Comda Ltd

Certification Practice Statement

Version 1.0

Publication Date: 12.03.2026

Comda Ltd

Kiryat Atidim #4 Tel Aviv

Comda company address:

Mailing Address: P.O. Box 58077, Kiryat Atidim, Tel Aviv 6158001, Israel.
Company Office Address: Kiryat Atidim, Building No. 4, Tel Aviv 6158001, Israel.
Tel: +972-3-6485255, Fax: +972-3-6474206, Email address: info@comda.co.il.

Version Management

Version Number	Change date	Changes
1.0	03.11.2023	New document
1.0	01.05.2024	General revision
1.0	12.03.2026	General revision + translation

1. Introduction

Comda Ltd. issues secure digital certificates.
Comda issues an electronic certificate which constitutes an electronic confirmation that a specific signature verification means belongs to a specific person, following identification of the applicant for the electronic certificate either face-to-face or remotely using designated means at a reasonable level of assurance.

This document regulates the manner in which Comda provides services for the issuance of secure electronic certificates and the manner in which such certificates are used, including identification and authentication, issuance, revocation and renewal of certificates, physical security controls, logical security controls and the certificate profile and certificate revocation lists (CRL).

The engagement between the applicant and Comda requires signing a subscriber agreement.

This document was prepared in accordance with RFC 3647. Comda declares that it also incorporates requirements according to ETSI standards and the latest version of the CA/Browser Forum Baseline Requirements. The procedures specified in this document are binding on Comda, its representatives, certificate holders and relying parties.

1.1 Overview

Comda's secure electronic certificate issuance services are intended to support secure electronic commerce and other electronic services in order to meet the technical, business and personal needs of users of electronic signature technologies.

Comda acts as a trusted third party that issues, manages and revokes secure electronic certificates in accordance with these procedures.

Certificate issuance services include registration, identification of the applicant, issuance, revocation and documentation of the activities performed by Comda. Revocation of certificates shall be carried out in the circumstances specified in Section 4.9.1 of this document.

This document applies to secure electronic certificates as defined under the Electronic Signature Law.

1.2 Document Name and Identification

This document is referred to as the "Certification Practice Statement", "CPS of Comda Ltd." or simply "CPS". It may be reviewed on the company website repository.

(www.comda.co.il/repository). Document Object Identifier (OID): 1.3.6.1.4.1.56578.4.1

1.3 PKI Participants

1.3.1 Certification Authority (CA):

Comda Ltd. operates as the Certification Authority and its procedures are based on international standards.

1.3.2 Registration Authority (RA):

Certificate issuance services may include Registration Authorities authorized by Comda to process certificate applications, identify applicants and register them according to these procedures. Registration Authorities operate under the hierarchical supervision of the Certification Authority and are required to comply with these procedures.

1.3.3 Subscriber:

See definition in Section 1.6 below.

1.3.4 Relying Party:

See definition in Section 1.6 below.

1.3.5. Other Participating Entities:

Comda Registration and Verification Clerks: Representatives of Comda whose responsibility is to receive certificate applicants, fill in the details of the certificate applicants, verify and authenticate the identity of the certificate applicants, perform the certificate issuance process in practice, and after issuance verify that it operates properly. Afterwards, collection of the payment and issuance of an invoice and receipt. In cases of certificate revocation – to verify the identity of the revoking party and to perform the revocation in practice.

Applicant's Representative: The person submitting the application when it concerns issuance of a certificate to an individual, or the authorized representative of the individual, or an authorized representative (authorized signatory) of the corporation or public institution when an application is submitted for issuance of a secure certificate to an authorized person on behalf of a corporation or on behalf of a public institution or an electronic signature authorized signatory. The identity of the authorized representative must be verified in accordance with these procedures.

1.4 Certificate Usage

1.4.1. Permitted Uses of the Certificate:

A secure electronic certificate issued in accordance with this CPS, the law and the regulations is a secure electronic certificate as defined in the law.

The secure electronic certificate may be issued as a certificate to an individual or as a certificate to an authorized person on behalf of a corporation or a public institution. The use of the certificate is carried out under the responsibility of the certificate holder and is intended for lawful uses only.

1.4.2. Restrictions on the Use of the Certificate:

Restrictions on the use of a secure electronic certificate may be determined by Comda and in accordance with an explicit request of the certificate holder. Such restrictions will appear in the certificate in the **Certificate Policies** field. To the extent that the certificate does not include restrictions on permitted use, any lawful use may be made of the certificate.

Only the certificate holders are responsible for the use made by them or on their behalf of certificates issued under these procedures, in any jurisdiction in which the contents of the certificate may be used or viewed. Accordingly, applicants and certificate holders should be aware of the existence of various laws regarding data transfer, and in particular data encryption, and that these laws may differ significantly from country to country. In addition, in most cases it is not possible to limit the distribution of content on the Internet or on certain other networks based on the location of the user/viewer. This may require applicants and certificate holders to comply with the laws of any jurisdiction in which the content of the certificates may be viewed or used.

1.5. Policy and Procedures

1.5.1. The Responsible Party for Implementing the Policy and Procedures:

The body responsible within Comda for the implementation of this CPS is the Security Forum.

1.5.2. Contact Person:

The person responsible for implementing the policy and procedures in Comda is the CEO.
Email: security@comda.co.il
Mailing address: Comda Ltd., Kiryat Atidim, Building 4, 11th Floor, P.O. Box 58007, Tel Aviv 61580
Tel: 03-6485255, Fax: 03-6491092.

Information regarding secure electronic signatures and training may be obtained from Comda after contacting the email: support@comda.co.il. Additional assistance may be obtained from Comda customer service representatives at Tel: 03-6485255, Fax: 03-6491092.

1.5.3. The Officer Responsible for Ensuring the Procedures Conform to the Certification Authority Policy:

The CEO of the Certification Authority is the officer responsible for ensuring that the procedures conform to the Certification Authority policy.

1.5.4. Approval of the Procedures:

These procedures were approved by the appropriate forum at the Certification Authority.

1.6 Definitions and Terms

The terms listed below shall have in these procedures the meaning below:

Signature Creation Device
Software, object or unique information required for the creation of a secure electronic signature. A signature creation device is used to produce an electronic signature. The signature creation device is unique to its owner, is kept secret by its owner, and is also known as a "private key" in the public key encryption method.

Signature Verification Device
Software, object or unique information required in order to identify that a secure electronic signature was produced by a specific signature creation device. The signature verification device has a one-to-one relationship with the signature creation device and is also known as a "public key" in the public key encryption method. A specific signature verification device serves as a means to identify that a secure electronic signature was produced using a specific signature creation device. The signature verification device may be made available to the public for the purpose of this verification.

Certificate Holder
An applicant to whom a secure electronic certificate has been issued.

Registration
The process within the framework of which an applicant (as defined below) submits a request for the issuance of an electronic certificate.

The Law
The Electronic Signature Law, 5761–2001.

Device or Hardware Device
A smart card, token, HSM or any other hardware component used for the creation and storage of the signature creation device.

Electronic Signature
A secure electronic signature as defined in the Law (as defined above).

Comda Repository
A database of Comda containing information available to the general public including, among other things, the CPS and lists of revoked certificates as published on the Comda

website.
The Comda repository also includes additional information which is not available to the general public, for example the database of valid certificates.

Applicant
A person or a corporation or a public institution submitting a request for the issuance of a secure electronic certificate as detailed in Chapter 4 below.

Relying Party
A third party receiving a message signed with an electronic signature and acting or refraining from acting on the basis of the electronic signature and/or on the basis of the information contained in the Comda repository.

Keys (Private, Public) or Key Pair
A private key and the public key uniquely associated with it according to accepted encryption methods, as required by the Law within the framework of the public key encryption method.

The Procedures or These Procedures
The procedures detailed below regulating the activity of Comda as a Certification Authority. These procedures apply only to secure certificates.

Comda Representative
An external entity to Comda appointed by Comda as a Registration Authority for the purpose of performing operations of applicant registration, identification of applicants and handling requests for the issuance of an electronic certificate.

Parties
Comda, its representatives and the users of the certificates, namely the certificate holder and the relying party.

Certificates or Electronic Certificates
Secure electronic certificates issued by Comda.

Revoked Electronic Certificate
An electronic certificate appearing in the Certificate Revocation List (CRL) in the Comda repository.

Valid Electronic Certificate
An electronic certificate appearing in the list of valid certificates in the Comda repository as a valid certificate. This repository is not open for public inspection.

Electronic Signature Regulations (Hardware and Software Systems)
Electronic Signature Regulations (Secure Electronic Signature, Hardware and Software Systems and Examination of Applications), 5762–2001.

2. Publication and Repository

The purpose of this chapter is to review the ways in which Comda publishes relevant information to the general public, to relying parties, to electronic certificate holders and to applicants, as applicable. The chapter includes reference to the types of information published, the frequency of publication and the manner of access to Comda's information repository.

2.1. Comda Repository

For the purpose of its operations, Comda manages a collection of databases intended for the storage and retrieval of electronic certificates and other information related to them, which shall hereinafter be collectively referred to as the repository. The Comda repository includes, among other things, the following sub-databases: a database of valid electronic certificates (including Comda's certificate), databases of revoked electronic certificates, information regarding the revocation of electronic certificates and lists of revoked electronic certificates, and other information as shall be determined by Comda from time to time.

Only part of the information published in the Comda repository is open for inspection by the general public. Open for controlled inspection is the list of revoked electronic certificates specifying the serial number and the date of revocation of the certificate.

The databases of Comda are registered with the Registrar of Databases in accordance with the Protection of Privacy Law, 5741–1981, and Comda shall act in accordance with and subject to this law.

2.2. Publication of Information Relating to Electronic Certificates through the Comda Repository

Within the framework of the Comda repository, Comda shall publish a list of revoked electronic certificates, updates to the procedures and other information in a manner consistent with these procedures.

The said information shall be published on the website, and with respect to updates to the CPS it shall include the effective date.

2.3. Frequency and Time of Publication in the Repository

Comda shall publish a new list of revoked certificates every two hours and no later than every 12 hours, or immediately after the revocation of a certificate, whichever occurs first. The validity of the list of revoked electronic certificates that has been published is for 24 hours.

The updated and valid list of revoked electronic certificates is the list appearing in the Comda repository. A relying party must perform a new online check in the database of revoked electronic certificates at any time at which it seeks to rely on an electronic

certificate in order to ensure that its examination is performed against the most up-to-date list of revoked electronic certificates.

2.4. Access Control to the Repository

It is possible to access freely the areas of the repository open to the public from the Comda website. The access address to the repository of revoked electronic certificates of Comda is: https://www.comda.co.il/repository.

Access to other parts of the repository is blocked except for role holders who have been authorized for this purpose in accordance with Comda procedures.

3. Identification and Authentication

The purpose of this chapter is to review the requirement of physical presence / remote identification of a certificate applicant at the time of the first issuance, the process of identification and authentication of the certificate applicant, the documents that must be presented, verification of the application, cases in which the application will be rejected, as well as procedures for identifying a certificate holder for the purpose of certificate revocation or re-issuance.

Original documents used for identification that are not in the Hebrew or English language shall be presented together with a notarized translation into the Hebrew or English language.

3.1. Naming

3.1.1. Types of Names:

The name of the certificate holder is stated in the certificate in accordance with the provisions of the X.509 standard. Several different electronic certificates may be issued under the same name to the same applicant, in his different roles. For example: Mr. Reuven Ploni will receive one certificate as a lawyer, a second as a supplier of the Ministry of Defense and a third as a reporter to the Merkava system of the Ministry of Finance.

3.1.2. The Name of the Certificate Holder Must Be Meaningful:

The name of the certificate holder must be meaningful in the sense that it can be attributed to a person or to a corporation or public institution in a manner that prevents an error in identification or attribution of the certificate to its holder.

3.1.3. Use of a Pseudonym or Omission of a Name:

Comda shall not issue an electronic certificate bearing a pseudonym of the certificate holder and which does not state the name of the certificate holder (an anonymous certificate). However, Comda may add, upon the explicit written request of the certificate holder, his pseudonym, in parentheses and adjacent to his first name appearing in the identification documents, while stating that it is a pseudonym.

3.1.4. Instructions for Interpreting Different Types of Names:

In order to ensure that the information included in the certificate is unique to the certificate holder, including the use of Distinguished Names (DN) and represents unique values that can be verified in accordance with international standards, Comda uses the X.500 standard and its various derivatives.

3.1.5. Uniqueness of the Certificate Holder's Name:

The certificate enables the unique identification of the certificate holder by means of a unique identity identifier. In the case of an individual, the identity card number that he holds. In the case of a corporation, the registration number of the corporation. In certain

situations, an additional identification identifier may be used in addition to the identity card number, such as a professional license number, an authorized dealer number and the like.

3.1.6. Provision of Information for Identification, Authentication and Trademarks:

Applicants and certificate holders undertake toward Comda and/or its representatives that the information and details provided by them in the application for the issuance of an electronic certificate are correct, accurate, do not infringe or violate the rights of any third parties, in any jurisdiction, with respect to their trademarks, service marks, trade names or any other intellectual property right, and that they do not seek to use any detail appearing in the application for the issuance of an electronic certificate for any unlawful purpose whatsoever, including, among other things, causing breach of contract or other unlawful interference in contractual relations, unfair competition, injury to the reputation of another and misleading a person, corporation or any other legal entity.

