be revoked in accordance with the procedure in this section 4.8.

It is recommended to the owner of a certificate to destroy the signature device used for an electronic signature that was verified by a revoked electronic certificate, since it remains possible to the use the signature device to create electronic signatures even after the electronic certificate is revoked.

4.8.6 Non-renewal of a Revoked Certificate

ComSign will not renew a revoked certificate but rather require the process for issuing a new certificate in its place.

4.8.7 Expiry of a Certificate:

A certificate will be valid from the date of issue for the duration of the validity period stated in the subscription agreement, unless it is revoked prior to that date.

4.8.8 Publishing a new CRL to Magna

An updated CRL concerning the revoked certificates will be sent to the ISA according and as stated in the security act and its regulations

4.9 Checking the Status of Certificates

ComSign makes the ComSign Repository available to certificate owners, addressees and third parties. It contains, *inter alia*, lists of electronic certificates that include the ComSign signature verification device and lists of revoked certificates, which can be accessed on the Internet at http://fedir.comsign.co.il/crl.

A link to the list of revoked certificates can also be found in the body of the electronic certificate, see section 7.1, below.

ComSign may supply "push" service to persons requesting information about the status or change of status of a particular certificate. ComSign may charge a fee for this service. Notification of a change in the status of a certificate does not serve as a substitute for the obligation to check the databases of revoked certificates, unless otherwise determined by law or agreement.

4.10 Confirmation by ComSign after a Certificate has Expired

After a certificate has expired (as well as while it is still valid), ComSign may confirm that it issued a certain electronic certificate, and a court may require a representative of ComSign to appear before it and provide details regarding issuance of the certificate. The Law requires ComSign to save these details in accordance with the requirements of law, see section 5.6, below.

5. Physical, Personal and Records Security

The purpose of this chapter is to review for applicants, certificate owners and relying parties, the steps that ComSign takes in order to ensure physical security, the security of its personnel, and the protection of its records.

In addition, the chapter includes a description of the records that ComSign keeps and the types of information stored therein.

ComSign operates a security system based on computer hardware, software and procedures. Together, they provide a high level of accessibility, reliability, continuous operation and enforcement of the security procedures, as well as an adequate response to security risks.

ComSign is in compliance with Israel Standard (IS) 27001 for IT Security Management and is audited annually by The Standards Institution of Israel (SII).

According to the Law and regulations, ComSign is obligated to comply with the strict security standards and inspections by SII to receive its quality certification.

ComSign's work procedures, which are reviewed and approved by the Registrar, include, *inter alia*, security policy, protection of the assets, personnel security, physical security, operations management, access control for ComSign's signature infrastructure, reliability of the installation and maintenances, and survivability in event of a disaster. The work procedures relate, *inter alia*, to the following subjects:

Definition of the infrastructure for the information security systems (with reference to IS 27001 for IT Security Management). This includes job descriptions for IT security positions.

Management of security means and security procedures, including documenting the inventory of "critical means" and how they are protected.

Establishment of a senior management forum on security, including data security, that meets regularly, once a month.

Definition of a quality control and quality assurance system for data security.

Conducting an annual risk analysis survey or investigation of a critical IT security incident.

Definition of the supervision over the various contractors working at ComSign and outsourcing employees.

Full documentation of the security policy – goals, purposes, threats and risks.

5.1 Physical Security Controls

In all matters related to physical security measures, ComSign acts in accordance with the ComSign Manual of Physical and Environmental Security Procedures that has been submitted to the Registrar as part of ComSign's application for licensing as a CA. This procedure contains the structure and the location of the site where ComSign's computerized systems and offices operate, physical access procedures to various offices at ComSign, air conditioning, exposure to water, fire prevention and fire protection, data storage and protection, backups, and handling waste.

These are the main points of ComSign's physical security:

5.1.1 The facilities related to issuing certificates, preparing devices and managing revocations will operate in an environment that provides these services with physical protection against damage caused by unauthorized access to systems or data. ComSign stores critical elements of the system in a protected location, prevents unauthorized infiltration or entrances, in accordance with the nature of ComSign's activity and to the satisfaction of the Registrar.

5.1.2 No person who enters this physically secure area is left alone for an extended period, without the supervision of an authorized person.

5.1.3 The physical protection is achieved by creating clearly-defined, perimeter security barriers (meaning, physical obstacles) around the services for issuing certificates, preparing devices and managing revocations. Any section of the facility that is shared with another organization will be outside this area.

5.1.4 Physical and environmental security controls are in place to protect that facility's infrastructure resources, the resources of the systems themselves and the facilities that support their operations. ComSign's physical and environmental security policy for the systems related to issuing certificates, preparing devices and revocation management services provides a response for physical access control, protection against nature disasters, fire safety, failure of support services (for example, electricity and communications), building collapse, leaking pipes, theft, breaking and entering, disaster recovery, etc.

5.1.5 Controls are in place to protect against unauthorized removal of equipment, information, media and software related to ComSign's work as a CA.

5.1.6 ComSign maintains an inventory of information assets and classifies them in order to assign the necessary protection required for each asset, in accordance with its risk management

analysis. The Security Manager keeps the inventory list of critical assets and the way they are protected. These assets could be either physical assets and/or logical data assets.

5.1.7 ComSign conducts a risk analysis to ascertain the business risks and determine the necessary security requirements and operational procedures. The risk analysis, together with existing security declarations, procedures and security policy are examined by a risks auditor and the Registrar, in order to ensure that there are responses to all of the risks that have been identified.

5.1.8 A risk analysis is conducted at least once/year, by an external, independent data security expert who is approved by the Registrar. ComSign is committed to correcting the faults, if any, that are found immediately after receiving the results of the survey. A report on the corrective actions taken is sent to the Registrar.

5.2 Security Policy

ComSign acts in accordance with Appendix No. 4a, the Division of Functions, which is part of procedures that were submitted to the SII and approved as part of confirmation of compliance with IS 27001 and IS 9001, and submitted to and approved by the Registrar.

This appendix includes all of the authorization areas for the ComSign employees and physical access authorizations to the various areas within ComSign. The appendix presents the process for separating functions and the ability to supervise and ensure that at least two people participate in each critical action.

Each functionary has limited exclusive access to each area within the ComSign building. Senior officials have limited access to areas defined as “very sensitive” from a security perspective. There is no one official who has exclusive access to all areas.

All the activities that Comsign defines as critical are implemented by at least two different people.

ComSign ensures compartmentalized entry to sections of the systems critical for its operation as a CA, so that no one person has access to all of the critical sections.

In addition, Comsign uses identification and documentation systems that guarantee control over each employee’s access to its computer systems. See section 5.5, below.

5.3 Senior Management Forum on Security

Comsign has a Senior Management Security Forum that also deals with data security. It meets on a regular basis, once/month. The Security Forum includes the CEO of ComSign, the Security Manager, a senior technical representative, and representatives of the issuance staff. The Security

Forum is presented a monthly security report by the Security Manager and guides him/her in his/her work.

5.4 Procedures Related to Personnel Management

ComSign acts according to personnel and management procedures that provide reasonable security relating to the reliability and professional ability of its employees and satisfactory implementation of their duties. These procedures deal with:

- Appointing functionaries in ComSign including the required documents, verification of knowledge, experience and skills of candidates, signing non-disclosure and no conflicts of interest agreements, and conducting additional reliability tests of candidates for positions of trust.
- Periodic reliability testing of people in positions of trust.
- Training and drilling employees in data security subjects.
- Termination of employment/departure of an employee.

The aforementioned procedures are consistent with this CPS, the provisions of the Law and regulations, and instructions of the Registrar regarding personnel. ComSign employs personnel with the appropriate knowledge, experience, expertise and skills required for their positions and for the services they provide to ComSign.

ComSign takes several control measures before employing an employee. These measures include an interview by a representative of Human Resources, an interview by the direct manager, reliability test, checking references, and obtaining documents that testify to the candidate's ability to do the job (certifications, diplomas, documentation of employment experience, etc.) The CEO of ComSign gives the final approval for all appointments of employees to positions of trust in ComSign.

As noted above, all of ComSign's activities that are defined as critical are implemented by a minimum of two persons. ComSign maintains a reserve of personnel as necessary in order to comply with the requirements of the Law, regulations, instructions of the Registrar and procedures. There are no positions that are dependent on a single person and each person has a replacement of the same level.

5.4.1 Positions of Trust:

All employees, contractors and consultants of ComSign and/or its representatives (hereinabove and hereinafter, "personnel") who can access or control registration, issuance,

usage and revocation of certificates by ComSign, including access to limited-access ComSign Repository operations, will be considered, for the purpose of these procedures, as fulfilling a position requiring special trust ("position of trust"). The aforementioned personnel include but are not limited to customer service personnel, system management personnel, designated engineering personnel and management personnel whose job is to supervise the infrastructure of ComSign's trust systems. The positions of trust and all of the authorizations of each person in a position of trust are listed in the ComSign procedures. Persons in positions of trust are appointed to their position by the CEO of ComSign, with the approval by the Security Manager. People in positions of trust in ComSign are obligated to maintain confidentiality and prevent conflicts of interest in the context of their work at ComSign.

Persons in positions of trust are employed on a personal contract that includes details of the position and its components, as well as the commitment of each employee who is defined as being in a position of trust that he/she understands the components of the positions and undertake to act in accordance with the Law, regulations, procedures and employment contract.

ComSign ascertains that there are no conflicts of interest involving employees in positions of trust and that there is no overlapping of identity among employees in positions of trust. Comsign considers the following positions to be positions of trust:

- CEO of ComSign.
- Security Manager – responsible for implementation of the security procedures.
- Identification clerk.
- Verification clerk.
- Key managers and holders of keys.
- Anyone with keys to the safe.
- Registration manager.
- Logs examiner.