Comda and its representatives shall not be responsible for the accuracy and correctness of the data provided to Comda, to a Comda representative, or to the Comda repository or otherwise provided by the applicant or the certificate holder for the purpose of their inclusion in the certificate, or for the fact that their inclusion or their provision itself violates any provision of law or the right of any third party.

Email addresses provided by the applicant for the purpose of their inclusion in the certificate are not examined by Comda, neither with regard to their validity, nor with regard to their association with the applicant, nor for any other purpose, and reliance upon them or use of them is at the responsibility of the relying party.

3.2. Initial Verification and Identification of the Applicant

3.2.1. Proof of Possession of a Private Key:

An electronic certificate shall not be issued to a person who does not possess a private key that meets the following requirements:

(a) The private key is based on an accepted standard making use of one of the following:
(1) an RSA or DSA key of at least 2,048 bits;
(2) an elliptic curve DSA key of at least 160 bits;

(b) Activation of the private key, or access to it, requires the use of unique physical or cryptographic means that meet a security level of at least FIPS 140-2 Level 2 or the Common Criteria standard at a security level of at least Common Criteria EAL2;

(c) If activation of the private key involves the use of a password, the password shall meet high-level security requirements according to Israeli Standard 1495 Part 3.

Proof of possession of the private key is performed on the basis that the generation of the key pair by the applicant is carried out at the time of certificate issuance by Comda on the

device in which the signature creation device is stored for which Comda will issue an electronic certificate. If the storage device was not supplied by Comda, Comda will issue an electronic certificate to the owner of the signature creation device subject to the submission of a written declaration by the applicant for the electronic certificate signed by his hand stating that the signature creation device and the storage device meet the requirements specified above.

3.2.2. Verification of the Identity of a Corporation:

Identification of an applicant/authorized person on behalf of a corporation as detailed in this subsection shall be carried out by two registration clerks on behalf of Comda, by way of identification of the authorized person face to face or remote identification using designated means at a reasonable level of assurance, as detailed below:

• **Corporation registered in Israel:** according to the certificate of registration, confirmation of a lawyer regarding the existence of the corporation, its name and its registered number, or instead of such confirmation of a lawyer – according to verification in the appropriate registries, and also according to a certified copy of the decision of the competent organ of the corporation regarding the authorized signatory on behalf of the corporation, or confirmation of a lawyer regarding such authorized signatory in a format that will be published on the Comda website from time to time.

• **Corporation not registered in Israel:** according to a certified copy of a document attesting to its registration, confirmation of a lawyer regarding the existence of the corporation, its name and its registered number, or instead of such confirmation of a lawyer – according to verification in the appropriate registries, and also according to a certified copy of the decision of the competent organ of the corporation regarding the authorized signatory on behalf of the corporation or confirmation of a lawyer regarding such authorized signatory in a format that will be published on the Comda website from time to time.

• **Palestinian corporation registered with the Palestinian Authority:** shall be identified like any corporation not registered in Israel and in addition the authorized signatory on its behalf shall be identified in accordance with the provisions of Section 3.2.3 below regarding an individual who is a resident of the Palestinian Authority.

• **Public institution:** according to the declaration of the applicant through the authorized signatory who has been identified as an individual resident of Israel and in addition through the following documents:
(1) an identification document issued to him by the state bearing his photograph and identity number;
(2) a written declaration by the state employee that he is an authorized signatory on behalf of the public institution;
(3) a document confirming that the state employee is an authorized signatory on behalf of the public institution;

For the purpose of this paragraph, **"public institution"** – government ministries, local authorities, as well as authorities, corporations or other institutions established in Israel according to law.

With regard to corporations (whether registered or not registered in Israel) and public institutions – the Certification Authority shall identify the authorized signatory as an individual resident of Israel or a foreign resident, as applicable, as detailed in Section 3.2.3 below.

With regard to a corporation not registered in Israel or a public institution – where a **"certified copy"** is required – the intention is a copy conforming to the original authenticated by one of the following:
• the authority that issued the original document;
• a lawyer licensed to practice law in Israel;
• an Israeli diplomatic or consular representative abroad.

3.2.3. Verification of the Identity of an Individual Applicant:

Identification of an individual applicant as detailed in this subsection shall be carried out by a registration clerk on behalf of Comda, by way of face-to-face identification and/or remote identification through a designated system, as detailed below:

Individual who is a resident of Israel: according to an identity card (including the appendix) together with one of the following documents (two different documents bearing a photograph are required in order to perform the identification process):

(1) a valid Israeli passport; or
(2) a valid Israeli driver's license with a photograph; or
(3) a travel document as defined in the Passports Law, 1952; or
(4) an identification document issued by the state to a state employee or to a person employed by it or performing a role on its behalf or performing a role according to law for the purpose of performing his work or role, provided that the document bears a photograph of the applicant and his identity number. For the purpose of this matter, **"state employee"** – including a soldier, police officer, prison guard, and any office holder or person holding a position according to legislation in an institution of the institutions of the state; or
(5) another identification document issued by a public authority according to law, provided that the document bears a photograph of the applicant and his identity number; or

another type of identification document, provided that the document bears a photograph of the applicant and his identity number;

or –

with regard to a person who does not possess an identification document according to subparagraphs (1)-(5) – an affidavit regarding the absence of the documents appearing in subparagraphs (1)-(5) above and in addition confirmation by a lawyer regarding the

identity of the applicant and that he knows the applicant personally, together with a photograph of the applicant signed by the lawyer, according to a format accepted by Comda.

In addition, in cases in which Comda seeks to increase the level of assurance in remote identification, Comda reserves the right to perform verification of identification documents according to information received from the Population Registry at the Ministry of the Interior (hereinafter: **"the Population Registry"**) including the following details: the identity number of the applicant, his family name and previous family name if any, first name, father's name, mother's name, year of birth, date of last issuance of an identity document, reason for issuance of the identity document, current address, and if present – death status and date of death.

Individual who is a foreign resident: according to a foreign passport or travel document or identity card, together with an additional identification document bearing the photograph of the applicant and identifying details of the applicant and of the issuer of the additional document (two different documents bearing a photograph are required in order to perform the identification process).

Individual who is a foreign resident for the purpose of reporting and identification vis-à-vis the "Sha'ar Olamy" system: according to the procedure for identification of a foreign resident individual and in addition according to an **"entity number"** issued to him by the Tax Authority and comparison with information received prior to issuance from the Tax Authority in accordance with an internal working procedure. The identification number of the foreign resident individual that will appear in the electronic certificate shall be the **"entity number."**

Individual who is a resident of the Palestinian Authority: for the purpose of issuing an electronic certificate to a resident of the Palestinian Authority who does not hold an Israeli identity card, Comda shall identify the applicant according to **"individual who is a foreign resident"** except in issuance for the purposes of **"Sha'ar Olamy"**, in which case identification shall be performed according to a Palestinian identity card or foreign passport and also by means of a **KHR card** issued by the Civil Administration in Judea and Samaria bearing the photograph of the applicant and identifying details of the applicant.

Identification of an authorized signatory on behalf of an individual: according to the request of an individual applicant authorizing the authorized signatory to act in his name and on his behalf and confirmation of a lawyer regarding such authorized signatory in a format that will be published on the Comda website from time to time. The Certification Authority shall identify the authorized signatory as an individual resident of Israel or a foreign resident as applicable, as detailed in the section above.

3.2.4. Applicant Whose Details Were Not Verified:

Comda shall not issue an electronic certificate to an applicant whose identity and/or the identity of the certificate holder cannot be verified or has not been verified by it.

3.2.5. Verification of Authorization:

Comda shall not issue an electronic certificate to an authorized person on behalf of a corporation without verifying with the corporation that the applicant has been authorized by the corporation (or by the individual as applicable) to act in its name and that the authorized person has been duly authorized by the corporation to act and sign on behalf of the corporation. The date of the confirmation may not be more than 3 months prior to the date of issuance of the electronic certificate, unless approved by the manager of the Certification Authority or a person authorized by him for this purpose.

3.2.6. Criteria for Reliance on Electronic Certificates from External Organizations:

Comda performs and manages issuances only within the framework of the Comda issuance system and does not rely on issuances performed by any external organization.

3.3. Identification and Authentication of Requests for Renewal of an Electronic Certificate

3.3.1. Identification and Authentication in the Case of Renewal of an Electronic Certificate without Generation of a New Signature Creation Device at the Request of the Applicant Before the Expiration of His Certificate:

Comda shall offer a service of remote renewal of an electronic certificate issued by it to a certificate holder before its expiration, either on its own initiative or upon the telephone request of the certificate holder. A telephone renewal request by the certificate holder must be made within a time range of between one (1) day and sixty (60) days before the certificate expiration date. A proactive telephone contact by Comda to the certificate holder may be made up to 24 hours before the expiration date.

The renewal is conditional upon identification of the electronic certificate holder by means of an identification question, verification of the identification details registered with Comda and verification of the details of the electronic certificate through authentication to the device on which the certificate is installed. In the event that the remote renewal process fails or does not operate for any reason until the expiration date of the certificate being replaced, a new issuance shall be performed according to the full and regular registration procedure, including identification of the applicant as performed with respect to every first issuance of an electronic certificate.

3.3.2. Identification and Authentication for the Purpose of Renewal after Revocation of the Electronic Certificate:

An electronic certificate cannot be renewed after it has been revoked and it is necessary to perform a new issuance under a full identification procedure.

3.4. Identification Verification of a Request for Revocation of an Electronic Certificate:

Comda shall revoke an electronic certificate upon the request of a certificate holder immediately after receipt of the request and after it verifies that the person requesting the revocation is indeed the certificate holder or his authorized representative. The certificate revocation action shall be performed by at least two clerks. Identification of the certificate holder / the authorized representative requesting the revocation of his electronic certificate shall be performed in one of the following ways:

• By means of the identification code determined by the certificate holder / the authorized representative himself at the time of submission of the request for issuance of the electronic certificate. A Comda representative shall verify the authenticity of the identification code by entering the code into the relevant system and receiving an indication of "correct" / "incorrect".

• If the certificate holder / the authorized representative did not determine an identification code or does not remember it, a Comda representative and/or someone on its behalf shall call the telephone number that the certificate holder / the authorized representative specified in the application for issuance of the certificate in order to verify that the certificate holder / the authorized representative is indeed the person requesting its revocation, and shall verify the details of the person requesting revocation of the certificate according to the personal details that he entered when requesting the certificate, including answers to identification questions provided by the certificate holder / the authorized representative at the time of issuance.

• Comda shall revoke a certificate issued to an authorized signatory in a corporation or in a public institution or to a member in an organization or in another institutional body or to an authorized person on behalf of an individual, upon the request of the corporation, the public institution, the organization or the institutional body or the individual in whose name he was authorized to act. The revocation request shall be submitted by a person authorized for that purpose by the corporation or the public institution, the organization or the institutional body and/or by the individual in the case of an authorized person on behalf of an individual and/or according to the arrangement established in the subscription agreement and in the application forms for issuance of a certificate. It is clarified that with respect to a public institution as defined in Section 3.2.2 above, Comda shall revoke the certificate issued to an authorized person on behalf of the public institution only after it has identified the person requesting the revocation (who is not the authorized person) as an individual resident of Israel and in addition through the following documents:

(1) an identification document issued to him by the state which bears his photograph and identity card number;
(2) a declaration of the state employee that he is an authorized signatory on behalf of the public institution;
(3) a document confirming that the state employee is an authorized signatory on behalf of the public institution.

4. Certificate Life-Cycle Operational Requirements

The purpose of this chapter is to detail the process of issuing the electronic certificate, from the stage of submission of the application and the required documents, through the logical issuance process and ending with the issuance of the certificate. In addition, the chapter includes an explanation of the procedure for renewal and revocation of the certificate, including who is authorized to submit requests for revocation and renewal. This chapter also details the obligations imposed on the holder of an electronic certificate.

The electronic certificate issuance process shall be carried out by at least two clerks of the Certification Authority.

4.1. Application for Issuance of an Electronic Certificate

4.1.1. Who May Submit an Application for an Electronic Certificate:

An individual or a corporation (including a public institution), whether a resident of Israel or a foreign resident, by himself or through an applicant authorized by him for this purpose, and subject to the submission of the required documents and approvals and compliance with the requirements and provisions of this CPS.

4.1.2. The Application Submission Process and the Obligations Imposed Within It:

Comda publishes on its website the forms that must be submitted as part of the application for an electronic certificate. The applicant may, by prior coordination, complete and send these forms to the offices of Comda prior to the actual issuance process. Comda may, but is not obligated to, send the applicant an invitation or reminder for the appointment scheduled for issuance, in the manner and by the means that Comda finds appropriate to use in a proportionate manner [telephone notification, SMS message, and email message].

Offers for the purchase of a service or product shall be sent by means of email messages, SMS messages, or telephone messages.