Each position has physical and logical access limits that are derived from the Law, regulations, instructions of the Registrar, and internal procedures of ComSign. The limitations are kept confidential. A person in a position of trust may not serve in more than

one of the following positions: security manager, registration clerk, administrator, systems operator or auditor.

5.4.2 Investigating and Checking Personnel:

ComSign and its representatives will conduct an initial investigation of all personnel working for ComSign. ComSign will conduct more comprehensive and detailed evaluations according to its human resources procedures and the instruction of the Registrar regarding personnel intended for positions of trust. ComSign will periodically investigate all persons in positions of trust to verify their reliability and professional capability, in accordance with ComSign's human resources procedures and the Registrar's instructions. Employees and representatives are not given access to sensitive areas or allowed to fulfill the functions of a position of trust until the required hiring investigations and checks are completed.

5.4.3 Prohibition on Employing Certain People:

Anyone who does not pass the initial investigation or a periodic investigation will not be employed by ComSign.

5.4.4 Operational Controls:

ComSign uses operational controls including organizational control, control of personnel, control of external parties and additional management controls. These controls include requirements related to training and instruction of ComSign's employees and/or its representatives, setting policy regulating the distribution of positions within ComSign, documentation requirements and procedures and scheduled audits.

The Security Manager conducts these operational controls to ascertain that work is being done in accordance with the procedures. If he/she finds that an employee is not doing what he/she is supposed to be doing, in accordance with his/her job description and the procedures, disciplinary action will be taken and the option of discontinuing his/her employment at ComSign will be considered.

5.4.5 Employee Training:

ComSign conducts training for its employees in accordance with an annual training program. The training including review of legal requirements, procedures and job descriptions, as well as learning lessons from security incidents and other events. The training program is produced during the last month of each calendar year and submitted to the Registrar.

5.4.6 Supervision of Contractors working at ComSign (there are no outsourcing employees):

When ComSign enters a contract with any subcontractor for work during which the subcontractor is given access to or control over application, issuance, usage or revocations processes of ComSign certificates, including work on limited-access parts of the ComSign Repository, the subcontractor undertakes, in its contract with ComSign, to uphold the strict security requirements to which ComSign is obligated in accordance with this CPS, the Law and regulations in respect of the work done by the subcontractor. In addition, the subcontractor will undertake to compensate ComSign in the event that any damage is caused as a result of breaching data security.

5.5 Documenting Actions using Records

5.5.1 Actions Documented in Records:

Comsign implements and manages reliable methods for maintaining records (a "log') of all the substantive actions it takes, for example: generating keys, applications for issuing a certificate, verification of an application for a certificate, revocations and recording them on the list of revoked certificates (CRL), entrances to and exits from the limited access areas of ComSign, records of the data security system and other similar records. Production of the log is an act of documenting actions taken using the ComSign computer system in the context of its services for issuing electronic certificates. The documentation is created by saving the records of actions taken by ComSign under the supervision of ComSign's Information Security Manager and in a manner that prevents it from being erased by unauthorized parties. The record includes both the actions taken and the identity of the person taking the action. The documentation is created using ComSign's command and control system. The purpose of the documentation is to make it possible to supervise and examine the actions taken by employees of ComSign during the processes of issuing and revoking certificates, etc. ComSign and/or its representatives will be careful to maintain reliable records in compliance with the documenting requirement stated in regulation 19 of Electronic Signature Regulations (Certification Authority), including documentation of critical actions and information related to all applications for issuing an electronic certificate and the issuance, usage, revocation, expiration or renewal of the certificates, including:

5.5.1.1. Identity of the certificate owner whose name is stated on each certificate and the documents that were used to identify him/her.

5.5.1.2. The identities of persons asking to revoke a certificate.

5.5.1.3. Other details listed on the certificate.

5.5.1.4. Substantive details related to the process for issuing electronic certificates, including the declaration of the applicant in accordance with regulation 13(b) of Electronic Signature Regulations (Hardware and Software Systems).

5.5.1.5. Documentation of details related to management of the private key (signature device) of ComSign, including those related to key generation, backup, storage and destruction and management of the key's software and hardware encryption.

5.5.1.6. Documentation of information security events, including attempts to compromise ComSign's software, to the extant that ComSign is aware of them, actions taken by ComSign with regard to information security, changes made in ComSign's information security system, hardware and software failures, etc.

The records may be kept as electronic messages or written documents, on the condition that their keys, storage, preservation and restoration are complete and precise, to the satisfaction of the Registrar. ComSign will keep the records listed in this section for 25 years.

5.5.2 Content of the Records:

The records include documentation of the date the record was made, the identity of the person taking the documented action in the record and the type of record.

5.5.3 Frequency the Records are Checked, Methods for Storage and Backup, and Persons with Access to the Records:

The records are checked on hourly, daily, weekly or monthly basis in accordance with the procedures approved by the Registrar. Actions defined as critical are to be checked by the Security Manager. In addition, ComSign will check the records in the event of any warning of a suspicious or unusual event.

The records are kept as part of electronic and manual audit reports. The reports are confidential and access to them is permitted only to specific officials after receiving the approval of the Security Manager. Any change in the records is permitted only if it complies with the person's defined job and must be documented. ComSign takes measures to prevent changes in the logs, and controls access to the manual and electronic reports.

The records containing Applicant details are kept in a secured room where access is permitted only to authorized people and only after they identify themselves using biometric identification and a personal code.

5.5.4 Using Records to Evaluate the Vulnerability of ComSign's Software and Hardware Systems:

The documented records are kept and examined in order to, *inter alia*, monitor and test the vulnerability of ComSign's software and hardware systems. The vulnerability level of ComSign's software and hardware systems (hereinafter, "risk assessment") is evaluated on the basis of data in the records. The most recent records are used for risk assessment, which is conducted daily, weekly, monthly or annually in accordance with ComSign's control and security procedures.

5.6 Storage Period for Records, Documents and Information Received from Certificate Owners

ComSign and/or its representatives will store, in a reliable manner, records related to the certificates for at least thirty (30) years after the date the certificate expired or was revoked. These records may be stored as computer retrievable electronic messages or as printed documents.

ComSign will store documents and information received from certificate owners and applicants for a period of at least 25 years, in accordance with regulation 20 of the Electronic Signature Regulations (Certification Authority).

5.7 Plans for Dealing with Unexpected Events and Disaster Response Plan

ComSign and/or its representatives will implement, document, store and periodically examine the applicable plans for responding to unexpected events, and the capabilities and procedures for responding to disaster, in a manner consistent with the provisions of this CPS and ComSign's security procedures (hereinafter, "the plans").

The plans are intended to respond to the following events:

- General loss of electric power and failure of the entire Uninterruptible Power Supply (UPS) system in the building where ComSign's computer system is located.
- Physical destruction of ComSign's computers and/or the information contained thereon, caused by *force majeure* and/or fire and/or flood and/or magnetic disruptions and/or any other cause beyond the control of ComSign.

ComSign maintains an alternative disaster recovery site (DRP) that enables ComSign to continue publishing the CRL even if a disaster damages ComSign's main site and prevents it from functioning. ComSign intends to take immediate action to upgrade the recovery site so that it will also be possible sign the CRL and issue new electronic certificates if the main site ceases to function.

These functions will be available at the earliest possible time after they are approved by the Registrar.

5.8 Termination or Interruption of ComSign's Activity

5.8.1 ComSign will terminate or interrupt its operations in the following circumstances:

- Issuance of a preemptory liquidation order for the liquidation of ComSign.
- The Board of Directors of ComSign adopts a resolution terminating ComSign's activity as a CA. In this case, the Registrar will be notified at least 30 days before the operations are terminated.
- The Registrar issues instructions to erase ComSign from the CA Register, in accordance with section 14 of the Law.

5.8.2 If ComSign's operations are terminated, ComSign will take the following steps, as described in section 18(a) or section 18(b) of Electronic Signature Regulations (Registration and Management) and the Securities Regulations (Signatory Certifier) 5763-2003, and act in accordance with the instructions of the Registrar:

- Refrain from issuing new electronic certificates.
- Revoke, as soon as possible, all of the valid electronic certificates that it has issued.
- Notify all certificate owners of this.
- Add the revoked certificates to the CRL.
- Transfer to the Registrar, within 72 hours after the termination of activity or erasure from the Registry, its signature devices and signature verification devices, and an accurate copy of the databases listing the electronic certificates that it issued and the revoked certificates.
- Within seven (7) days after the termination of activity transfer to the Registrar accurate copies of all the documents it received for the purpose of issuing electronic certificates.

5.8.3 If ComSign's operations are terminated for reasons other than the Registrar issuing instructions that ComSign be erased from the CA Registry, ComSign may, subject to approval of the Registrar and the conditions it sets, transfer its management to another CA. In this case, certificate owners have the right to demand the substitute CA to revoke their certificates.

5.8.4 Without derogating from the instructions of any law, Comsign will immediately notify the owners of all certificates that are valid on the date it shall terminate operations and take action to minimize the potential disruptions that subscribers and relying parties are likely to suffer as the result of the termination of its activity. The notice will be sent by e-mail and published in at least two daily newspapers.

5.8.5 Comsign will ensure the continued maintenance of the records required for providing proof of certification for legal proceedings.

5.8.6 ComSign will cancel the appointment of all Registration Agents authorized to act on its behalf.

6. Logical Security

The purpose of this chapter is to review for applicants, certificate owners and relying parties, the steps that ComSign takes in order to protect its signature devices (private keys) and those of the certificate owners. Furthermore, this chapter reviews the logical security processes ComSign uses for the comprehensive protection of its various systems.

The following points summarize the principles of ComSign's logical security:

Protect the integrity of ComSign's systems and data against viruses, malware and other unauthorized software.

Minimize the damage caused by security incidents by using incident reports and response procedures.

Secure handling of media used by ComSign in order to protect it against damage, theft and unauthorized access.

Maintain media management procedures that provide protection against the aging and physical deterioration of media during the period that records must be kept.

Implement procedures for positions of trust and management that influence the supply of services for issuing certificates.

Secure use of all media in accordance with the requirements of the data classification scheme. Disposal of media containing sensitive data is carried out only when the media is not needed.

Monitor the capacity requirements and create forecast of future capacity requirements in order to ensure the accessibility of processing power and storage means.

Act and cooperate, within reasonable amount of time, in order to rapidly respond to incidents and limit the impact of security breaches. All incidents are to be reported as quickly as possible after they occur.

Maintain requirement-compliant control processes that commence operations as soon as the system boots and cease operation only when the system is turned off.

Regularly monitor and review the control logs in order to identify any indications of malicious activity.

6.1 ComSign's Signature Device

The length of ComSign's signature device (private key) is 2048 bytes. A reliable hardware device (FIPS 140-1, Level 3) is used to generate, protect and destroy ComSign's signature device (private key). ComSign's key pair is valid until March 19, 2029. The key pair may be replaced prior to that date, subject to the prior approval of the Registrar. The new public key will be published in ComSign's Repository. Moreover, the key pair will also be replaced if the regulations defining the

size and/or algorithm of ComSign signature device (private key) is changed or there is any other reason that requires replacement of the key pair, subject to prior approval of the Registrar.

The algorithms used for signing certificates and their parameters will comply, at all times, with the requirements of the Law, regulations and instructions of the Registrar.

6.2 Protecting the Signature Device – of the Certificate Owner and ComSign

6.2.1 Protecting ComSign's Signature Device:

In order to diffuse the risk of fraud, the following measures are taken to protect ComSign's signature device (private key): ComSign's signature device (private key) is completely encrypted on a hardware-based encryption card and stored in ComSign's safe. The encryption key that encrypted the signature device (private key) is divided into several parts. Each part is deposited with an employee of ComSign who does not directly deal with certificate managing and issuing services. All of these employees undergo strict, periodic reliability investigations. Only by assembling all parts, using a controlled and supervised process, would make it possible to reconstruct the encryption key.

ComSign's CA signature device that it uses to sign electronic certificates was generated by ComSign alone, and is kept in its sole possession. The signature device of ComSign and/or any of its representatives are protected by reliable hardware and security measures that comply with the requirements of the Electronic Signature Regulations (Hardware and Software Systems), meaning that ComSign's signature device complies with all of the following:

(1) Based on an RSA or DSA key that is at least 2,048 bits long;

(2) Protected by means that comply with the FIPS 140-2, Level 3 standard, at least;

(3) Backed-up using protected, secure means, to the satisfaction of the Registrar; the back-up is stored separately;

(4) Additional requirements issued by the Registrar in order to provide a reasonable level of security against infiltration, disruption or malicious use.

Harm to ComSign's signature device is defined as a "disaster." In order to respond to a disaster of this type, ComSign has designed and maintains a plan for business continuity in the event of disaster. The business continuity (or "disaster recovery") plan of ComSign provides a response to damage or a suspicion of damage to ComSign's signature device. Therefore, for example, the system data that ComSign requires for continuous operation is

backed-up and stored in appropriate, safe locations in a manner that will make it possible for ComSign to return to work within a reasonable amount of time after a disaster. The back-up and recovery functions are implemented by persons in positions of trust, as noted above.

In the event of damage to ComSign's signature device, ComSign will act as follows:

- Immediately inform the Registrar and all certificate holders of the damage by e-mail and publication in at least two daily newspapers.
- Immediately inform the registration agents and all other parties with whom ComSign has contracts requiring such notice.

6.2.2 Confidentiality Partners:

ComSign will utilize confidentiality partners who each hold, separately, parts of its private key(s), to improve the reliability of its signature device and to enable key reconstructions as defined in section 6.1, above.

The use of confidentiality partners is intended to ensure the security and protection of ComSign's signature device so that at least six persons are needed to generate and encrypt ComSign's signature device. For decrypting and using the device, at least four persons are required

6.2.3 Hardware Protection:

ComSign will use approved, reliable, hardware-based (HSM), encryption modules for all actions that require using its signature device.

6.2.4 Protecting a Certificate Owner's Signature Device

The certificate owner's signature device must be protected using encryption software or hardware tokens, in accordance with the requirements of the Electronic Signature Regulations (Hardware and Software Systems) and as specified in this CPS [See section 4.5.8, above].

Certificates are issued in accordance with the procedure described in section 4.3, above. In particular, ComSign does not receive, keep or create the signature device of applicants or certificate owners or any information that would enable reconstructing or creating a signature device for or on behalf of the applicant or certificate owner, and does not have access to signature device and/or any of the aforementioned information. If the applicant acquired the hardware device that creates and houses the signature device from ComSign, ComSign hereby gives notice it takes responsibility for the compliance of the signature device

and the signature verification device that identifies the signature device with the provisions of regulation 8 of the Electronic Signature Regulations (Hardware and Software Systems). If the applicant did not acquire the hardware device where the signature device will be installed from ComSign, ComSign will act in accordance with section 4.1.17, above, and issue an electronic certificate to the applicant only after it checked that the signature device and the signature verification device that identifies the signature device comply with the provisions of regulation 8 of the Electronic Signature Regulations (Hardware and Software Systems). Regarding compliance with regulation 8(1)(b) and (c) of the aforementioned regulations, ComSign may rely on a declaration by the applicant regarding the signature device that device he/she uses, its manner of operation and access to it. In these two cases, ComSign is responsible for the electronic certificate issued for the signature device, in accordance with the Law and this CPS.

6.2.5 Transferring Responsibility for a Signature Device Does Not Release Certificate Owner from Responsibility:

Transferring responsibility for a signature device, exposing it to a third party and/or transferring control over it to a third party does not release the transferring party (the certificate owner) from his/her responsibility and liability for the creation, usage, safe keeping or proper destruction of his/her signature device.

6.3 Encryption

Today, ComSign's certificate issuing services are based upon the encryption algorithm (RSA) for the keys. However, ComSign is committed to supporting other standards for electronic signature as alternatives are developed, according to the demands of the market, and subject to the Law and its regulations.

The algorithms used for signing electronic certificates and their parameters will, at all times, comply with the accepted standards and instructions of the Registrar.

6.4 Security of Messages

Every message transmitted between ComSign and other parties in accordance with these procedures will be transferred in a way that provides appropriate security mechanisms. Without limiting the generality of the above mentioned statement, electronic messages, return receipts for electronic messages and any other message that has an affect on the security of the certificate issuing services shall also be suitably secured.

In accordance with regulation 5(a) of the Electronic Signature Regulations (Hardware and Software Systems), the means of communications used for identifying an applicant, issuing and revoking an electronic certificate will comply with high-level security requirements.

6.5 The Reliability of the Systems

For providing these services, ComSign and its representatives will use only reliable systems that comply with the technical requirements of the Law and its regulations.

In accordance with regulation 5(b) of the Electronic Signature Regulations (Hardware and Software Systems), components of the system used for identifying an applicant, issuing and revoking an electronic certificate will comply with the Common Criteria EAL4 standard.

Comsign uses reliable information security systems. These systems are kept concealed from the general public but are audited by external parties. One of these audits is an annual audit of ComSign conducted by an independent auditor who checks the systems' reliability, and that work according to the procedures is done according to the requirements of the Registrar.

Moreover, an annual risk analysis is conducted by an external, independent data security expert who is approved by the Registrar. It should be noted that ComSign complies with the ISO 27001 Standard for Information Security and is audited by independent auditors to ensure compliance with these standards.

6.6 Synchronizing Critical Operations according to a Real-Time Clock

All of ComSign's critical operations are synchronized to a time clock that relies on a trustworthy, external, third-party time source that supplies official Universal Time readings at any given moment.

6.7 Date and Time Stamps

A date and time stamp is intended to improve the reliability of ComSign's certificate issuing services. A date and time stamp attests to the correct date and time when an action was performed and the identity of the person or device that created the stamp. The date and time stamp reflects Greenwich Mean Time (GMT) and uses the Universal Time Convention (UTC). A ComSign date and time stamp relies on a trustworthy, third-party time source that supplies official Universal Time readings at any given moment.

ComSign will imprint a date and time stamp on the following data, whether directly on the data itself or on a parallel, reliable audit channel:

Certificates.

Lists of revoked certificates and other records of databases of revoked certificates.

Additional data, according to this CPS.