The applicant is obligated to provide Comda with complete, correct and full information required by it for the purpose of initiating the issuance process. Corporations, individuals and public institutions may submit an application through an authorized signatory.

For issuance to an individual resident of Israel, the applicant shall provide the following information and documents:

1. An identity card and one of the following identification documents, provided that they are valid:

(1) an Israeli passport;
(2) an Israeli driver's license bearing the photograph of the applicant;
(3) an identification document issued by the state to a state employee, to a person

performing a role or holding an office on its behalf or in an institution of the institutions of the state, or to a person performing a role according to law, for the purpose of performing his work or role as stated, provided that the document bears the photograph of the applicant and his identity number; for the purpose of this matter, **"state employee"** – including a soldier, police officer and prison guard.

A person who does not possess an identification document according to subparagraphs (1) to (3) and has submitted an affidavit to that effect, one of the following:

(1) a travel document, as defined in the Passports Law, 1952, bearing the photograph of the applicant;
(2) another type of identification document provided that the document bears the photograph of the applicant and his identity number;
(3) confirmation by a lawyer regarding the identity of the applicant and that he knows the applicant personally and that he is aware that his confirmation is intended to support the application for issuance of an electronic certificate, together with the photograph of the applicant signed by the lawyer, according to a format acceptable to Comda.

2. An applicant wishing that the electronic certificate issued to him will bear his **maiden name** instead of the current family name appearing on the identity card must notify Comda in advance and bring to the issuance appointment also a document **"Population Registry Extract"** from the Population and Immigration Authority.

3. Address: street, city, state, postal code, country (residence).

4. Telephone numbers (of the place of residence).

5. Email address (as provided by the applicant – not verified).

6. Signed subscription agreement.

7. Other information as determined by the Certification Authority.

For issuance to an individual resident abroad, the applicant shall provide the following information and documents:

1. A valid passport with a photograph.

2. An official document bearing a photograph.

3. With respect to a Palestinian trader for the purpose of identification vis-à-vis the **"Sha'ar Olamy"** system – by a Palestinian identity card or foreign passport and in addition also a **KHR card**.

4. With respect to a foreign resident (including a Palestinian trader) for the purpose of reporting and identification vis-à-vis the **"Sha'ar Olamy"** system also the **"entity number"** issued to him by the Tax Authority.

5. Address: street, city, state, postal code, country (residence).
6. Telephone numbers (of the place of residence).
7. Email address (as provided by the applicant – not verified).
8. Signed subscription agreement.
9. Other information as determined by the Certification Authority.

For issuance to an authorized person of a corporation, the applicant shall provide the following information and documents:

1. Certificate of registration of the corporation.
2. Confirmation by a lawyer regarding the existence of the corporation (including its name and number) (the certificate of registration is not sufficient since the corporation may have been dissolved in the meantime).
3. A certified copy of the decision of the competent organ of the corporation regarding the applicant being an authorized signatory on behalf of the corporation or confirmation by a lawyer regarding such authorized signatory.
4. All the information and documents required for issuance to an individual for the purpose of verifying the identity of the authorized person.

For issuance to an authorized person of a public institution

(government ministries, local authorities, as well as authorities, corporations or other institutions established according to legislation):

1. An official document containing the details of the withholding tax file of the institution.
2. An official document approved by a senior office holder in the institution authorizing him to act on behalf of the institution.
3. A declaration by a state employee that he is an authorized signatory on behalf of the public institution in a format acceptable to Comda.
4. All the information and documents required for issuance to an individual for the purpose of verifying the identity of the authorized person.

For issuance to an authorized person of a corporation or public institution not registered in Israel:

1. A certified copy of the certificate of registration of the corporation.

2. Confirmation by a lawyer regarding the existence of the corporation (including its name and number) and a certified copy of the decision of the competent organ of the corporation regarding the applicant being an authorized signatory on behalf of the corporation or confirmation by a lawyer regarding such authorized signatory.

3. All the information and documents required for issuance to an individual for the purpose of verifying the identity of the authorized person.

For issuance to an authorized person of a Palestinian corporation registered with the Palestinian Authority:

Identification shall be performed as for any corporation not registered in Israel and in addition the identity of the authorized signatory on its behalf who is a resident of the Palestinian Authority shall be verified as stated above regarding an individual who is a resident of the Palestinian Authority.

4.2. Processing the Application for Issuance of an Electronic Certificate

4.2.1. Performance of Identification and Verification Actions:

The identification shall be carried out by an identification clerk. The identification clerk shall identify the applicant and have him sign the application form and the subscription agreement, and shall present to the applicant an information and warning form regarding the risk involved in the use of an electronic signature and the obligations imposed on him, and shall have him sign a declaration that he has been warned as stated above.

4.2.2. Approval or Rejection of the Application:

Once the identification process has been completed, all documents have been examined and found to be complete, valid and signed, and the technological requirements for issuance have been met, the application shall be transferred to Comda's issuance computer. If any of the above requirements have not been met, the process shall be stopped until the missing or incorrect item has been completed or corrected. If the installation process is stopped – an explanation shall be given to the applicant at the time of the stoppage. Comda may refuse to issue a certificate to any applicant for reasonable reasons, such as suspicion of incorrect identity, non-compliance of the signature creation device with the Hardware and Software Regulations, non-payment for the service and the like, without bearing any liability or responsibility for losses or expenses arising from such refusal. Upon Comda's refusal to issue a certificate, Comda shall return to the certificate applicant without delay the registration fee paid by him, if such fee was paid, for the certificate.

Comda maintains a registry of all applications for issuance of electronic certificates that were examined and rejected by it, as well as certificates that were revoked in circumstances originating from suspicion regarding the correctness of details provided by the certificate applicant. The registry is internal and is used only by Comda as part of the process of examining applications.

4.2.3. Timelines for Processing the Application:

Information and documents provided as part of the process of examining and processing the application shall be examined shortly after they are delivered to Comda. An application submitted to Comda by the applicant personally, together with the required documents, during Comda's working hours, shall be examined in the presence of the applicant.

An application that has been examined and found to be valid shall be transferred for certificate issuance without any delay, provided that this is possible during Comda's working hours.

4.3. Issuance of an Electronic Certificate

4.3.1. Actions of the Certification Authority at the Time of Issuance:

In order to ensure identification of the applicant for the electronic certificate and to verify the connection between the applicant and his public key (signature verification device), individuals and/or authorized signatories of corporations submitting an application to receive an electronic certificate in a first issuance must undergo remote identification by biometric means used by Comda or appear personally before Comda and/or one of its representatives.

The issuance shall be performed in the presence of the applicant by the identification clerk.

The identification clerk shall offer the applicant a device for the creation and storage of the signature creation device and the electronic certificate that has been examined and approved by Comda. If the applicant wishes to use a device that was not supplied to him by Comda, Comda shall examine whether the applicant possesses a means for producing a secure electronic signature and that the signature creation device and the signature verification device identifying the said signature creation device comply with the provisions of Regulation 8 of the Electronic Signature Regulations (Hardware and Software Systems). For the purpose of the examination the applicant shall be required to present to Comda the following details and documentation:

- Name of the manufacturer.
- Product/model name.
- A copy of the approval granted to the device by the following bodies: NIST and/or Common Criteria.

For the purpose of compliance with the provisions of Regulations 8(1)(b) and (c) of the Electronic Signature Regulations (Hardware and Software Systems), Comda may suffice with a declaration from the applicant that he has provided Comda with correct details to the best of his knowledge regarding the signature creation device, the manner of its activation and access to it. Comda is not responsible for verifying the correctness of the declaration and Comda shall not be responsible for additional examinations of the signature creation device or for its ongoing use, subject to the manner of generation of the private key as regulated in Section 4.5.1 below.

The details of the certificate holder shall be entered into the system, and the applicant shall generate the signature creation device (the private key) and the signature verification device (the public key) by means of a password known only to him. In the case of issuance of a signature creation device on a network device, the password shall be entered at the stage of initialization of the partition on the server on which the signature creation device will be stored. In this case, the applicant shall enter his password for the purpose of generating the signature creation device (the private key) and the signature verification device (the public key) directly on the hardware device without the possibility of exposing the password and the signature creation device to a Comda employee. In the case of issuance of a signature creation device on a network device stored at a third party, the password shall be entered at the stage of initialization of the partition on the server on which the signature creation device will be stored. In this case, the applicant shall enter his password for the purpose of generating the signature creation device (the private key) and the signature verification device (the public key) directly on the hardware device without the possibility of exposing the password and the signature creation device to a Comda employee.

The identification clerk shall verify the validity of the keys and the certificate and their presence on the hardware device (with the assistance of the certificate holder) and shall offer the certificate holder to check its validity (signing a document, etc.).

At the time of issuance, the certificate holder shall determine an identification code that will be used by him, among other things, for revocation of the certificate if necessary. This code shall be entered by the identification clerk into a system that does not allow recovery of the password but only provides an indication of "correct" or "incorrect" upon entering the identification code, see Section 3.4 above, as well as a code for remote certificate renewal, see Section 3.3.1 above. The identification clerk shall detail to the certificate holder the certificate revocation procedure.

The identification clerk shall deliver the device to the certificate holder and shall explain to him the obligation to keep it under his control. The identification clerk shall explain to the certificate holder the importance of safeguarding the device as well as the importance of safeguarding the password and/or the component used for access to the device in secure and protected locations.

4.3.2. Notification to the Certificate Holder of the Issuance:

The issuance of the certificate shall be carried out in the presence of the applicant, either physically or remotely, and delivery of the certificate to the certificate holder or his authorized representative shall be performed at the time of completion of the issuance.

4.4. Acceptance of the Electronic Certificate

4.4.1. Conduct Considered as Acceptance:

Delivery of the electronic certificate by Comda to the certificate holder shall be considered acceptance whether the certificate holder confirmed its receipt or not, provided that the

delivery was documented in Comda's records. Use of the certificate by the certificate holder shall also be considered acceptance.

4.4.2. Publication of the Electronic Certificate by the Certification Authority:

Upon issuance of the electronic certificate, Comda shall record the details of the certificate in the list of valid electronic certificates in the Comda repository and in additional repositories. Access to the repository of valid certificates is restricted in accordance with Comda's internal work procedures. Holders of electronic certificates may publish their certificates in additional repositories.

4.4.3. Notification to Other Entities by the Certification Authority Regarding the Issuance:

Comda may, but is not obligated to, notify certain third parties of the issuance of an electronic certificate.

4.5. The Key Pair and Use of the Electronic Certificate

4.5.1. The Private Key of the Electronic Certificate Holder and the Use of the Certificate:

The key pair created by the applicant must comply with the requirements of Regulation 8 of the Electronic Signature Regulations (Hardware and Software Systems) as detailed below: "The electronic signature is produced using a key based on an accepted standard making use of one of the following: (1) an RSA or DSA key of at least 1024 bits; (2) an Elliptic Curve DSA key of at least 160 bits."

Comda issues to its customers RSA keys of 2048 bits or ECC keys of at least 160 bits. The device that creates and stores the signature creation device may be supplied by Comda or may be supplied by the applicant. Comda shall not issue an electronic certificate to a signature verification device that does not meet the requirements as regulated in Section 4.3.1 above.

Comda shall ensure that the keys are generated during the issuance process and that it will not be possible for the applicant to arrive at the issuance process with a signature creation device that was generated in any preliminary process. This is intended to prevent the possibility of introducing keys belonging to another identity into the device. During the verification process the applicant's signature creation device shall not be exposed to Comda.

At the time of receipt of the electronic certificate the certificate holder must verify that the details specified in it are correct according to the information provided by him as set forth in Section 4.1.2 above. If an error is discovered in the details of the certificate, the certificate holder must, according to the subscription agreement, notify Comda immediately upon discovery of the error and request the revocation of the electronic certificate. In the event of a discrepancy in the information provided by the applicant prior to issuance (whether in the application form for issuance of the certificate and/or in the personal details form and/or in

the subscription agreement), Comda shall revoke the electronic certificate and issue a new electronic certificate to the certificate holder without additional payment. In any other case the electronic certificate shall be revoked and the certificate holder shall be charged the full payment for issuance of the new certificate. It is clarified that revocation of an electronic certificate not resulting from a fault for which Comda is responsible shall not entitle the certificate holder to any refund, whether full or partial.

It is the sole responsibility of the certificate holder, throughout the entire validity period of the certificate, to take all reasonable measures to safeguard his signature creation device and to prevent its use without his authorization; to notify Comda immediately upon becoming aware of any compromise of his control over the signature creation device; and to use the electronic certificate in a manner consistent with these procedures and with the law.

The authorized person and/or the certificate holder are hereby warned that failure to safeguard the signature creation device of the electronic certificate holder may enable use of the secure electronic signature of the certificate holder for the purpose of obligating the certificate holder, conducting transactions, creating representations in the name of the certificate holder, and performing any other action that may be carried out using the secure electronic signature in a manner that may cause significant damage to the certificate holder and/or to those relying on the certificate. Hence the great importance of safeguarding the signature creation device and protecting it as detailed in these procedures.