7. Certificate and CRL Profiles

7.1 Certificate Structure

7.1.1 Structure Layout for an Individual's Certificate:

Field Name	Description	Example
Version	Certificate Version	"V3"
Serial number	The certificate's serial number. Single-value this number is one value of monovalent	"bc be ac 46 8b 09 ad e5 2d 31 ed f0 8e 00 02 ed ab"
Signature algorithm	The signature algorithm used by the certificate owner. Hash algorithm may be either an SHA2 or SHA1 type, as instructed by the Registrar.	"sha1RSA"
Issuer (CA)	Fields describing the CA	
	Full name – CN	Corporations
	CA name – O	"ComSign Ltd"
	Country -C	"IL"
Validity	Fields describing the certificate's validity	
Valid from	Date the certificate becomes valid (issue date)	"Tuesday, December 10 06:10:33 2002"
Valid to	Expiration date	"Thursday, December 08 05:24:21 2003"
Subject	Details of the Individual Certificate Owner	
	CN (Full name of the certificate owner in English and his/her identity number)	"Levy Israel ID_012345678"
	Family name (English) SN	Levy
	First name (English) G	Israel
	Identity number	"01_012345678"
	O identity code and the corporation number	07-012345678
	OU – Full name of the certificate owner	Levy Israel
	Position – T	Personal certificate
	Country – C	IL
Public Key	Public key of the certificate owner length	RSA 2048 Bits

CRL Distribution Points	Link to the CRL	[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://fedir.comsign.co.il/crl/Corporations.crl [2] CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl1.comsign.co.il/crl/Corporations.crl
qcStatements	1.3.6.1.5.5.7.1.3	This certificate is limited to NIS 50,000.
Authority Key Identifier	Key Identifier of an intermediate certificate	KeyID= 93 a1 4b 84 20 bc de 68 60 9b dc 85 d5 83 51 cd 8c d9 c8 b2
Certificate policies	CPS that regulates operations of the CA (ComSign)	[1]Certificate Policy : Policy Identifier=1.3.6.1.4.1.19389.2.1.1 [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.comsign.co.il/CPS [1,2] Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Reference: Organization=ComSign Notice Number=11 Notice Text=The certificate owner was identified in person on the basis of documents and/or other identifying information. The procedures of ComSign will apply to use of this certificate. The responsibility and liability of ComSign is limited as described in the procedures. Limitations on use of the certificate – optional This certificate is installed on an automatic signature device – if the certificate is installed on such a device.
Enhanced Key Usage	This usage changed for sign and identify certificates	Secure e-mail (1.3.6.1.5.5.7.3.4) and/or Client authentication (1.3.6.1.5.5.7.3.2) Smart card logon (1.3.6.1.4.1.311.20.2.2)

Details of the authorized signatory Subject's alternative name	Details of the authorized signatory	
	E-mail address of the certificate owner RFC22 Name	"israelleavy@israel.co.il
	Country – C	"IL"
	O – identity code and the corporation number	07-012345678"
	OU Full name in Hebrew	לוי ישראל
	Position – T	תעודה אישית
	Family name (Hebrew) – SN	"לוי"
	First name (Hebrew) – G	"ישראל"
	CN (Name of the certificate owner in English and identity number)	לוי ישראל 12345678ID_
Authority Info [1] Access		[1] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://fedir.comsign.co.il/cert/Corporations.crt
Netscape Cert Type		SMIME (20)
Subject Key Identifier		07 19 61 9a d1 4e 07 71 06 25 a3 78 71 19 bc b3 0a 83 7c 5c
Key Usage	Description of the purposes for which it is permissible to use the certificate.	Digital Signature, Non-Repudiation, Key Encipherment (e0)
Thumbprint algorithm	The signature algorithm used to sign the certificate.	"sha1"
Thumbprint	Details of the certificate signed by the CA	e2 a1 5a 40 07 e4 a3 c3 88 66 91 14 5b 9c 00 ff e4 1d 24 8e

7.1.2 Layout Structure for the Certificate of an Authorized Signatory of a Corporation or Public Institution:

Field Name	Description	Example
Version	Certificate Version	"V3"
Serial number	The certificate's serial number. Single-value this number is one value of monovalent	"bc be ac 46 8b 09 ad e5 2d 31 ed f0 8e 00 02 ed ab"
Signature algorithm	The signature algorithm used by the certificate owner. Hash algorithm may be either an SHA2 or SHA1 type, as instructed by the Registrar.	"sha1RSA"
Issuer (CA)	Fields describing the CA	
	Full name CN	"Corporations"
	CA name - O	"ComSign, Ltd."
	Country	"IL"
Validity	Fields describing the certificate's validity	
Valid from	Date the certificate becomes valid (issue date)	"Tuesday, December 10 06:10:33 2002"
Valid to	Expiration date	"Thursday, December 08 05:24:21 2003"
Details of the authorized signatory of the corporation or public institution Subject	Details of the Authorized Signatory of a Corporation or Public Institution:	
	Full name CN	Avraham Shlomo ID_012345678
	Family name (English) SN	Avraham
	First name (English) G	Shlomo
	Identity number	"0123456789"
	O – Code and company number	05-519999999
	OU Name of the Corporation/ Public Institution in English	Comda
	Position – T	Manager
	Country – C	"IL"
Public Key	Public key of the certificate owner length	RSA (2048 bits)

CRL Distribution Points	Link to the CRL	[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://fedir.comsign.co.il/crl/Corporations.crl [2] CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl1.comsign.co.il/crl/Corporations.crl
1.3.6.1.5.5.7.1.3	qcStatements	30 48 30 3c 06 08 2b 06 0H0<..+. 01 05 05 07 0b 01 30 30 . ..... 00 30 2e 81 29 54 68 69 73 0..) This 20 63 65 72 74 69 66 69 certifi 63 61 74 65 20 69 73 20 cate is 6c 69 6d 69 74 65 64 20 limited 74 6f 20 35 30 2c 30 30 t o 50,00 30 20 4e 49 53 81 01 20 0 NIS.. 30 08 06 06 04 00 8e 46 0..... F 0b 01 ..
Authority Key Identifier	Key ID	KeyID= 93 a1 4b 84 20 bc de 68 60 9b dc 85 d5 83 51 cd 8c d9 c8 b2
Regarding certificates issued for MOD applicants, the content of the "O" and "OU" fields are switched.		
Certificate policies	CPS that regulates operations of the CA (ComSign)	[1]Certificate Policy : Policy Identifier=1.3.6.1.4.1.19389.2.1.1 [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.comsign.co.il/CPS [1,2] Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Reference: Organization=ComSign Notice Number=11 Notice Text=The certificate owner was identified in person on the basis of documents and/or other identifying information. The procedures of ComSign will apply to use of this certificate. The responsibility and liability of ComSign is limited as described in the procedures. Use of this certificate is subject to the signature rights procedure of the corporation/public institution. Limitations on use of the certificate – optional This certificate is installed on an automatic signature device – if the certificate is installed on such a device.

Key Usage	Description of the permitted uses for the certificate	Secure Email (1.3.6.1.5.5.7.3.4) Authentication (1.3.6.1.5.5.7.3.2) Smart card logon (1.3.6.1.4.1.311.20.2.2)
Details of the authorized signatory Subject's alternative name	Details of the authorized signatory of the corporation/public institution	
	E-mail address RFC822 Name	Shlomo@test.co.il"
	Country – C	"IL"
	O – Code and company number	05-519999999
	OU – Name of the Corporation/ Public Institution in hebrew	Comda
	Position – T	מנהל
	Family name (Hebrew) – SN	"אברהם"
	First name (Hebrew) – G	"שלמה"
Authority Info [1] Access	Full name CN	אברהם שלמה ID_012345678
Authority Information Access		[1] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://fedir.comsign.co.il/cert/Corporations.crt
Netscape Cert Type		SMIME (20)
Subject Key Identifier		3 b a0 59 1c 5f 7c 2b 1f f0 3f df e0 25 55 09 67 10 f2 52 b6
Key Usage	Description of the purposes for which it is permissible to use the certificate.	Digital Signature, Non-Repudiation, Key Encipherment (e0)
Thumbprint algorithm	The signature algorithm used to sign the certificate.	"sha1"
Thumbprint	Details of the certificate signed by the CA	"f1 36 18 f7 fe 2a 1a 34 24 47 e6 7f 85 24 93 40 4d d5 18 73"
Regarding certificates issued for MOD applicants, the content of the "O" and "OU" fields are switched.		

7.1.3 Layout Structure for a Certificate for Users of the Electronic Full Disclosure System ("*Magna*"):

Field Name	Description	Example
Version	Certificate Version	"V3"
Serial number	The certificate's serial number. Single-value this number is one value of monovalent	"b7 59 5f 17 4e b7 69 40 9e 94 b0 00ý d1 76 a8 ac 09"
Signature algorithm	The signature algorithm used by the certificate owner. Hash Algorithm may be either an SHA2 or SHA1 type, as instructed by the Registrar.	"sha1RSA"
Issuer (CA)	Fields describing the CA	
	Country	"IL"
	CA name - O	"ISA"
	Full name CN	"ComSign ISA Magna Issuing CA"
Validity	Fields describing the certificate's validity	
Valid from	Date the certificate becomes valid (issue date)	"Tuesday, December 10 06:10:33 2002"
Valid to	Expiration date	"Thursday, December 08 05:24:21 2003"
Subject	Details of the Authorized Signatory of a Corporation or Public Institution:	
	Full name CN	Amir Israeli ID#012345678@IL 000000007876
	Family name (Hebrew) – SN	"עמיר"
	First name (Hebrew) – G	ישראלי
	0.3.2342.13200300.100.1.1	"ID#012345678@IL"
	OU – Sub-unit of the Corporation/ Public Institution (in English)	Magna
	O – Name of the Corporation/ Public Institution in English	ISA
	Country – C	IL

	2.5.4.65	The certificate owner was identified in person on the basis of documents and/or information as required by law. The signature verification device was checked and approved. The procedures of ComSign will apply to use of this certificate. The overall responsibility and liability of ComSign and its representatives towards any person with respect to a specific certificate will be limited to certificates issued to applicants (1) who are required by law to use them (2) at the request of any authority of the State of Israel for amounts not exceeding NIS 500,000 (five hundred thousand). Regarding all electronic signatures and transactions related to that certificate, the use of the certificate by the authorized signatory of a corporation/public institution is subject to the respective signature rights procedure of the corporation/public institution. ComSign is registered with the Registrar of Certification Authorities in Israel.
Public Key	Public key of the certificate owner	RSA (2048 bits)
Enhanced Key Usage	Purpose of the certificate	Client Authentication (1.3.6.1.5.5.7.3.2) Microsoft Trust List Signing (1.3.6.1.4.1.311.10.3.1)
Authority Key Identifier	Key identifier of the intermediary certificate	KeyID= 40 e6 4a 17 0c 2b dc d1 e1 0c 29 b4 ba 85 44 55 d0 2f e5 8c
Basic constraints		Subject Type= End Entity Path Length Constraint= None
Certificate policies	CPS that regulates operations of the CA (ComSign)	[1]Certificate Policy : Policy Identifier=User Notice [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.comsign.co.il/CPS [1,2] Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Reference: Organization=Replace this text Notice Number=11\ Notice Text=”Please press the [More Info] button to access the Hebrew CPS.”

CRL Distribution Points	Link to the CRL	[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://fedir.comsign.co.il/crl/Corporations.crl [2] CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl1.comsign.co.il/crl/Corporations.crl
Details of the authorized signatory Subject's alternative name	E-mail address of the certificate owner – RFC822	amirisraeli@test.co.il
2.5.29.9	Subject directory attributes	30 17 30 15 06 03 55 1d 0. 0...U. 09 31 0e 13 0c 30 30 30 .1... 000 30 30 30 30 30 37 38 37 00000787 36 6
Key Subject Identifier		b 98 bd 66 b2 3e f5 5a bf 82 6f c7 b8 ad 4e 7c b1 1 82 91 85
Key Usage		Digital Signature, Non- Repudiation (c0)
Thumbprint algorithm	The signature algorithm used to sign the certificate.	"sha1"
Thumbprint	Details of the certificate signed by the CA	"8 e a2 c8 0b ed 87 1a 80 7d a8 06 77 69 c0 cd 9a 68 d6 2e da"

7.1.4 Structure Layout for Domain Control Validated (DV) SSL Certificated:

Field Name	Description	Example
Version	Certificate Version	"V3"
Serial number	The certificate's serial number. Single-value this number is one value of monovalent	"f5 bb ad ea 31 23 4b 00 5d 5b 4f 76 de 6f 8b 02 e0 fd df f0"
Signature algorithm	The signature algorithm used by the certificate owner. The hash algorithm is of SHA2 type.	"SHA256 with RSA Encryption" OID = 1.2.840.113549.1.1.11
Issuer (CA)	Fields describing the CA	
	Full name – CN	ComSign Organizational CA
	CA name – O	"ComSign Ltd"

	Locality – L	"Tel Aviv"
	Country -C	“IL”
Validity	Fields describing the certificate’s validity	
Valid from	Date the certificate becomes valid (issue date)	“Tuesday, November 04 06:10:33 2014”
Valid to	Expiration date	“Thursday, November 02 05:24:21 2017”
Subject	Details of the Individual Certificate Owner	
	CN – A DNS Name containing the Fully-Qualified Domain Name or an IP Address containing the IP address of a host to be covered by the certificate	“www.test.com”
	OU – A fixed description of the certificate type.	"Domain Control Validated"
Public Key	Public key of the certificate owner length	RSA 2048 Bits
Authority Information Access	indicates how to access information and services for the issuer: [1] OCSP Service location. [2] Certification Authority Issuer Certificate	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp1.comsign.co.il [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://fedir.comsign.co.il/cacert/ComsignOrganizationalCA.crt
Authority Key Identifier	Key Identifier of an intermediate certificate	KeyID=f5 bb ad ea 31 23 4b 00 5d 5b 4f 76 de 6f 8b 02 e0 fd df f0

Certificate policies	Specifies the regulations for operations of the CA (ComSign Organizational CA): [1] ComSign CPS – DV Section [2] Domain validated with Compliance to the Baseline Requirements of the CA/Browser Forum – No entity identity asserted	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.19389.3.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.comsign.co.il/CPS [2]Certificate Policy: Policy Identifier=2.23.140.1.2.1
CRL Distribution Points	Link to the CRL	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://fedir.comsign.co.il/crl/ComsignOrganizationalCa.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl1.comsign.co.il/crl/ComsignOrganizationalCa.crl
Enhanced Key Usage	purposes for which the certified public key may be used	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)
Subject Key Identifier	Identification of the certificate according to its particular public key	“f5 bb ad ea 31 23 4b 00 5d 5b 4f 76 de 6f 8b 02 e0 fd df f0”
Subject alternative name	A DNS Name containing the Fully-Qualified Domain Name or an IP Address containing the IP address of a host to be covered by the certificate	“www.test.com"
Key Usage	Description of the purposes for which it is permissible to use the certificate.	Digital Signature, Key Encipherment (a0)

7.1.4.1. DV SSL Certificate Policy identifiers

7.1.4.1.1. The following Certificate Policy identifier is included in the certificate. It is reserved for use by any CA as an optional means of asserting compliance with the CA Browser Forum Requirements as follows:

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baselinerequirements(2) domain-validated(1)} (2.23.140.1.2.1). The Certificate complies with these Requirements, and it **lacks** Subject Identity Information except for the Domain Name authorization.

7.1.4.1.2. All DV-SSL Certificates also include a policy identifier in the Certificate's certificatePolicies extension that indicates the compliance with CA Browser Forum Requirements. This Certificate Policy identifier points to the publically disclosed Certificate Policy Statement of Comsign:

Policy Identifier=1.3.6.1.4.1.19389.3.1.1
[1,1]Policy Qualifier Info:
Policy Qualifier Id=CPS
Qualifier:
http://www.comsign.co.il/CPS

7.1.4.1.3. DV SSL Subject information fields

All DV-SSL certificates do not include organizationName, streetAddress, localityName, state Or ProvinceName, or postalCode in the Subject field.

The following field is included in order to emphasize the lack of conformation of any of these issues regarding the Certificate Applicant:

subject:organizationalUnitName: OU = "Domain Control Validated"

7.1.5 Structure Layout for Organization Identity Validated (OV) SSL Certificated:

Field Name	Description	Example
Version	Certificate Version	"V3"
Serial number	The certificate's serial number. Single-value this number is one value of monovalent	"f5 bb ad ea 31 23 4b 00 5d 5b 4f 76 de 6f 8b 02 e0 fd df f0"

Signature algorithm	The signature algorithm used by the certificate owner. The hash algorithm is of SHA2 type.	"SHA256 with RSA Encryption" OID = 1.2.840.113549.1.1.11
Issuer (CA)	Fields describing the CA	
	Full name – CN	ComSign Organizational CA
	CA name – O	"ComSign Ltd"
	Locality – L	"Tel Aviv"
	Country -C	"IL"
Validity	Fields describing the certificate's validity	
Valid from	Date the certificate becomes valid (issue date)	"Tuesday, November 04 06:10:33 2014"
Valid to	Expiration date	"Thursday, November 02 05:24:21 2017"
Subject	Details of the Individual Certificate Owner	
	CN – A DNS Name containing the Fully-Qualified Domain Name or an IP Address containing the IP address of a host to be covered by the certificate	"www.test.com"
	O – Organization Name	O = Test Ltd.
	L – Locality	"Tel Aviv"
	S - State	"Israel"
	C - Country	"Israel"
	OU – A fixed description of the certificate type.	"Domain Control Validated"
Public Key	Public key of the certificate owner length	RSA 2048 Bits

Authority Information Access	indicates how to access information and services for the issuer: [1] OCSP Service location. [2] Certification Authority Issuer Certificate	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp1.comsign.co.il [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://fedir.comsign.co.il/cacert/ComsignOrganizationalCA.crt
Authority Key Identifier	Key Identifier of an intermediate certificate	KeyID=f5 bb ad ea 31 23 4b 00 5d 5b 4f 76 de 6f 8b 02 e0 fd df f0
Certificate policies	Specifies the regulations for operations of the CA (ComSign Organizational CA): [1] ComSign CPS – OV Section [2] Organization validated with Compliance to the Baseline Requirements of the CA/Browser Forum – Subject identity validated	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.19389.3.1.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.comsign.co.il/CPS [2]Certificate Policy: Policy Identifier=2.23.140.1.2.2
CRL Distribution Points	Link to the CRL	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://fedir.comsign.co.il/crl/ComsignOrganizationalCa.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl1.comsign.co.il/crl/ComsignOrganizationalCa.crl
Enhanced Key Usage	purposes for which the certified public key may be used	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)

Subject Key Identifier	Identification of the certificate according to its particular public key	"f5 bb ad ea 31 23 4b 00 5d 5b 4f 76 de 6f 8b 02 e0 fd df f0"
Subject alternative name	A DNS Name containing the Fully-Qualified Domain Name or an IP Address containing the IP address of a host to be covered by the certificate	"www.test.com"
Key Usage	Description of the purposes for which it is permissible to use the certificate.	Digital Signature, Key Encipherment (a0)

7.1.5.1. OV SSL Certificate Policy identifiers

7.1.5.1.1. The following Certificate Policy identifier is included in the certificate. It is reserved for use by any CA as an optional means of asserting compliance with the CA Browser Forum Requirements as follows:

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baselinerequirements(2) subject-identity-validated(2)} (2.23.140.1.2.2). The Certificate complies with these Requirements, and it **includes** Subject Identity Information.

7.1.5.1.2. All OV-SSL Certificates also include a policy identifier in the Certificate's certificatePolicies extension that indicates the compliance with CA Browser Forum Requirements. This Certificate Policy identifier points to the publically disclosed Certificate Policy Statement of Comsign:

Policy Identifier=1.3.6.1.4.1.19389.3.1.2
[1,1]Policy Qualifier Info:
Policy Qualifier Id=CPS
Qualifier:
http://www.comsign.co.il/CPS

7.2 Links (Pointers) to the CPS in a Certificate

In order to enable users of electronic certificates to locate and access these procedures and other relevant information easily, computer-based links are used (URLs or others identifiers and mechanisms.)

7.3 Warnings, Liability and Responsibility Limitations in a Certificate

Each certificate contains a reference to the limitations on ComSign's liability and responsibility toward the applicants, certificate owners and third parties who rely on the certificate or might be harmed due to the use of the certificate, with a link to the full version of the aforementioned warnings, limitations, and limits of responsibility as described in this CPS.