4.5.2. The Public Key and Its Use and the Use of the Electronic Certificate by a Relying Party:

A relying party must verify the validity of the electronic certificate issued by Comda if it wishes to ensure that:
(a) the electronic signature was created by the signer whose name appears in the electronic certificate;
(b) the electronic message that was signed has not been altered since the creation of the electronic signature; and
(c) the use of the certificate does not fall within the restrictions on permitted uses of the certificate, if such restrictions exist.

Verification of the signature creation device (the private key) with which the electronic certificate holder signs with his secure electronic signature is performed using the public key (signature verification device). The examination is carried out against the Certificate Revocation List (CRL) published to the public by Comda and whose link appears within the electronic certificate.

Comda publishes on its website at **www.comda.co.il** the list of its signature verification devices used for issuing secure electronic certificates as well as the lists of revoked secure electronic certificates related to these signature devices.

A relying party that has not verified the validity of the certificate risks relying on an electronic certificate that is not valid and may bear responsibility for damages caused as a result of failure to verify the validity of the electronic certificate. Comda shall not be responsible for any damages caused due to reliance on a revoked electronic certificate.

The electronic certificate holder and Comda may restrict the permitted uses of the electronic certificate. Restrictions on the use of the certificate at the request of the certificate holder shall be made only upon the explicit request of the certificate holder. These restrictions are stated in the electronic certificate or incorporated into it by reference and enable warning certificate holders and relying parties regarding the permitted uses of electronic certificates and the restrictions, if any, on the scope of such uses. Comda shall not be responsible for damage caused due to uses exceeding such restrictions. Parties relying on Comda electronic certificates must examine the content of the certificate and search for such warnings and restrictions.

An electronic certificate issued for a corporation or a public institution or to an authorized person on behalf of an individual confirms that the person recorded therein is an authorized signatory on behalf of that corporation or public institution or the individual in whose name he is authorized to act, however it does not constitute proof of such authorization or of the authority of the authorized signatory to perform a specific action on behalf of the corporation or the public institution or the individual. Parties relying on messages signed with an electronic signature are solely responsible for performing due diligence and exercising reasonable judgment as required with respect to regular handwritten signatures before relying on the content of such messages.

4.6. Renewal of a Certificate

4.6.1. Circumstances for Renewal of an Electronic Certificate:

A condition for renewal of a certificate is that the certificate being renewed is valid at the time of renewal. A certificate that has expired cannot be renewed, and in such case issuance of a new electronic certificate will be required. Comda may, but is not obligated to, notify the holder of the electronic certificate, in a proportionate manner and by means it deems appropriate, including by telephone notice, SMS message and email message, of the expected expiration date of the electronic certificate in his possession and of the need to renew it. The said notice is intended solely for the convenience of the certificate holder in the certificate renewal process, and the sending or non-sending of such notice to the electronic certificate holder shall not obligate Comda and/or impose upon it any liability and/or responsibility of any kind arising from and/or related to the expiration of the certificate and/or its non-renewal. Offers to purchase a service or product shall be sent by means of email messages, SMS messages or telephone messages only if approved by the certificate holder at the time of issuance or at a later time.

4.6.2. Who May Request Renewal of an Electronic Certificate:

Renewal may be carried out at the request of the electronic certificate holder or according

to an order of a competent authority or upon the demand of Comda. The responsibility to renew the certificate rests solely on the certificate holder.

4.6.3. Handling of Renewal Requests:

Renewal of the electronic certificate during the validity period of the certificate being renewed may be carried out as regulated in Section 3.3.1 above. In such case the key pair of the certificate holder shall remain the same also during the period of extension of the validity of the renewed electronic certificate.

In a case where the above renewal process is not available and/or the electronic certificate of the certificate holder has been revoked or has expired or the certificate holder did not set a password or does not remember it, a new registration shall be performed according to the full and regular registration procedure, including identification of the applicant as performed with respect to any first issuance of a certificate.

Comda reserves the right to amend and update the certificate renewal procedures. Updated renewal procedures are presented (upon their publication) by means of a revised version of the procedures at the Internet address:
http://www.comda.co.il/repository/

4.6.4. Notification to the Electronic Certificate Holder Regarding the Renewal:

Notification regarding the renewal shall be provided to the electronic certificate holder at the time of the renewal and as part of the renewal procedure. In circumstances in which a renewal is not performed but rather a new issuance, the provisions of Section 4.3.2 above shall apply.

4.6.5. Conduct Considered as Acceptance of a Renewed Electronic Certificate:

Use of a renewed electronic certificate by the certificate holder shall be considered as his approval of its delivery into his possession subject to the terms of issuance, renewal and use.

4.6.6. Publication of the Renewed Electronic Certificate by the Certification Authority:

Renewal of the validity of the electronic certificate is updated by Comda, at the time of renewal, in the list of valid electronic certificates in the Comda repository and in additional repositories, in accordance with the law and the regulations. Access to the repository of valid electronic certificates is restricted in accordance with Comda's internal working procedures. Holders of electronic certificates may publish their certificates in additional repositories.

4.6.7. Notification of Renewal by the Certification Authority to Other Entities:

Certificates renewed within the framework of projects that require notification to the project operators, whether by virtue of a legal requirement or by virtue of a contractual engagement under which the renewed electronic certificate was issued, shall be published

by Comda to the registries managed and under the control and supervision of the project operators. In circumstances in which a renewal is not performed but rather a new issuance, the provisions of Section 4.4.3 above shall apply.

4.7. Replacement of the Key Pair for an Electronic Certificate (re-key)

This CPS does not permit replacement of the key pair of a valid electronic certificate. In any case in which replacement of the key pair is required, for example as a result of a change in standard, requirements to increase security, or suspicion of compromise or loss of control of the private key, whether at the initiative of the Certification Authority or at the request of the certificate holder, a new electronic certificate shall be issued and a new key pair shall be generated within the issuance process.

4.7.1. Circumstances for Replacement of the Key Pair of an Electronic Certificate:

Not relevant – see above.

4.7.2. Who May Request Replacement of the Key Pair of an Electronic Certificate:

Not relevant – see above.

4.7.3. Handling of Requests for Replacement of the Key Pair:

Not relevant – see above.

4.7.4. Notification to the Certificate Holder Regarding Replacement of the Key Pair:

Not relevant – see above.

4.7.5. Conduct Considered as Acceptance of an Electronic Certificate Whose Key Pair Was Replaced:

Not relevant – see above.

4.7.6. Publication by the Certification Authority of a Certificate Whose Key Pair Was Replaced:

Not relevant – see above.

4.7.7. Notification by the Certification Authority to Other Entities Regarding Replacement of the Keys:

Not relevant – see above.

4.8. Making Changes to an Electronic Certificate

This CPS does not permit making a change or correction to a valid electronic certificate. In any case in which correction or modification of the certificate or the text appearing in it is required, for any reason whatsoever, whether at the initiative of the Certification Authority or at the request of the certificate holder, a new electronic certificate shall be issued and a new key pair shall be generated within the issuance process.

4.8.1. Circumstances for Changing an Electronic Certificate:

Not relevant – see above.

4.8.2. Who May Request a Change to an Electronic Certificate:

Not relevant – see above.

4.8.3. Handling of Requests to Change an Electronic Certificate:

Not relevant – see above.

4.8.4. Notification to the Certificate Holder Regarding the Change to the Electronic Certificate:

Not relevant – see above.

4.8.5. Conduct Considered as Acceptance of an Electronic Certificate That Was Changed:

Not relevant – see above.

4.8.6. Publication by the Certification Authority of the Electronic Certificate That Was Changed:

Not relevant – see above.

4.8.7. Notification by the Certification Authority to Other Entities Regarding the Change to the Electronic Certificate:

Not relevant – see above.

4.9. Revocation and Suspension of an Electronic Certificate

4.9.1. Circumstances for Revocation of an Electronic Certificate:

An electronic certificate, including an **Intermediate Certificate**, shall be revoked:

- upon a verified request of the certificate holder or of his authorized representative.
- if Comda has been informed by the certificate holder, or becomes aware by other means, that an event of theft, loss, modification, unauthorized use, non-compliance with standards with respect to the signature creation device and the signature verification device, defect or other compromise of the signature creation device or of the certificate holder's control over the signature creation device has occurred, provided that Comda is satisfied as to the reliability of the notification.
- immediately when Comda becomes aware that a detail identifying the certificate holder

appearing in the certificate is incorrect, or that the reliability of the certificate has been compromised in another manner, provided that Comda is satisfied as to the reliability of the notification.

• immediately when Comda becomes aware of a defect in its secure electronic signature, or in its signature creation device, or in its hardware and software systems, or in the information security of these systems in a manner that may impair the reliability of its signature or the reliability of the electronic certificates it issues.

• immediately when Comda becomes aware that a certificate for an authorized person was issued without valid authorization, that the certificate holder has died (if it concerns a person), or that an order for liquidation has been issued (if it concerns a corporation), provided that Comda is satisfied as to the reliability of the notification.

• if Comda's activity as the Certification Authority has ceased without its activity being transferred to another Certification Authority, or if this is required of Comda in order to comply with the requirements appearing in these procedures.

• if a material defect is discovered in the certificate issuance process, whether the source of the defect is Comda, the applicant or any other entity involved in the issuance process.

4.9.2. Who May Request Revocation of an Electronic Certificate:

A request for revocation of a certificate shall be submitted by the certificate holder or an authorized person or another third party that has been expressly authorized to do so in the subscription agreement or by virtue of a legal provision. Where the certificate concerns a corporation and/or an authorized signatory on behalf of a corporation or a public institution or an authorized person of an individual / authorized dealer, Comda shall revoke an electronic certificate upon the request of the corporation, the public institution, the organization or the institutional body, the entity for whom the certificate was issued for the authorized person, or the authorized person himself. The revocation request shall be submitted by a person authorized for that purpose by the entity entitled to revoke the certificate and/or in accordance with the arrangement established in the subscription agreement and in the application forms for issuance of a certificate.

A request may also come from a Registration Authority to Comda requesting revocation of an electronic certificate issued by that Registration Authority, provided that the existence of this possibility and the grounds for revocation by the Registration Authority were brought to the attention of the certificate holder prior to issuance and were included in the subscription agreement of the certificate holder.

Comda itself shall initiate revocation of an electronic certificate immediately upon becoming aware that a circumstance listed in Section 4.9.1 above has occurred, and upon such occurrence Comda must revoke the electronic certificate.

4.9.3. Handling of Requests for Revocation of an Electronic Certificate:

A request for revocation of an electronic certificate shall be submitted by the person authorized to submit it either by telephone, by email or in writing. The revocation request shall be handled by an identification clerk at Comda. The identification clerk at Comda shall

verify the identity of the person requesting the revocation in accordance with the provisions of Section 3.4 above. If the verification succeeds – the certificate shall be revoked by a registration officer at Comda. In any other case – the certificate shall be suspended until final clarification of the matter subject to Comda's internal working procedures. The revocation action that is performed shall not be under the control of a single person only.

4.9.4. Granting an Extension to the Electronic Certificate Holder Prior to Revocation:

An electronic certificate for which circumstances requiring its revocation have occurred shall be revoked immediately without granting any extension of any kind.

4.9.5. The Time Available to the Certification Authority for Revocation of the Electronic Certificate:

An electronic certificate that must be revoked shall be revoked immediately.

4.9.6. Obligation of a Relying Party to Check the List of Revoked Electronic Certificates:

It is the duty of a relying party to verify the validity / correctness of an electronic certificate prior to relying on it. Comda makes available to certificate holders, relying parties and third parties the Comda repository which includes, among other things, lists of certificates including Comda's signature verification devices and lists of revoked electronic certificates of subscribers that may be accessed through the Internet address: https://www.comda.co.il/repository.

A link to the list of revoked electronic certificates may also be found within the electronic certificate itself. See Section 7.1.8 below as well as the Comda website.

The verification must always be performed against the most up-to-date published list of revoked electronic certificates (**CRL**).

4.9.7. Frequency of Publication of the List of Revoked Electronic Certificates:

Except for special arrangements arising from contractual engagements or legal requirements, Comda shall publish every two hours, and at least once every 12 hours, a list of revoked electronic certificates (CRL) valid for 24 hours. If a certificate is revoked by Comda, the list shall be updated shortly after the revocation is performed.

4.9.8. Maximum Retrieval Time of the List of Revoked Electronic Certificates:

The list of revoked electronic certificates (CRL) is available with maximum availability at all times. Comda ensures that retrieval times are minimal to the smallest possible extent without detracting from the said maximum availability.

4.9.9. Online Checking of the Status of Electronic Certificate Validation (OCSP):

Comda provides its customers holding electronic certificates with a service that allows

verification of the status of the electronic certificate using an online protocol for checking certificate validation status (Online Certificate Status Protocol – OCSP).

The results of the verification comply with the requirements of **RFC6960** and/or **RFC5019** and are signed by Comda.

4.9.10. Requirements for Online Revocation Checking:

The existence of a dedicated data communication line or access through the Internet. Details of the requirements and their specifications are determined within the framework of the separate engagement between Comda and the subscriber.

(1) Comda supports the OCSP service using the **GET** method for issued certificates.
(2) For the status of electronic certificates of a subscriber, Comda updates the information available through OCSP at least once every **4 days**. The validity of the response of this service shall never exceed **10 days**.
(3) For the status of **Intermediate Certificates**, Comda updates the information available through OCSP at least:
a. every **12 months**
b. within **24 hours** from revocation of an Intermediate Certificate
(4) When the OCSP server receives a request to check the status of an electronic certificate that was not issued, the response given shall be **"unknown"**.

4.9.11. Other Forms of Publication of Revoked Electronic Certificates:

The list of revoked electronic certificates is available online and immediately for examination by a relying party. Any other form of publication, such as **"pushing" the CRL to a subscriber to the service**, shall be permitted according to legal provisions. Comda may charge a fee for this service. Notification of a change of status does not constitute a substitute for the obligation to check the repositories of revoked electronic certificates unless this is determined by law or by agreement.

4.9.12. Special Requirements for Revocation Resulting from Loss of Control of the Key Pair:

Loss of control by the electronic certificate holder over the signature creation device (the private key) requires immediate reporting to Comda and a request for revocation of the electronic certificate. Comda shall revoke the electronic certificate immediately shortly after receiving the notification as regulated above in the regular revocation procedure corresponding to the circumstances of the revocation, provided that Comda is satisfied as to the reliability of the notification.

4.9.13. Circumstances Allowing Suspension of the Electronic Certificate:

Any circumstance under which an electronic certificate must be revoked (see Section 4.9.1 above) shall be considered a circumstance under which the validity of the electronic certificate may be suspended. The discretion of the Certification Authority as to whether to suspend the certificate or revoke it shall depend on additional circumstances and on the

request of the certificate holder or the person authorized by him to request its suspension or revocation within the framework of the subscription agreement. For example, disappearance of the signature creation device in circumstances in which the electronic certificate holder believes that it may be located through a reasonable search may constitute reasonable grounds for suspension of the certificate.

4.9.14. Who May Request Suspension of the Electronic Certificate:

The entity authorized to request suspension of the electronic certificate is the certificate holder or a person authorized by him in the subscription agreement to request revocation or suspension of the certificate.

4.9.15. Handling of a Suspension Request:

The manner of handling a request for suspension of an electronic certificate shall be as regulated in Section 4.9.3 above concerning the manner of handling a request for revocation of a certificate.

4.9.16. Limitation of the Duration of the Suspension Period:

Suspension of the electronic certificate shall not exceed a period of **48 hours**, at the end of which the suspension shall be removed or the certificate shall be revoked. The duration of the suspension period shall be determined according to the circumstances and taking into account the request of the person requesting the suspension. During the suspension period of the electronic certificate the certificate shall be entered into the **Certificate Revocation List (CRL)**.

4.10. Electronic Certificate Status Verification Services for a Relying Party

4.10.1. Operational Characteristics:

Verification of the certificate status shall be performed by the relying party against the Certificate Revocation List (**CRL**) on the Comda website.

4.10.2. Service Availability:

The electronic certificate status verification service shall be available **24 hours a day, 7 days a week**. If the availability of the services is impaired for any reason, the Certification Authority shall act to restore the service as soon as possible. See also **Section 5.7**, which addresses recovery from a disaster situation.

4.10.3. Additional Characteristics – Unlocking:

Hardware devices include security mechanisms according to which access for activation of the signature creation device is protected by a password. The hardware device shall be locked after a number of failed attempts to enter the password. Comda shall allow holders of electronic certificates to receive a service for unlocking the card without Comda being given access to the signature creation device. This shall be performed through a dedicated mechanism.

4.11. Expiration of an Electronic Certificate:

All electronic certificates shall enter into force on the date and time of their issuance by Comda. The electronic certificate shall be valid for the period appearing in the subscription agreement and on the certificate, unless the certificate is revoked or renewed before then.

4.12. Escrow and Recovery of the Private Key

This CPS does not allow escrow of the private key or its recovery.

4.12.1. Policy and Procedures for Escrow of the Private Key and Its Recovery:

Not relevant – see above.

4.12.2. Characteristics of a Session Key and Recovery Policies and Procedures:

Not relevant – see above.

5. Physical, Procedural and Personnel Controls

The purpose of this chapter is to review for the applicant, the electronic certificate holder and the relying party the physical control measures, personnel security and protection of records used by Comda in the course of its operations. In addition, this chapter provides a description of the records maintained by Comda and the types of information stored in them.

Comda implements a security system based on computer hardware, software and security procedures. All these provide a high level of availability, reliability and continuous operation as well as an adequate response against security risks.

Comda complies with stringent security standards and undergoes inspections by the Israeli Standards Institute for the purpose of obtaining quality certifications. Comda complies with **Israeli Standard 27001**, which deals with information security, and undergoes annual audits by the Israeli Standards Institute and by an independent security audit expert.

Comda's internal work procedures include, among other things, security policy, asset protection, personnel security, physical security, operations management, management of access to Comda's signing infrastructure, maintenance and continuity of operations in the event of a disaster.

5.1. Physical Controls

5.1.1. Site Structure and Location:

Facilities related to the issuance of electronic certificates and the management of revocations operate in an environment that physically protects the services against damage through unauthorized access to systems or data. Comda maintains the parts of the system essential to its operation in a protected and secured site that prevents intrusion and entry without authorization, according to the nature of Comda's activity. Physical protection is achieved through the establishment of clearly defined perimeter security barriers (i.e., physical barriers) surrounding the certificate issuance services, device preparation and revocation management. Physical protection provides protection against natural disasters, fire hazards and water damage, damage to supporting infrastructures such as electricity and communications, structural collapse, theft, burglary and unauthorized intrusion.

5.1.2. Physical Access:

Any person entering the secured site area shall not remain without supervision by an authorized person. Comda implements controls to protect against unauthorized removal of equipment, information, media and software related to Comda's services. Comda maintains an inventory of information assets and assigns classification levels for the protection requirements of those assets, in accordance with the risk management analysis it performs. The Security Manager maintains an inventory list of critical assets and the means for their protection. These assets may be physical assets and/or logical information assets.

5.1.3. Electricity and Air Conditioning:

The electricity supply and air conditioning system includes means and controls for monitoring deviations and malfunctions, and alternative supply in cases of malfunction or interruption of the electrical current to the secured site.

5.1.4. Exposure to Water Damage:

The secured site is disconnected from the water supply network and protective measures have been taken against flooding and water damage to facilities and equipment.

5.1.5. Protection from Fire Damage and Fire Prevention:

Fire detection, monitoring and extinguishing systems are installed at the site.

5.1.6. Protection of Data Storage Media:

All data storage media are located within the secured site and are subject to physical protections and access control. Backup systems are stored separately and are also protected by the measures taken to protect the primary storage media.

5.1.7. Prevention of Information Loss During Waste Disposal:

Comda implements dedicated procedures regulating shredding or physical destruction of documents or storage media containing confidential or restricted information.

5.1.8. Off-site Backup:

Comda implements a full backup policy and maintains a disaster recovery system located in physical and geographical separation from the company's secured operational site. See Section 5.7 below.

5.2. Administrative Controls

5.2.1. Trusted Roles:

All employees, contractors and consultants of Comda and/or its representatives who have access to, or control over, registration, issuance, use and revocation operations of certificates on behalf of Comda, including access to restricted functions of the Comda repository, shall be considered as holding positions requiring special trust (hereinafter: **"Trusted Roles"**).

Such personnel include, among others, customer service staff, system administration personnel, dedicated engineering staff and management personnel responsible for supervising the trusted system infrastructure of Comda.

The trusted roles and the permissions of each trusted role holder are detailed in Comda's internal procedures. Trusted role holders are appointed by the CEO of Comda with the approval of the Security Manager. Trusted role holders are obligated to maintain confidentiality and avoid conflicts of interest in the performance of their duties.

Trusted role holders operate under an individual employment contract that includes a detailed description of the role and its responsibilities, as well as the employee's commitment that they understand the responsibilities and agree to operate according to the procedures and the employment agreement.

Comda ensures that no conflict of interest exists among personnel serving in trusted roles and that there is no overlap in identity between personnel performing these roles. The roles defined by Comda as trusted roles include:

- CEO of Comda
- Security Manager responsible for implementing security procedures
- Identification Officer
- Key Managers and Key Custodians
- Safe Key Custodian
- Registration Officer
- Log Auditor

Each role has physical and logical access restrictions derived from Comda's internal procedures. These restrictions are confidential. A trusted role holder may not serve in more than one of the following roles: **Issuing Authority Manager, Security Manager, Registration Officer, System Operator or Auditor** (see Section 5.2.4).

5.2.2. Number of Personnel Required for Certain Tasks:

All activities defined as critical at Comda are performed by a minimum of **two different individuals**. Comda maintains personnel redundancy in order to comply with its procedures. No role depends on a single individual and each employee has an alternate at the same level.

5.2.3. Identification and Authentication for Each Role:

Comda operates an access control and user management policy using biometric systems and advanced physical identification devices that allow monitoring and control of both the identity of individuals entering secured areas and their access to secured system components. These systems also maintain records regarding entry times, access times, and the areas and system components accessed.

5.2.4. Roles Requiring Separation of Duties:

Comda's security policy prohibits assigning multiple trusted authorities to the same individual. For example, the Security Manager cannot simultaneously serve as an Identification Officer.

Certain tasks—such as the **generation of Comda's key pair**—require the involvement of multiple role holders, each performing a portion of the process without which the action cannot be completed.

Comda enforces separation of duties in accordance with its procedures, which were presented to the **Israeli Standards Institute** and approved under **ISO 27001 and ISO 9001 certifications**. These procedures define employee authorization levels and physical access permissions to various areas within Comda.

The security policy ensures that:

- Critical operations require participation of **at least two individuals**.
- Each role holder has access only to specific areas of the Comda facility.
- Access to highly sensitive areas is restricted to senior personnel.
- No single individual has exclusive access to all areas.

5.3. Personnel Controls

5.3.1. Qualifications, Experience and Training Requirements:

Comda employs personnel with the knowledge, experience, expertise and skills required for their roles and for the services they provide.

Before hiring employees, Comda conducts several checks including:

- Personal interviews
- Integrity assessments
- Reference checks
- Verification of professional qualifications (certifications, education, work experience)

The CEO of Comda provides final approval for the appointment of any candidate to a trusted role.

5.3.2. Procedures for Background Checks and Verification:

Comda and its representatives conduct preliminary screening of all personnel employed in its services. More extensive and thorough checks are conducted for personnel designated for trusted roles according to Comda's personnel procedures.

Comda also conducts **periodic investigations** of personnel in trusted roles to verify their reliability and professional competence. Employees and representatives are not granted access to sensitive areas or trusted roles until all necessary investigations have been completed.

Any individual who fails the initial or periodic investigation will not be employed by Comda.

Comda also implements operational controls including:

- Organizational controls
- Human resources controls
- Controls over external parties
- Additional management controls

These controls include requirements regarding employee training, role definitions, documentation requirements and scheduled audits.

The **Security Manager** conducts operational audits to ensure work is performed according to procedures. Employees found not complying with procedures may be subject to disciplinary action, including termination of employment.

5.3.3. Training Requirements:

Comda conducts employee training sessions that include knowledge refreshment, procedures review, role definitions and lessons learned from security incidents or other operational events. The annual training program is updated during the last month of each calendar year.

5.3.4. Frequency of Training:

Training frequency is determined within the annual program and includes **quarterly training cycles**. Training frequency may increase in cases of procedural changes or adoption of new technologies.

5.3.5. Job Rotation:

Comda does not operate a policy requiring mandatory job rotation for its employees.

5.3.6. Disciplinary Procedures:

Comda maintains strict reporting and investigation procedures in the event of malfunctions or complaints. Findings indicating violation of work procedures by employees or independent contractors are handled through disciplinary measures, up to termination of employment or contract.

5.3.7. Requirements for Independent Contractors:

When Comda engages subcontractors to perform tasks that grant them access to or control over certificate registration, issuance, use or revocation operations—including access to restricted repository functions—the subcontractor must contractually commit to maintaining the strict security requirements imposed on Comda under this CPS.

The subcontractor must also indemnify Comda for any damage resulting from information security breaches.

5.3.8. Documentation Provided to Issuing Authority Staff:

Staff of the issuing authority receive full access—according to their role definitions—to the issuing authority's internal procedures, this CPS and the security and operational instructions issued from time to time.

5.4. Event Logging Procedures

Logging is the documentation of events occurring within Comda's electronic certificate issuance services through Comda's computing infrastructure. Documentation is performed by storing event records in a manner that prevents deletion by unauthorized parties.

5.4.1. Types of Events Logged:

Comda and/or its representatives maintain reliable records documenting all actions and events related to their operations close to the time of occurrence, including:

- System startup and shutdown times
- Password changes
- Unauthorized system access attempts
- Key generation or modification
- Certificate issuance and revocation
- System access authorizations

5.4.2. Log Processing Frequency:

Records are reviewed **hourly, daily, weekly or monthly**, depending on the procedures. Critical actions are reviewed and approved by the Security Manager. Logs are also examined whenever alerts indicate suspicious or unusual events.

5.4.3. Log Retention Period:

Logs are archived for **up to 25 years**.