7.4 Structure of the CRL

Field Name	Description	Example
Version		V2
The Certificate Authority	Fields describing the CA (CN, O, OU)	
	Name of the Certificate Authority CN	"Corporations"
	Organization name – O	"ComSign Ltd."
	Country	"IL"
Validity	Fields describing the CRL's validity	
	Date the CRL was published	"Tuesday, December 10 06:10:33 2002"
	Date the next CRL wll be published (at the latest)	"Wednesday, December 11 06:10:33 2002"
Signature algorithm	The signature algorithm used by the certificate owner. May be either a SHA2 or SHA1 type, as instructed by the Registrar.	"sha1RSA"
revoked certificates	Fields describing the revoked certificates	
	Serial number of the certificate, Single-value	"bc be ac 46 8b 09 ad e5 2d 31 ed f0 8e 00 02 ed ab"
	Date the certificate was revoked	"Tuesday, December 10 06:10:33 2002"
	Serial number of the certificate, Single-value	"bc be ac 46 8b 09 ad e5 2d 31 ed f0 8e 00 02 ed ab"
	Date the certificate was revoked	"Tuesday, December 10 06:10:33 2002"
Serial number	Serial number of the CRL	#

8. Audits

ComSign is subject to the procedures approved by the Registrar. The authority granted to the Registrar also includes auditing and inspection processes in accordance with the Law and regulations. Moreover, audits are conducted at ComSign in accordance with Regulation 4 of the Electronic Signature Regulations (Registration and Management of Certification Authority) and the need to submit the auditor's opinion to the Registrar as required by the Law and regulations.

Comsign will ensure that a professional certified in data security, who is approved by the Registrar (hereinafter, "the auditor") audits ComSign's work as a CA at least once/year, in order to examine and evaluate compliance with these procedures, and the instructions, regulations and standards that apply to ComSign. The auditor will be an independent contractor who is not employed by nor subject to ComSign in any manner.

ComSign will study the audit reports and take care to correct any shortcomings, as soon as possible.

Furthermore, in order to comply with the standards IS 27001 and ISO 9000, audits will be conducted by organizations that are licensed to conduct audits in accordance with the requirements of those standards.

9. Registration Agents

9.1 Introduction

Some of the certificate issuing services provided by ComSign may also be provided by representatives on its behalf. The representatives of ComSign must be approved by the Registrar before being appointed to serve as Registration Agents. The representative acts at ComSign's discretion and subject to the prior, written approval of the Registrar, after ComSign submits a detailed application. ComSign's representatives will participate in the services provided by ComSign for all matters relating to receiving and handling applications for electronic certificates, identifying applicants, and registering them. Representatives of Comsign are obligated to act in accordance with the Law, its regulations and instructions given by the Registrar, and comply with all of the various requirements listed in this CPS.

ComSign is responsible for the work of its representatives as determined by Law.

9.2 An Application to act as a ComSign Registration Agent

9.2.1 Any person and/or corporation and/or a public institution that wishes to act as a Registration Agent for ComSign will submit to ComSign a signed application, verified and approved by an attorney. An application not verified by an attorney and/or not containing all of the required information will not be processed. The application shall include, *inter alia*, the following details:

9.2.1.1. Name, address, fax and telephone numbers and e-mail address/(es) of the applicant, its administrative contact people and its authorized representatives.

9.2.1.2. Details of any information that might affect the reliability of the applicant (for example, current or former insolvency) and which might materially influence the ability of the applicant to act as a Registration Agent for ComSign.

9.2.1.3. Certified copies of the incorporation certificate, the corporation's founding documents, minutes of resolutions adopted by the appropriate bodies in the corporation regarding its appointment as a Registration Agent for ComSign, and minutes authorizing the person appointed by the corporation to act as a representative and undertake on its behalf in any matter regarding the appointment of the corporation as a Registration Agent for ComSign.

9.2.1.4. An attorney's statement on the corporation's field of activity, the identity of the corporation's representative who is authorized to make commitments on its behalf and confirmation that the decisions of the relevant corporate bodies regarding its appointment and functioning as a Registration Agent for ComSign are valid, bind the

corporation and were adopted in accordance with the corporation's incorporation documents and resolutions.

9.2.1.5. An undertaking to comply strictly with all provisions of the Law and its regulations.

9.2.1.6. A declaration by the applicant that it is able to fulfill the requirements of the procedures, and an undertaking by the applicant to comply literally with the instructions of this CPS.

9.2.1.7. Any other information required by ComSign, the CA Registrar or by the Law and its regulations

9.2.2 The representative who submits the application will take all required steps and will sign all documents required in order to receive the CA Registrar's approval for his/her appointment as a Registration Agent for ComSign.

9.3 The Address for Submitting an Application to Act as Registration Agent for ComSign

Applications to act as a Registration Agent for ComSign, containing all documents and information required by ComSign and by the Law and its regulations, approved and verified by an attorney (including additional information as required) will be submitted to the offices of ComSign Ltd. After they are approved by ComSign, ComSign will submit them to the CA Registrar for its final approval.

9.4 Responsibility for Actions of Registration Agents

ComSign is responsible for actions of Registration Agents acting on its behalf as determined by Law.

10. Additional Legal and Business Issues

Everything stated in this chapter is subject to the instructions of the Law and regulations.

10.1 Payments

ComSign will collect payment from certificate owners for the use of its services, but not for access to the CRL. In order to remove any doubt, it is hereby clarified that changes in the prices of ComSign's services will not be applied retroactively.

10.2 Financial Commitments

ComSign will post a bank guarantee or other guarantee or insurance, as required by sections 11(a)(3) and 15(b) of the Law and chapter 3 of the Electronic Signature Regulations (Certification Authorities), and as established by the registrar, in order to ensure compensation for any party that might suffer harm from an act or omission caused by ComSign not having met its obligations according to this CPS, as described in section 10.6.1.

10.3 Confidential Information

10.3.1 Definition of Confidential Information:

ComSign is hereby committed to treat the following information as confidential and not to divulge it to any third party unless otherwise stated below and subject to any law:

- Information included in an application for a certificate (other than information that is inserted into the certificate or the Repository and that Registrar has permitted its publication according to this CPS and according to law) and in subscription agreements. It is hereby clarified that the information contained in the database of valid and revoked certificates lists is confidential, except for the lists of valid and revoked certificates that include the serial number and validity period of each certificate.
- Records created or managed by ComSign, as specified in section 5.5 above.
- Information dealing with ComSign's data security system and included in the audit reports.
- Information included in the plans for handling unexpected events and disaster preparation plans.

10.3.2 Publication/Exposure of Confidential Information:

ComSign and/or its representative will nor publish any confidential information nor expose it to a third party unless:

- A verified request is submitted according to ComSign's requirements by the person to whom ComSign and/or its representative are bound to protect the said confidential information.
- Court order.

ComSign may charge the person requesting the confidential information a reasonable payment for the service prior to exposing the said information. As stated above, ComSign's Repository is registered as a database according to the Privacy Protection Law.

10.3.3 Publishing information related to the validity/revocation of certificates

ComSign's Repository will include a list of revoked certificates, that includes their serial numbers and the date of revocation, as well as information related to certificate revocation and additional information regarding the certificate's status (see chapter 2, above, dealing with ComSign's Repository).

10.4 Maintaining the privacy of information

ComSign's databases are registered at the Registrar of Databases and in accordance with the Protection of Privacy Law, 5741-1981. ComSign will act in accordance with and subject to this law and according to the instructions and requirements of the Registrar in these matter, as issued from time to time.

10.5 Property Rights

Unless agreed to the contrary, the property rights to the information and data in this document are considered the property of ComSign.

10.6 Representations and Obligations

10.6.1 Representations and obligations of ComSign:

Comsign declares that during its operation as a CA it will ensure that:

- The certificate does not contain any factual misrepresentations of which ComSign is aware;

- There are no copying mistakes in the data, as received by ComSign from the certificate applicant e, that result from ComSign not taking reasonable precautions when creating the certificate;
- The certificate complies with all material requirements of these procedures, the Law and its regulations;
- All information stated in the certificate or included in it by reference, other than the certificate owner's e-mail address, was verified by ComSign. After the certificate is issued, ComSign will not have an ongoing obligation to investigate and check the degree of accuracy and correctness of the information included in the application for issuing a certificate, unless ComSign receives explicit notification that one of the details appearing on the certificate is incorrect. In this case, the certificate will be revoked and it will be possible, at the request of the certificate owner, to issue a new certificate that contains the correct information.
- At the time the certificate was issued, ComSign complied with these procedures;
- ComSign's signature device was not impaired.

ComSign will not be held responsible for damage caused by relying on an electronic certificate that it issued, if it can prove that it took all reasonable precautions to fulfill its obligations according to the Law and this CPS. The responsibility of ComSign is, as noted, subject to the limitations listed later in this chapter.

Without detracting from the above, ComSign is committed to:

- Provide the infrastructure and the certificate issuing services, including the establishment, publication and operation of ComSign's Repository, in a trustworthy and accessible manner as required by law and detailed in these procedures;
- Provide the controls and foundation for ComSign's public key infrastructure (PKI), including protection of ComSign's keys, and to act according to the procedures for Confidentiality Partners, as presented in this CPS;
- Implement the procedures for verifying certificate applications, as presented in this CPS;
- Issue certificates according to chapter 4 of the procedures and to respect various representations made to certificate owners and relying parties in to these procedures;

- Publish a list of revoked certificates in ComSign's Repository, in a manner that is accessible, on-line and immediate for whomever wishes to rely on a particular electronic certificate, as described in chapter 2 above.
- Act according to the commitments of a CA and protect the rights of certificate owners and relying parties, according to chapter 4 of the procedures, the Law and its regulations.
- Revoke certificates as required by section 4.8 of the procedures.
- Handle certificates renewals as stated in chapter 4.7 of the procedures.

10.6.2 Representations and Obligations of ComSign's Registration Agents:

Everything stated in section 10.6.1, above, will also apply to the ComSign's Registration Agents, as far as it is relevant to their activities.

10.6.3 Representations and Obligations of the Certificate Owner:

Certificate owners are obligate to act in accordance with representations and obligations that appear in section 4.5.5, above, during the entire period of the certificate's validity.

10.7 Limitations on the Liability of ComSign and its Representatives

ComSign's liability is defined by law and limited according to section 21 of the Law and according to legislations. ComSign may limit its liability according to section 21(b) of the Law, including the types of certificate usage or transaction amounts for which the certificate may be used.

If the aforementioned limitations are listed on the electronic certificate, ComSign and its representatives will not be responsible for damage caused as a result of violating these limitations. Furthermore, ComSign may limit its liability toward a certificate owner in the subscription agreement, as long as this agreement does not contradict the provisions of the Law or this CPS.

Limitations on certificate usages will be executed only according the certificate owner's specific request. The form of the request will be formulated subject to the approval by the Registrar.

ComSign and/or its representatives –

- Do not guarantee that a certificate owner will not deny any certificate or message. (It should be noted that the Law does deal with the denial or non-denial of a signature.)

- Do not guarantee any software other than the technology and software that ComSign uses to issue the certificates and the device on which the signature device is stored, if supplied by ComSign.
- Are not responsible for any damages caused by relying on a revoked certificate whose details were published in the CRL, as required by the Law, prior to being relied upon, subject to providing proof that they took all reasonable measures to fulfill their obligations according to the Law and this CPS.

10.7.1 Exception of Liability for Certain Damages

ComSign and/or its representatives will not be liable for any indirect damages resulting from and/or related to any use, for any purpose, of certificates and/or electronic signatures. ComSign and/or its representatives may be held liable only for direct damages caused naturally and in the ordinary course of events from the non-execution of its obligations in accordance with the Law.

10.7.2 Limit on Financial Liability

Comsign may limit its overall, combined liability for use of an electronic signature, and this limitation will appear in a conspicuous manner on the certificate and the applicant will be informed of this limit before the certificate is issued. ComSign will publish its policy regarding limitations on its liability for different types of certificates in a conspicuous place on its Internet site.

In any event, the total liability of ComSign and/or its representatives toward any party (including, *inter alia*, a subscriber, applicant or relying party) will not exceed the relevant liability limit, as follows.

10.7.2.1. For anything relating to certificates issued to the applicants (1) who are required to use them to comply with signature requirements set by law or (2) according to the requirements of a State authority, the total responsibility of ComSign for a certificate will not exceed a sum of NIS 500,000 (five hundred thousand New Israeli Shekels).

10.7.2.2. The total combined liability of ComSign and/or its representatives toward any person for any other certificate will be limited to a sum that does not exceed NIS 50,000 (fifty thousand New Israeli Shekels) for all of the electronic signatures produced and all of the transactions related to a particular certificate, and not exceed NIS 10,000 (ten thousand New Israeli Shekels) for a single electronic signature produced and a single transactions related to that single signature.

The above limitation on damages and payment for damages applies to any type of loss and damage including direct damages, compensation, indirect damages, special and consequential damages, exemplary compensations or secondary damages caused to any person including the subscriber, applicant, recipient or a relying party and which are caused due to relying on or using a certificate that ComSign issues, manages, uses, suspends or revokes, or for relying upon or using an expired certificate. This limitation on damages or payment for damages also applies to contractual liability, tort liability and any liability claim. Subject to the aforementioned conditions, the liability limit for each certificate will be allocated first to the earlier claims in order to reach a final settlement of the conflict, unless an authorized court instructs otherwise. In no event shall ComSign be obliged to pay an amount exceeding the total maximum liability sum for each certificate, regardless of the method used to distribute maximum liability among several claimants.

10.8 Dangerous Activities

The electronic certificates are not intended for use in control equipment, in dangerous circumstances and/or uses that require fail-proof performance, such as operating nuclear facilities, aircraft navigation, communication systems, air traffic control systems and/or any situation in which failure might be a direct cause of death or bodily harm or environmental damage.

10.9 Force Majeure

ComSign and its representatives shall not be responsible for any breach, delay, or avoidance of performance in accordance with this CPS caused by events beyond its control such as force majeure, wars, periods of market emergency, epidemics, power outages beyond the control of ComSign, fires, earthquakes and other disasters for which ComSign was unable to reasonably prepare.

10.10 Validity of the CPS

10.10.1 Validity of the CPS

This CPS, and all changes and amendments thereto, will become valid and invalidate the previous version immediately upon its publications at http://www.comsign.co.il/cps.

This CPS may be amended by issuing a partial update. The fact of the partial update, as well as any correction to these procedures, will be published with the date that the Registrar gave his/her mandatory approval, in a manner that will make it possible to monitor the date on which a document became valid and when the previous document or

chapter became invalid. Amendments will be applicable from the date of publication after having been approved by the Registrar, however this does not add obligations towards anyone to whom a certificate was issued previously, on the basis of a previous CPS as long as the certificate remains valid. After an updated CPS is published, certificate owners are given a 60-day extension for filing objections, amendments or reservations – so that ComSign may consider them and submit them to the Registrar, if necessary. ComSign will send a written response to all comments received. There will be no response to comments received more than 60 days after the updated CPS is published.

10.10.2 End of validity

ComSign's procedures, as published from time to time, will remain in force until replaced by a new version of the procedures.

10.11 Notifications

If any party to these procedures wishes or is required to send a notification, request, or application regarding these procedures, the said message shall be sent using an electronically-signed message in a manner that conforms with the requirements of these procedures, or in writing. Electronic messages will be valid when the sender receives a valid return receipt, which must be received within five (5) days. Otherwise, a written notification must be sent to ComSign. Written messages to ComSign must be delivered using a courier service that provides a written delivery receipt, or by registered mail to the address of ComSign.

From ComSign or a Registration Agent to another person: To the most recent registered address. Each Registration Agent of Comsign must immediately notify ComSign of any legal notification received that might affect ComSign.

The above mentioned does not apply to certificate revocation notices, as described in section 4.8 above.

10.12 Settling Disputes

Prior to using any kind of mechanism for conflict resolution (including legal proceedings or arbitration) to deal with a dispute related to any aspect of these procedures or to a certificate issued by ComSign, the injured party must notify ComSign, the Registration Agent and any party to the dispute, so they can attempt to settle the dispute among themselves.

10.13 Applicable Law

These procedure have been formulated in accordance with the laws of the State of Israel without reference to other laws and/or rules regarding the choice of law, and without any requirement to establish a commercial connection to Israel. The choice of law was made to ensure uniform procedures and interpretation for all users, without reference to their place of residence or where their certificates are used.

ComSign declares that these CPS were formulated according to the ETSI TS 456 standard.

10.14 Subjection to Law

The procedures in this CPS are subject to the Law, its regulations and the instructions of the Registrar.

10.15 Conformity with WebTrust

NOTE: The procedures in this sub-section 10.15 are not regulated under the Electronic Signature Law and are not subject to approval by the Registrar. However, these procedures comply with WebTrust Principles and Criteria for Certification Authorities Version 2.0 (WTCA), Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.1.6 and Network and Certificate Systems Security Requirements, v.1.0 and were audited, validated and approved as such by ComSign and an external accredited auditor.

10.15.1 General Statement on Conformity.

The current and successive English versions of this document intends to meet or exceed the requirements of the Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates ("**Baseline Requirements**") and the Guidelines for Extended Validation Certificates ("**EV Guidelines**"), as published by the Certification Authority / Browser Forum ("**CAB Forum Guidelines**") at http://www.cabforum.org. If any inconsistency exists between this sections of this English version of this CPS dealing with the issue of SSL Certificates and the Baseline Requirements or EV Guidelines, the Baseline Requirements and EV Guidelines shall take precedence. In case multiple or alternative methods or options are possible by the baseline requirements or guidelines in order to perform a certain task and/or multiple or alternative methods or options are offered in order to comply to those requirements and guidelines, ComSign reserves the right to choose any

of the methods or options applicable at any times and may choose to change its procedures at all times and decide to do so on a case to case basis.

10.15.2 ComSign is obligate to develop, implement, enforce, and annually update a Certificate Policy and/or Certification Practice Statement that describe in detail how the CA implements the latest version of these Requirements.

10.15.3 Fees concerning SSL Certificate services

10.15.3.1. Certificate issuance or renewal fees

Fees are subject to change and are published on the ComSign web site. (www.comsign.co.il) or in subscriber agreements. Changes shall not take effect retroactively.

10.15.3.2. Certificate access fees

There are no certificate access fees.

10.15.3.3. Revocation or status information access fees

There are no revocation or status information access fees.

10.15.3.4. Fees for other services such as policy information

Fees are provided by ComSign on a regularly updated pricing list with no retroactive effect.

10.15.3.5. Refund policy

No refund is applicable to early termination, revocation and the like. Issue of a new certificate following revocation is subject to full payment.

10.15.4 Compliance audit and other assessments

10.15.4.1. Frequency or circumstances of assessment

ComSign undergoes periodic and non-periodic inspections and audits of its CA facilities to validate that it is operating in accordance with the security practices and procedures laid down in this CPS and in internal documents.

ComSign reserves the right to require periodic and non-periodic inspections and audits of any RA facilities to validate that the RA is operating in accordance with the security practices and procedures laid out in this CPS and in internal documents.

10.15.4.2. Identity/qualifications of assessor

The auditor shall be WebTrust accredited and shall have qualifications in accordance with best commercial practice and as mandated by law. The auditor must perform CA or Information System Security Audits as its main task, and must be thoroughly familiar with the ComSign's CPS.

10.15.4.3. Assessor's relationship to assessed entity

The auditor and ComSign shall have a contractual relationship for the performance of the audit, and be sufficiently organizationally separated from the ComSign to provide an unbiased, independent evaluation. The auditor shall be a certified public auditor if so required by WebTrust.