5.4.4. Protection of Audit Logs:

Logs are stored in a secure electronic format within Comda's computing systems as part of the secured site and protected by both physical and logical security controls. Access is restricted through user management and access control mechanisms.

5.4.5. Backup of Audit Logs:

Comda maintains appropriate backup mechanisms for logs, ensuring high availability, reliability and protection against data loss.

5.4.6. Audit Log Collection System:

Comda operates an internal system for collecting audit records from the various systems involved in certificate issuance services. The system allows both collection and retrieval of records at any time and is subject to auditor review according to regulatory requirements.

5.4.7. Notification to Responsible Authorities:

The log monitoring system includes real-time alerts for significant events, which are immediately reported to the Issuing Authority Manager and the Security Manager. According to Comda's internal procedures, certain security incidents also require immediate reporting to third parties.

5.4.8. System Vulnerability Assessment:

Logs are documented, stored and analyzed in order to monitor and assess the vulnerability level of Comda's hardware and software systems. Vulnerability assessments are conducted as part of the **annual security and risk survey**, based on log data. Additional risk assessments may be performed daily, monthly or annually according to Comda's audit and security procedures using the most up-to-date log data.

5.5. Archiving of Records

Comda archives records as written documents or in the form of computerized messages, provided that their archiving, storage, preservation and retrieval are accurate and complete.

5.5.1. Types of Records Archived:

The records archived by Comda relate to actions and information essential for every application for issuance of an electronic certificate and to the issuance, use, revocation, expiration or renewal of electronic certificates, entry to and exit from protected areas within Comda, documentation of information security systems and the like. The record includes documentation of the date of the record, the identity of the person performing the action documented in the record and the type of record. The purpose of the documentation is to enable supervision and examination of the actions performed by Comda employees during the process of issuance of the electronic certificate and its revocation, as well as: the identity of the electronic certificate holder whose name is stated in each certificate and the documents by which he was identified; the identity of the persons requesting revocation of electronic certificates; other details specified in an electronic certificate; material details relating to the process of issuance of electronic certificates, including the applicant's declaration; documentation of details relating to management of Comda's private key (signature creation device), including creation of Comda's private key, its backup, its preservation, its destruction, and the manner of management of the software and hardware for encryption of the private key; documentation of events relating to information security, including attempts to harm Comda software, insofar as such became known to Comda, actions performed by Comda in connection with information security, changes in Comda's information security array, hardware and software failures and the like.

5.5.2. Retention Period for Archived Records:

Comda and/or its representatives shall preserve in a reliable manner records relating to electronic certificates for at least thirty (30) years after the date of revocation or expiration of the electronic certificate. These records may be preserved as electronic messages retrievable by computer or as written documents.

Comda shall preserve documents and information received from holders of electronic certificates and applicants for at least 25 years.

5.5.3. Protection of the Archive:

The records are preserved in electronic and manual audit reports. The reports are confidential and access to them is restricted by physical and technological means. The records in Comda are defined as confidential and access to them is granted only to a specific role holder after approval by the Security Manager. Any change in the records is permitted according to the role definition and is documented. Comda takes measures to prevent changes in the records, while using control over access to the manual and electronic reports.

The records containing customer details are kept in a secured room, entry to which is permitted only to authorized persons and only after biometric identification and a personal code.

5.5.4. Procedures for Backup of the Records Archive:

The backup system is operated only with respect to electronic records. Comda uses appropriate backup means for the records, at a high level of availability, reliability and protection against loss of information.

5.5.5. Requirement for Date and Time Stamps on Archived Records:

Electronic records include a date and time stamp indicating the time of creation of the record. See Section 6.8 below. Written records include the date of their creation indicated manually.

5.5.6. Archive System (Internal or External):

Comda implements an internal archive system for collection and preservation of records. The system enables both collection of the material and its retrieval at any given moment and is subject to the auditor's review in accordance with the requirements of the procedures.

5.5.7. Procedures for Collection and Verification of Archival Information:

Physical records are preserved in the original format and comply with the requirements in accordance with Comda's internal work procedures. Electronic records, including physical documents converted by scanning into an electronic format, are created, preserved and retrieved in accordance with the provision of law granting them the status of an original document.

5.6. Key Change of the Certification Authority

Where circumstances requiring replacement of the key pair (private and public) by means of which the Certification Authority signs the electronic certificate of the issuance server or the electronic certificate issued to the certificate holder occur, the key generation process described in Section 6.1 below shall take place. Once the key pair has been replaced, the electronic certificates to be issued thereafter shall be signed only by means of the new (replaced) key pair and no further use shall be made of the replaced key pair. Not every replacement of keys requires revocation of electronic certificates that are valid at the time of the replacement and that were signed by means of the previous key pair. For a case requiring revocation of an electronic certificate as a result of compromise of the signature creation device and the need to replace the key pair, see Section 4.9.1 above.

5.7. Disaster Recovery (DRP) and System Compromise

5.7.1. Procedures for Dealing with Unexpected Events and Compromise of the Certification Authority:

Comda and/or representatives of Comda shall implement, document, and periodically examine the appropriate plans for dealing with unexpected events and the capabilities and procedures for disaster preparedness, in a manner consistent with the provisions of these procedures and with Comda's security procedures (hereinafter: **"the plans"**).

The plans are intended for the following cases which prevent the continuation of operation of the Certification Authority site:

- A general electrical power failure and failure of the entire uninterruptible power supply system in the building where Comda's computing infrastructure is located.
- Physical destruction of Comda's computing systems and/or of the information contained therein by force majeure and/or fire and/or flood and/or magnetic disturbances and/or any other reason not under Comda's control.
- Logical or physical information security breach.

5.7.2. Compromise of Computing Resources, Software or Information

In any event the result of which is impairment of the availability of the computing systems of the Certification Authority, malfunction handling procedures shall be activated in an attempt to overcome the impediments and restore the computing systems of the Certification Authority to proper operation within the limits of the availability times in which these systems operate. If it is clarified to the Certification Authority that it is not possible to overcome the compromise within the limits of availability, the procedure for continuation of activity of the Certification Authority in the event of a disaster, as regulated in Section 5.7.4 below, shall be activated.

5.7.3. Procedures in the Event of Compromise of the Private Key of an Entity in the Hierarchy of the Certification Authority

Loss of control of or compromise of the private key of an entity in the hierarchy of the

Certification Authority in circumstances requiring generation of a new key pair and issuance of a new electronic certificate in place of the certificate signed by the compromised private key shall be carried out in accordance with Comda's internal work procedures, including replacement of electronic certificates whose reliability has been impaired, in coordination with certificate holders and, in appropriate circumstances, also with relying parties.

5.7.4. Business Continuity Following a Disaster Event

Comda has an alternative disaster recovery site (DRP) that enables Comda to continue publishing the list of revoked electronic certificates in the event of a disaster affecting Comda's primary site and preventing its operation.

5.8. Termination and/or Cessation of Comda's Operations

Comda shall terminate and/or cease its operations under the following circumstances:

1. A final liquidation order has been issued ordering the dissolution of Comda.
2. The Board of Directors of Comda has decided to cease Comda's activity as a Certification Authority.

If Comda ceases its operations, it shall take the following actions:

1. Cease issuing new electronic certificates.
2. Revoke as soon as possible all valid electronic certificates it has issued.
3. Immediately notify the certificate holders.
4. Enter the revoked electronic certificates into the Certificate Revocation List (CRL).
5. Cancel the appointment of any Registration Authority authorized to act on its behalf.
6. Continue maintaining the records required to provide proof of certification for the purposes of legal proceedings.

Where Comda's operations are discontinued, Comda may transfer its management to another entity. In such a case, a certificate holder shall have the right to request that the replacement Certification Authority revoke their certificate.

Without derogating from the provisions of any applicable law, Comda shall immediately notify every holder of a valid electronic certificate at the time of cessation of activity and shall act to minimize potential disruptions that subscribers and relying parties may suffer as a result of the cessation of its activity. The notification shall be sent by email.

5.9. Physical Security – Network Device

A corporation or individual wishing to store the signature creation device on an internal organizational network device is responsible for implementing internal security measures preventing unauthorized access to the device, removal of the signature creation device from the device and/or its copying.

Where the network device storing the signature creation device is under the control of a third party, a higher level of security is required, including placing the network device in a secured area protected by physical security measures such as:

- Access control systems
- Authorization management for access to the secured area
- Monitoring and logging systems
- Alarm systems

All of the above must be to the satisfaction of the Certification Authority.

Where the network device is hosted at Comda, Comda shall ensure that all security requirements imposed on Comda as a Certification Authority also apply to the network device.

6. Technical Security Controls

6.1. Generation and Installation of Key Pairs

6.1.1. Key Pair Generation:

Generation of the key pair of the electronic certificate holder is performed by the certificate holder using trusted hardware that complies with the requirements of these procedures and in a manner that prevents access to or interference with the generation process.

The key pair shall remain under the full control of the electronic certificate holder, or a person acting on their behalf, at all times.

6.1.2. Delivery of the Private Key to the Certificate Holder:

Delivery of the private key to the electronic certificate holder shall take place at the time of issuance and in a secure manner that protects the exclusive control of the certificate holder, or their representative, over the private key.

Key generation shall be performed within a hardware device that prevents unauthorized access to the signature creation device. The Certification Authority is prohibited from holding a copy of the private key of the electronic certificate holder.

6.1.3. Delivery of the Certificate Holder's Public Key to the Certification Authority:

Delivery of the certificate holder's public key to the Certification Authority must be performed through a mechanism ensuring that the public key is transferred intact and without modification, and that the electronic certificate holder possesses the private key corresponding to the public key being transmitted.

6.1.4. Publication of the Certification Authority's Public Key to Relying Parties:

Generation of Comda's key pair is carried out under physical and logical security conditions by trusted role holders specially appointed for this purpose.

At least **six individuals** are required for the creation and encryption of Comda's signature creation device. **At least four individuals** are required to restore the key.

As an additional security measure, parts of the key are distributed among trusted role holders so that only the combination of all role holders possessing the key parts together enables decryption and restoration of the key.

The public key of the Certification Authority is publicly available to relying parties relying on electronic certificates issued by the Certification Authority on the Certification Authority's website at:

https://www.comda.co.il/repository

6.1.5. Key Sizes:

The size of Comda's signature creation device (private key) is **521 bits using the ECC algorithm**.

The private key of an electronic certificate holder shall not be less than:

- **112 bits using the ECC algorithm**, or
- **2048 bits using the RSA algorithm**.

The private key size shall at all times comply with the current requirements of Regulation 8 of the Electronic Signature Regulations (Hardware and Software Systems).

Comda's key pair is valid until **25/05/2048**. Comda's key pair may be replaced before this date. The new public key will be published in Comda's repository.

The key pair will also be replaced if standards governing the length and/or algorithm of the signature creation device (private key) are changed.

6.1.6. Public Key Generation Parameters and Quality Control:

Comda's public key is generated within a **key ceremony** conducted according to internal procedures designed to establish a secure environment both physically and in terms of the reliability of the participants and hardware used.

A trusted hardware device (**FIPS 140-2 Level 3**) is used for the generation, protection and destruction of Comda's signature creation device (private key).

The public key of an electronic certificate holder is generated at the time of certificate issuance as regulated in **Section 3.2.1 above and Section 6.2.1 below**, subject to the conditions specified therein.

6.1.7. Key Usage (X.509v3 Key Usage Field):

For every electronic certificate signed using the key pair of the Certification Authority, the following key usage fields are enabled:

- **Digital Signature**
- **Certificate Signing**
- **Off-line CRL Signing**
- **CRL Signing**

The keys are used exclusively for the creation of electronic certificates and CRLs within a protected hardware environment that complies with the procedures and standards under which Comda operates.

In order to comply with the **X.509v3 standard**, the key usage field in electronic certificates signed by the Certification Authority's signature creation device includes usage restrictions in accordance with the subscription agreement and the certificate issuance request.

6.2 Protection of the Private Key and Cryptographic Controls

6.2.1. Standards and Controls for Cryptographic Devices

Comda's signature creation device, used by the Certification Authority to sign electronic certificates, is generated solely by Comda and remains under its exclusive control.

Comda's signature creation device and/or that of its representatives is protected using trusted hardware and security mechanisms. Specifically, Comda's signature creation device shall meet all of the following conditions:

1. If based on an **RSA or DSA key**, it shall be at least **2048 bits** in length.
2. If based on an **ECC key**, it shall be at least **112 bits** in length.
3. It shall be protected by a device meeting at least **FIPS 140-2 Level 3** security requirements.
4. It shall be backed up using protected and secure mechanisms, and the backup shall be stored separately.

Within a reasonable period prior to revocation or expiration of the Certification Authority's signing device, the Certification Authority shall generate a **new signing key pair** to prevent disruption of ongoing operations. Generation of the new key pair shall also comply with the above standard or any higher standard required at that time.

Generation and storage of the certificate holder's signature creation device shall also be performed using trusted hardware devices (e.g., **smart cards, tokens, HSMs**).

Where access to the certificate holder's private key is controlled by a password, the password must comply with **high-level security requirements according to Israeli Standard 1495 Part 3**, or alternative requirements where exemption from that standard is justified.

6.2.2. Split Knowledge and Multi-Person Control (m of n) Over the Private Key

To distribute authority and reduce the possibility of fraud, the following measures are applied for protection of Comda's private key:

- Comda's private key is encrypted in its entirety on a **hardware-based cryptographic card** and stored in Comda's safe.
- The **encryption key protecting the private key** is divided into several parts.

- Each part is entrusted to a Comda employee who is **not directly involved in certificate issuance or management services**.
- All such employees undergo **strict and periodic reliability checks**.

Only the **combination of all parts through a controlled and monitored process** enables reconstruction of the encryption key.

6.2.3. Escrow of the Private Key

Not applicable. Comda's private key is **not held in escrow**. Protection is implemented as described in Section 6.2.2.

6.2.4. Backup of the Private Key

Comda performs backup operations for all its systems, including the private key, as part of its **disaster recovery preparations**.

Backup of the private key is carried out by trusted role holders, and storage of the backups separately is subject to the security procedures applied to the protection of Comda's signature creation device.

6.2.5. Archiving of the Private Key

Comda's signature creation device shall be preserved under secure conditions consistent with the protection requirements defined in these procedures after its revocation or expiration and after it ceases to be used, for an additional period of **not less than 12 months**.

Archiving of the private key of an electronic certificate holder whose certificate has expired or been revoked is at the **sole discretion of the certificate holder**. The certificate holder is under **no legal or contractual obligation** to archive their signature creation device after revocation or expiration.

6.2.6. Import and Export of the Private Key

The hardware devices used by Comda for generating signature creation devices—both for the Certification Authority and for certificate holders—are designed so that **the private key is generated within the hardware device**, and it is **not possible to import or export the private key from the device**.

6.2.7. Storage of the Private Key in the Device

The signature creation device of both the Certification Authority and the electronic certificate holder shall be stored within a **secure hardware device** as specified in Section 6.2.1 above.

6.2.8. Activation of the Private Key

Access to and activation of the signature creation device (private key) is permitted only to the owner of the signature creation device or a person authorized on their behalf.

Activation of the signature creation device shall only be possible using a **password or another unique identification method** (e.g., biometric identification) belonging to the signature device owner or their authorized representative, in accordance with legal requirements.

6.2.9. Termination of Private Key Operation

Operation of the private key terminates upon completion of each activation and use, after which the key becomes inactive.

6.2.10. Destruction of the Private Key

Destruction of the private key results in destruction of the logical information constituting the signature creation device.

This may be achieved either by:

- Complete deletion of the logical information stored in the hardware component where the private key is stored, or
- Complete destruction of the hardware device in a manner preventing further use or reconstruction of the stored information.

6.2.11. Cryptographic Device Rating

The signature creation devices of both the Certification Authority and the certificate holder are protected by **encryption software or hardware tokens (TOKENs)** and comply with the provisions set forth in these procedures.

Where the applicant receives from Comda the hardware device generating and containing the signature creation device, **Comda is responsible** for ensuring that the signature creation device and the signature verification device comply with the requirements of **Regulation 8 of the Electronic Signature Regulations (Hardware and Software Systems)**.

Where the applicant does **not** receive the hardware device from Comda, Comda will issue an electronic certificate only after verifying that the applicant possesses a signature creation device capable of producing a secure electronic signature and that both the signature creation device and the signature verification device comply with Regulation 8.

For the purpose of compliance with **Regulation 8(1)(b) and (c)**, Comda may rely on a declaration from the applicant regarding the signature creation device used, its operation and access to it.

Comda shall not be responsible for an electronic certificate issued for a signature creation device that **was not supplied by Comda**.

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archiving

Comda archives in its repository the public keys of its signing servers and applies to them, with the necessary adjustments, the provisions of Section 5.5 above.

The electronic certificate holder has **no legal or contractual obligation** to archive the public key after destruction, expiration, or revocation of the corresponding private key.

6.3.2. Validity Period for the Use of the Electronic Certificate and Key Pair

The validity period for the use of an electronic certificate is determined at the time of its issuance. This period shall **not exceed five (5) years**, or a shorter period if required due to technological requirements or other reasons necessitating replacement of the key pair and issuance of a new electronic certificate.

Renewal of an electronic certificate before its expiration **does not require replacement of the key pair**.

Two valid electronic certificates **cannot be issued for the same key pair**. Therefore, renewal of an electronic certificate requires expiration of the previous certificate.

6.4. Activation Data

6.4.1. Generation and Installation of Activation Data

The generation of activation data required for operation of the signature creation device and its installation in the hardware device storing it (e.g., smart card, storage chip, network device, HSM, etc.) shall comply with all security requirements of these procedures.

6.4.2. Protection of Activation Data

The activation data required for operation of the signature creation device shall be protected by cryptographic means and shall at all times remain under the full control of the owner of the signature creation device or an authorized representative responsible for its protection.

6.4.3. Other Aspects of Activation Data

Not applicable.

6.5. Computer Security Controls

6.5.1. Specific Technical Requirements for Computer Security

In providing its services, Comda and its representatives shall use **trusted systems only**.

System components used for issuance and revocation of electronic certificates shall meet **Common Criteria EAL4 security level**.

Comda uses trusted information security systems. These systems are confidential and not accessible to the general public but are subject to external audits. As part of these controls, Comda undergoes **annual audits by an independent auditor** to verify system reliability and compliance with procedures.

In addition, a **yearly risk assessment** is conducted by an independent external information security expert to evaluate system security.

Comda complies with **ISO 27001 information security standards** and is audited by independent entities to maintain compliance with these standards.

6.5.2. Computer Security Rating

Comda complies with the information security standards defined in these procedures.

6.6. Technical Security Controls During the Certificate Validity Period

6.6.1. System Development Controls

Before any development or enhancement of a system component used by the Certification Authority is introduced into operation, it must undergo **quality assurance and compatibility testing**.

In addition, such developments are examined during the **annual risk assessment conducted by an independent external expert**.

6.6.2. Security Management Controls

Comda operates, under the management of the Security Manager of the Certification Authority, a **monitoring and control system** that continuously tracks security issues in order to:

- Detect security failures
- Protect system integrity and Comda's information against viruses and malicious or unauthorized software

- Minimize damage resulting from security incidents through incident reporting and response procedures
- Handle media used by Comda securely to protect it from damage, theft or unauthorized access
- Implement media management procedures ensuring protection against deterioration or obsolescence during the required record retention period
- Maintain procedures for all trusted and management roles affecting the availability and quality of electronic certificate services
- Monitor capacity requirements and forecast future capacity needs to ensure availability of processing power and storage resources
- Respond quickly to security incidents and limit the impact of security breaches

All incidents are reported **as soon as possible after occurrence** and remain under monitoring until resolution.

6.6.3. Security Controls During the Validity Period of the Electronic Certificate

Comda operates a continuous control system intended to ensure the **integrity and proper functioning of hardware systems** responsible for encryption and signing of information relating to electronic certificates and their validity status, including:

- Lists of valid certificates
- Lists of revoked certificates
- Additional information relating to their operation or revocation

(See also Section 6.6.2 above.)

6.7. Network Security Controls

Comda implements a **network security policy, access control, and user management** while maintaining strict separation between systems responsible for electronic certificate issuance and management and online systems connected to the Internet.

The online components are protected by security mechanisms designed to:

- Prevent system intrusion
- Prevent introduction of viruses or malicious software
- Detect unauthorized intrusion attempts

6.8. Date and Time Stamp

The date and time stamp is intended to improve the reliability of Comda's electronic certificate issuance services.

A date and time stamp indicates the **correct date and time of an operation and the identity of the person or device that created the stamp**.

The time stamp reflects **Greenwich Mean Time (GMT)** and follows **Universal Coordinated Time (UTC)** conventions.

Comda's time stamp relies on a **trusted third-party time source** providing official world time readings at any given moment.

Comda shall apply date and time stamps to the following data, either directly or within a trusted parallel audit trail:

- Electronic certificates
- Certificate Revocation Lists (CRL) and other database records relating to certificate revocations
- Other information as required by these procedures

6.9. Logical Security – Signature Server

When the signature creation device is stored on a **signature server**, it must be generated and stored within a **cryptographic module certified under Common Criteria EAL4 or at least FIPS 140-2 Level 3**, which does not allow duplication of the signature creation device after generation or copying outside the storage device (except for backup purposes).

Access to and activation of the signature creation device shall require **unique identification of the signature owner** and shall be limited only to the partition within the signature server where the signature creation device is stored.

Operation of the signature creation device and access to it shall ensure the **exclusive control of the signer over the signature**, using a physical cryptographic component or a unique password that complies with the relevant standards and the requirements of Regulation 8(1)(b) and 8(1)(c) of the Electronic Signature Regulations (Hardware and Software Systems).

When the signature creation device is stored on a **signature server controlled by a third party**, a higher level of security is required to ensure the exclusive control of the signature owner over the private key.

This higher security level is achieved through a **combination of mechanisms**, including:

- A separate device used to activate the signature creation device (e.g., smart card, one-time password generator, or mobile phone with one-time passwords)

- A permanent password known only to the authorized user (or biometric authentication)

Only after these steps is access granted to the signer's personal storage device through a **separate unique password**, after which access to the signature creation device within the signer's designated partition on the signature server becomes possible.

7. Certificate, CRL and OCSP Profiles

7.1 Certificate Structure

7.1.1 Version Number(s)

Comda issues electronic certificates compliant with **X.509 version 3**.

7.1.2 Certificate Extension Fields

Comda uses the following certificate extensions:

- **Authority Key Identifier** – OID 2.5.29.35
- **Subject Key Identifier** – OID 2.5.29.14
- **Key Usage (critical)** – OID 2.5.29.15
- **Certificate Policies** – OID 2.5.29.32
- **Subject Alternative Name** – OID 2.5.29.17
- **Basic Constraints (critical)** – OID 2.5.29.19
- **Extended Key Usage** – OID 2.5.29.37
- **CRL Distribution Points** – OID 2.5.29.31
- **Authority Information Access** – OID 1.3.6.1.5.5.7.1.1
- **Qualified Certificate Statement** – OID 1.3.6.1.5.5.7.1.3

7.1.2.1 Extension Fields in the Root Certificate of the Certification Authority (Root CA)

(i) basicConstraints

a. This extension appears as a **critical extension**.
b. The **CA field** is set to **true**.
c. The **pathLenConstraint field** is set to **1**.

(ii) keyUsage

a. This extension is present and marked as **critical**.
b. Bit positions for **digitalSignature**, **CertSign**, and **cRLSign** are set.

(iii) certificatePolicies

a. This extension is **not present**.

(iv) extendedKeyUsage

a. This extension is **not present**.

(v) Subject Information

The **Certificate Subject** contains the following:

- **countryName (OID 2.5.4.6)**
  Contains the two-letter **ISO 3166-1 country code** for the country in which the CA's place of business is located = **IL**
- **organizationName (OID 2.5.4.10)**
  Contains the Subject CA's name = **Comda Ltd.**
- **Common Name (OID 2.5.4.3)**
  ComSign Advanced Root CA

(vi) Certificate Details

Data:

Version:
3 (0x2)

Serial Number:
7b63902e2183a98d46670baaa731c737

Signature Algorithm:
sha512ECDSA

Issuer:

countryName = IL
organizationName = Comda Ltd.
commonName = ComSign Advanced Root CA

Validity:

Not Before: Jun 25 07:53:03 PM 2023
Not After : Jun 25 10:08:20 PM 2048

Subject:

countryName = IL
organizationName = Comda Ltd.
commonName = ComSign Advanced Root CA

Subject Public Key Info:

Public Key Algorithm: **ECC 521**
Public-Key: **(521 bit)**

X509v3 extensions:

X509v3 Basic Constraints: critical
CA: TRUE

X509v3 Key Usage: critical
Digital Signature, Certificate Sign, CRL Sign

X509v3 Subject Key Identifier:
43192870d62e82bba711f4ea19ae38e1fbbbe8c4

Signature Algorithm:
sha512ECDSA

7.1.2.2 Intermediate Certificate

(i) certificatePolicies

a. This extension is present and **not marked as critical**.
b. certificatePolicies:policyQualifiers:qualifier:cPSuri contains the **HTTP URL** for the Root CA's Certificate Policies and Certification Practice Statement.

(ii) cRLDistributionPoints

a. This extension is present and **not marked as critical**.
b. It contains the **HTTP URL of the CA's CRL service**.

(iii) authorityInformationAccess

a. This extension is present and **not marked as critical**.
b. It contains the **HTTP URL of the Issuing CA's OCSP responder** (accessMethod = **1.3.6.1.5.5.7.48.1**).
c. It also contains the **HTTP URL of the Issuing CA's certificate** (accessMethod = **1.3.6.1.5.5.7.48.2**).

(iv) basicConstraints

a. This extension is present and **marked as critical**.
b. The **CA field is set to true**.

(v) keyUsage

a. This extension is present and **marked as critical**.
b. Bit positions for **CertSign** and **cRLSign** are set.