10.15.4.4. Topics covered by assessment

a) The audit only compares the practices laid down in this CPS with the onsite ComSign's implementation. All aspects of ComSign's operation as specified in this CPS shall be subject to an audit compliance inspection. b) The audit shall also consider the operations of ComSign's subcontractors. c) It is the Relying Party's and cross-certifying CA's own responsibility to judge whether the CPS meets the requirements in this CPS, or to trust the statement of compliance by ComSign.

10.15.4.5. Actions taken as a result of deficiency

Any discrepancies between a ComSign operation and a stipulation of its CPS must be noted and immediately notified to ComSign that will determine a remedy, including a time for completion.

Any remedy may include permanent or temporary CA cessation, but several factors must be considered in this decision, including the severity of the discrepancy and the risks it imposes and the disruption to the certificate using community. The action taken may allow ComSign to continue operations for thirty days pending correction of any problems prior to revocation, or indicate the irregularities, but allow ComSign to continue operations until the next audit without revocation. The decision regarding what actions to take will be based on previous response to problems, the severity of the irregularities, and the recommendations from the auditor. Depending on the situation, contractual agreements, applicable laws and regulations, ComSign may have to notify all its subscribers and indicate how it will proceed.

10.15.4.6. Communication of Results

a) Conclusive results of the audits shall be distributed to ComSign and the audited RA.

Conclusive result is hereby defined to be the information of all irregularities, which may affect a relying party's trust in a certificate, including an adequate judgment of its level of seriousness but excluding detailed information that can be used to attack the system.

b) A CA or RA found not to be in compliance with this CPS shall be notified immediately at the completion of the audit. Required remedies shall be defined and communicated to the CA or RA as soon as possible to limit the risks. The implementation of remedies shall be communicated to the ComSign management. A special audit may be required to confirm the implementation of the effectiveness of the remedy.

10.15.5 Processing Certificates' Suspension Requests

Any circumstance that may lead to the need for revocation and any circumstance in which a requester chooses to temporarily suspend the Certificate in order to prevent the use of the Certificate during a certain time, can be considered as a valid reason for suspension.

Example reasons for suspension: the device holding the private key has been misplaced but will probably be found again, the device holding the private key is broken, the certificate holder has a lengthy leave during which he or she will not make use of the certificate, a payment as agreed in the contract between ComSign and the subscriber is overdue.

The decision to suspend a Certificate can originate either with ComSign or with ComSign's authorized representatives.

Suspension requests of Certificates' are processed after adequate authentication and authorization of the requestor. The identification process is detailed in section 3.2.6.

A suspended Certificate can be un-suspended by the same parties that can request the suspension. Un-suspension requests are processed after adequate authentication and authorization of the requestor. The identification process is detailed in section 3.2.6. The request for un-suspension shall be recorded and archived. All relevant information about the certificate will stay archived for a period as specified in this CPS.

The suspension period is limited and may not exceed 2 business days following which the Certificate may either be un-suspended or revoked.

ComSign shall update the Certificate status upon revocation, suspension and un-suspension and publish it in the CRL within the time frame states in this CPS.

10.15.6 Notification upon Revocation or Suspension

ComSign must be notified as soon as possible of a revocation request if the request is based

on the invalidity of the certified data or the possible (future) compromise of the private key, and not later than after 12 hours if the notifying party is not subject to Force Majeure.

ComSign shall not be held responsible for unauthorized use of a certificate's private key during the revocation request grace period or afterwards.

Upon revocation or suspension of a Certificate by ComSign, the procedures set forth in this CPS and the applicable internal documents shall apply and the certificate holder and, if applicable, the legal representative of the organization (or his authorized delegate) will be notified of the revocation or suspension as per the procedures for notification outlined in this CPS.

10.15.7 Name Claim Disputes

In case of any name claim dispute, the claimant will contact ComSign's registration servicers who will investigate the grounds on which the name claim dispute is based. Any entity acting within the ComSign PKI Infrastructure is obliged to give appropriate and sufficient co-operation to an investigation mentioned in this section. In case the name claim dispute is due to an error of ComSign, ComSign will undertake immediate action, free of charge, to solve the problem. In case the name claim dispute is due to negligence or malicious actions of a certificate holder/subscriber or a Relying Party, ComSign reserves the right to terminate the contractual relationship immediately, to revoke the certificate and to refuse to continue any collaboration with that person or organization. ComSign further reserves the right to undertake legal actions and collect costs and expenses.

10.15.8 Certificate Profile

10.15.8.1. ComSign uses the standard X.509 version 3 to construct electronic Certificates for use within the ComSign PKI Infrastructure. X.509 allows ComSign to add certain certificate extensions to the basic Certificate structure. ComSign uses a number of certificate extensions for the purposes intended by X.509 version 3 as per Amendment 1 to ISO/IEC 9594-8, 1995.

10.15.8.2. ComSign's key pair has the key usage "Signing Certificates and CRL's" enabled in the corresponding certificate and is only used for the purpose of generating certificates and CRL's, as defined in section 7.3.3 of ETSI TS 101 456, within physically secure premises.

The X.509v3 certificates issued by ComSign contain the key usage certificate extension, restricting the purpose to which the certificate can be applied, in compliance with the procedures under which the certificate is issued.

The certificate extensions used correspond the definitions in RFC 5280.

10.15.8.3. In addition to the CRL structure, as detailed in section 7.4 of this document, ComSign may use the following CRL Entry Extensions, as defined in RFC 5280:

10.15.8.3.1. Reason Code (OID = 2.5.29.21):

Unspecified	(0),
keyCompromise	(1),
cACompromise	(2),
affiliationChanged	(3),
superseded	(4),
cessationOfOperation	(5),
certificateHold	(6),
removeFromCRL	(8),
privilegeWithdrawn	(9),
aACompromise	(10)

10.15.9 Life cycle security controls

The controls are such that the security meets the required level defined by ComSign's internal procedures that were made available to the WebTrust auditor and approved by the Registrar. In particular, for certificate generation, ComSign shall ensure that:

10.15.9.1. Certificate and revocation status information signing cryptographic hardware is not tampered with during shipment; AND

10.15.9.2. Certificate and revocation status information signing cryptographic hardware is not tampered with while stored; AND

10.15.9.3. The installation, activation, backup and recovery of ComSign's signing keys in cryptographic hardware shall require dual control of at least two trusted roles; AND

10.15.9.4. Certificate and revocation status information signing cryptographic hardware is functioning correctly; AND

10.15.9.5. The SSCD preparation shall be securely controlled by the service provider; AND

10.15.9.6. The SSCD shall be securely stored and distributed whenever the storage or distribution could possibly lead to key compromise or misuse of the SSCD; AND

10.15.9.7. SSCD deactivation and reactivation shall be securely controlled; AND

10.15.9.8. Where the SSCD has associated user activation data (e.g. PIN code), the activation data shall be securely prepared and distributed separately from the secure signature-creation device. This may be achieved by ensuring distribution of activation data and delivery of SSCD via a different route and medium.

10.15.10 Miscellaneous

10.15.10.1. ComSign applies a data backup procedure that operates a rotated daily backup of its CA related data storing it either on-site or off-site according to an established backup rotation schedule.

10.15.10.2. Events and audit logs are produced on ongoing basis and reviewed constantly. System reports are produced on a daily basis and reviewed daily by ComSign's management. Records are produced on hardware and software.

11. Miscellaneous

11.1 Completeness of these Procedures

This text of the CPS replaces all other, previous texts and any other text, whether written or oral, has no validity, either explicit or implied, unless otherwise stated in these procedures as amended from time to time.

11.2 Assignment of Rights and Obligations

ComSign may assign its rights and/or obligations as described in these procedures to any other party, subject to the prior written approval of the Registrar.

11.3 Waivers

No waiver, discount, delay, extension or avoidance of on-time action by ComSign and/or a certificate owner shall be interpreted as a waiver on their part of any rights as described in this CPS, and shall not be used as an argument or injunction against a claim on their part.

11.4 Titles and Appendixes of these Procedures

The titles and subtitles appearing in these procedures are presented only for the sake of convenience and reference, and may not be used for direct or indirect interpretation, or for enforcing the instructions of these procedures. The appendixes, including the definitions of these procedures, are an integral and binding part of these procedures for all purposes.

11.5 Interpretation

Unless determined otherwise, these procedures will be interpreted in a manner consistent with the provisions of the Law and its regulations, and reasonable commercial behavior in the given circumstances. When interpreting these procedures, it is necessary to consider their international extent and application, the benefits inherent in encouraging uniformity of their implementation and maintaining good faith.

11.6 Contradictory Instructions

In the event of any contradiction between these procedures and the Law, regulations and instructions of the Registrar – the Law, regulations and instructions of the Registrar shall prevail. In the event of any contradiction between the provisions of the subscriber agreement and provisions of this CPS, the provisions of this CPS will prevail. In the event of any contradiction between the provisions of the updated CPS, and a previous version of the CPS, the updated version will prevail.

11.7 Publication

These procedures are published:

- In an electronic version form in ComSign's Repository, at http://www.comsign.co.il./cps.
- In an electronic version via e-mail upon submitting an appropriate request to ComSign's e-mail address.
- In a printed form, which can be received, upon submitting a written request from ComSign [customer services], at its mailing address.
- Comsign will place, at its expense, notice of any update to this CPS in two daily newspapers.

Additional information may be found in ComSign's web site at http://www.Comsign.co.il. Furthermore, the customer service department may also be contacted at this e-mail address: info@comsign.co.il.

11.8 Comments and Suggestions

We would be pleased to receive comments and suggestions from our users about future amendments to the procedures. Please send your comments to ComSign by e-mail or mail to the company's address.