(vi) Subject Information

The **Certificate Subject** contains the following fields:

a. **countryName (OID 2.5.4.6)**
The two-letter **ISO 3166-1 country code** for the country in which the CA's place of business is located = **IL**.

b. **organizationName (OID 2.5.4.10)**
The Subject CA's name.

c. **Common Name (OID 2.5.4.3)**
Comda represents that it followed the procedures set forth in its **Certificate Policy and Certification Practice Statement** to verify that, as of the certificate issuance date, all Subject Information was accurate.

(vii) Example – Comsign Advanced Professional CA Certificate Details

Data

Version: 3 (0x2)

Serial Number:
780000000a27ff7aff34015cfd00010000000a

Signature Algorithm:
sha512ECDSA

Issuer

countryName = IL
organizationName = Comda Ltd.
commonName = Comsign Advanced Root CA

Validity

Not Before: Jun 25 10:32:49 PM 2023
Not After : Jun 25 10:42:49 PM 2034

Subject

commonName = Comsign Advanced Professional CA
organizationName = Comda Ltd.
countryName = IL

Subject Public Key Info

Public Key Algorithm: ECC
Public-Key: (521 bit)

X509v3 Extensions

Authority Information Access

OCSP – URI:
http://ocsp1.comsign.co.il/ocsp

CA Issuers –
http://fedir.comsign.co.il/crl/ComsignAdvancedRootCA.crt

X509v3 Basic Constraints (critical)
CA: TRUE, pathlen: 0

X509v3 Certificate Policies

Policy: X509v3 Any Policy
CPS:
http://www.comda.co.il/repository

X509v3 CRL Distribution Points

Full Name:
http://fedir.comsign.co.il/crl/ComsignAdvancedRootCA.crl

Full Name:
http://crl1.comsign.co.il/crl/ComsignAdvancedRootCA.crl

X509v3 Key Usage (critical)
Certificate Sign, CRL Sign, Digital Signature

X509v3 Subject Key Identifier

cd14eb85272d3a139f7a7b40bd51a90e4d887dea

X509v3 Authority Key Identifier

KeyID = 43192870d62e82bba711f4ea19ae38e1fbbbe8c4

Signature Algorithm

sha512ECDSA

7.1.2.3 Structure of Subscriber Certificates

(i) Certificate Structure for an Individual

Field Name	Description	Example
Version	Certificate version	"V3"

Field Name	Description	Example
Serial Number	The serial number of the certificate. This value is unique.	"00 bc be ac 46 8b 09 ad e5 2d 31 ed f0 8e 02 ed ab"
Signature Algorithm	The signature algorithm used by the certificate holder.	SHA256ECDSA

Issuer

Fields describing the issuing authority:

Field	Example
CN – Full Name	Comsign Advanced Professional CA
O – Issuer Organization Name	Comda Ltd.
C – Country	IL

Validity

Fields describing the certificate validity period.

Field	Description	Example
Valid from	Start of validity (date of issuance)	Tuesday, 10 December 2023 06:10:33
Valid to	Expiration date	Monday, 09 December 2025 05:24:21

Subject (Certificate Holder Details)

Details of the individual for whom the certificate was issued.

Field	Example
CN – Full name of certificate holder (English) and ID number	Levy Israel ID 012345678
SN – Last name (English)	Levy
G – First name (English)	Israel

Field	Example
SerialNumber – ID number	01-012345678
O – Organization name (Identification code and ID number)	07-012345678
OU – Organizational Unit (Full name of certificate holder in English)	Israel Levy
T – Title	Personal Certificate
C – Country	IL

Public Key

Field	Description	Example
Public Key	Public key length of the certificate holder	ECC (256 Bits)

CRL Distribution Points

Link to the Certificate Revocation List (CRL):

[1] CRL Distribution Point
Distribution Point Name:
Full Name:
URL=http://fedir.comsign.co.il/crl/ComSignAdvancedCorpCA.crl

[2] CRL Distribution Point
Distribution Point Name:
Full Name:
URL=http://crl1.comsign.co.il/crl/ComSignAdvancedCorpCA.crl

OCSP Distribution (Online Certificate Status Protocol)

Link to the OCSP server:

[1] Authority Information Access
Access Method = OCSP (1.3.6.1.5.5.7.48.1)
URL = http://ocsp1.comsign.co.il/ocsp

[2] Authority Information Access
Access Method = Certification Authority Issuer (1.3.6.1.5.5.7.48.2)

qcStatements

OID: **1.3.6.1.5.5.7.1.3**

Authority Key Identifier

Key Identifier of the intermediate certificate:

KeyID = e36c6ddd5ab0fd0316cdb2e4e92caf847ee567f1

Certificate Policies

Policies (CPS) regulating the activity of the issuing authority (Comda).

The email address of the certificate holder **has not been verified by the issuing authority for reliance purposes**.

Certificate Policy:
Policy Identifier = 1.3.6.1.4.1.19389.2.1.1

Policy Qualifier:
CPS
http://www.comda.co.il/repository

User Notice:
Organisation = Comda
Notice Number = 11
Notice Text =
The certificate holder was identified remotely based on documents,
a remote identification system and/or other identifying information
and/or face-to-face identification.
Use of this certificate is subject to Comda's procedures.
Comda's liability is limited as detailed in the procedures.
Restrictions on the use of the certificate are optional.

Extended Key Usage

Purposes for which the certificate may be used (vary by certificate type):

- Secure Email (1.3.6.1.5.5.7.3.4)
- Client Authentication (1.3.6.1.5.5.7.3.2)
- Smart Card Logon (1.3.6.1.4.1.311.20.2.2)

Subject Alternative Name (Authorized Signatory Details)

Field	Example
RFC822 Name – Email address provided by certificate holder	levy@israel.co.il
C – Country	IL
O – Organization name (Identification code and ID number)	07-012345678
OU – Organizational Unit (Full name in Hebrew)	ישראל לוי
T – Title	Personal Certificate
SN – Last name (Hebrew)	לוי
G – First name (Hebrew)	ישראל
CN – Certificate holder name (Hebrew) and ID number	לוי ישראלID_012345678

Authority Information Access

[1] CA Issuer
URL=http://fedir.comsign.co.il/cacert/ComSignAdvancedCorpCA.crt

[2] OCSP
URL=http://ocsp1.comsign.co.il/ocsp

Subject Key Identifier

9e8d8b8a912a3f9066ecc6250ee14b69e09f9b16

Key Usage

Purpose of the certificate:

Non-Repudiation

Thumbprint Algorithm

sha256

Thumbprint (Signature Value)

Certificate details signed by the issuing authority:

e2 a1 5a 40 07 e4 a3 c3 88 66 91 14 5b 9c 00 ff e4 1d 24 8e

(ii) Certificate Structure for an Authorized Signatory in a Corporation or Public Institution

Field Name	Description	Example
Version	Certificate version	V3
Serial Number	Unique certificate serial number	00 bc be ac 46 8b 09 ad e5 2d 31 ed f0 8e 02 ed ab
Signature Algorithm	Algorithm used by the certificate holder	sha256ECDSA

Issuer

Field	Example
CN	Comsign Advanced Corporations CA
O	Comda Ltd.
C	IL

Validity

Field	Example
Valid From	Tuesday, 10 December 2023 06:10:33
Valid To	Monday, 09 December 2025 05:24:21

Subject (Corporate Signatory)

Field	Example
CN	Avraham Shlomo ID_012345678
SN	Avraham

Field	Example
G	Shlomo
SerialNumber	01-012345678
O – Identification code + company registration number	05-519999999
OU – Corporation/Public institution name (English)	Comda LTD.
T – Title	Manager
C – Country	IL

Public Key

ECC (256 Bits)

CRL Distribution Points

http://fedir.comsign.co.il/crl/ComSignAdvancedCorpCA.crl
http://crl1.comsign.co.il/crl/ComSignAdvancedCorpCA.crl

OCSP

http://ocsp1.comsign.co.il/ocsp

Certificate Policies

CPS:
http://www.comda.co.il/repository

Extended Key Usage

- Secure Email
- Client Authentication
- Smart Card Logon

Subject Alternative Name (Hebrew Details)

Field	Example
Email	Shlomo@test.co.il

Field	Example
Country	IL
Organization	05-519999999
OU (Hebrew)	קומדע בע"מ
Title	מנהל
SN (Hebrew)	אברהם
G (Hebrew)	שלמה
CN (Hebrew + ID)	אברהם שלמהID_012345678

Subject Key Identifier

9e8d8b8a912a3f9066ecc6250ee14b69e09f9b16

Key Usage

Non-Repudiation

Thumbprint Algorithm

SHA256ECDSA

Thumbprint

f1 36 18 f7 fe 2a 1a 34 24 47 e6 7f 85 24 93 40 4d d5 18 73

7.1.3 Algorithmic Object Identifiers (OIDs)

Use of Signature Algorithm

Comda uses the following signature algorithm:

SHA256 with RSA Encryption – OID 1.2.840.10045.4.3

7.1.4 Name Forms

Various names may appear in certificates issued by Comda, as described in Section 3.1.

The names may include the following:

- The name of a person or organization as it appears in the identification document used for identification, as specified in Section 3.2.
- An email address according to the **RFC822** standard, as provided by the certificate holder.
- A name in the **Distinguished Name structure** according to **RFC1779**, including fields such as: **CN, O, OU, C, G, SN, T**.

7.1.4.1 Information about the Issuing Authority

The content of the **Distinguished Name Field** of the certificate issuer shall always correspond to the **Subject DN** of the issuing authority.

7.1.4.2 Subject Information Field in the Certificate

By issuing the certificate, **Comda confirms that it complies with the requirements of this policy document** and that, as of the date of issuance of the certificate, the information contained in the **Subject Information field** is accurate.

7.1.4.3 Subject Alternative Name Extension Field

See Section **7.1.2**.
Comda shall **not issue certificates for Reserved IP Addresses or Internal Names**.

7.1.4.4 Subject Distinguished Name Fields

For possible **Subject DN fields**, see Section **7.1.2**.

All included information shall be verified in accordance with the provisions set forth in **Sections 3.2.2 and 3.2.3**.

The **Subject DN fields** shall contain only meaningful information related to the certificate holder and **not metadata**, such as:

- "."
- "-"
- blank spaces
- or any indication of missing, incomplete, or irrelevant values.

7.1.5 Restrictions on Names

Comda does **not impose restrictions on names**, provided that the names comply with the conditions specified in **Section 3.1**.

7.1.6 Object Identifier for Certificate Policy

Certificates issued by Comda comply with the **Comda Certificate Policy**, which has the following object identifiers:

(i) Individual Certificate:
OID **1.3.6.1.4.1.56578.2.1**

For additional details regarding object identifiers in the **Root Certificate, Intermediate Certificate, or Subscriber Certificates**, see **Section 7.1.2 above**.

7.1.7 Policy Constraints Extension

The **Policy Constraints extension** is **not used**.

7.1.8 Structure and Syntax of Certificate Policy Attributes

Comda specifies in the **Certificate Policies field** a reference to this document and to the certificate policy described herein.

Comda specifies in the **QCStatement field** compliance with **electronic signature standards**, according to specifications defined by several international organizations, as detailed in Comda's internal procedures.

In cases where an **electronic certificate is issued for a signature key stored on a network device**, this fact shall be indicated in the certificate under the **certificate policies** field.

Where the **network device is hosted by a third party**, this fact shall be explicitly indicated in the certificate under the **certificate policies** field, so that a relying party is aware that the **signature key is stored on a network device operated by a third party unrelated to the certificate holder or the organization on whose behalf the signature is made**.

7.1.9 Clarification Regarding the Country Code in Certificates Issued to Residents of the Palestinian Authority or Palestinian Corporations

Comda shall include the following clarification in the electronic certificate **in both Hebrew and English**:

English:
"The information provided under the 'country code' section is based on the ISO-3166 Code, is for technical purposes only, and is without prejudice to the legal status of any country or territory or of its authorities."

Hebrew:
"המידע המופיע תחת סעיף 'country code' הינו בהתאם לתקן ISO-3166, הינו טכני בלבד ואין בו כדי להוות אמירה כלשהי ו/או להשליך על המעמד המשפטי של מדינה, טריטוריה, רשות או סמכויותיהן".

7.2 Structure of the Certificate Revocation List (CRL)

7.2.1 Version Number

The **CRL files are version 2**.

7.2.2 CRL and CRL Entry Extensions

CRL Profile

Field Name	Description	Example
Version	CRL version	V2

Issuer

Fields describing the issuing authority.

Field	Example
Issuer CN (Common Name)	Comsign Advanced Professional CA
Organization (O)	Comda Ltd.
Country (C)	IL

Validity

Fields describing the validity of the CRL.

Field	Description	Example
This Update	CRL publication time	Tuesday, 10 December 2023 06:10:33
Next Update	Next CRL publication time (at the latest)	Wednesday, 11 December 2023 06:10:33

Signature Algorithm

Field	Description	Example
Signature Algorithm	The signature algorithm used to sign the CRL file	sha256

Revoked Certificates

Fields describing the revoked certificates.

Field	Description	Example
Serial Number	The serial number of the certificate (unique value)	00 bc be ac 46 8b 09 ad e5 2d 31 ed f0 8e 02 ed ab
Revocation Date	Date on which the certificate was revoked	Tuesday, 10 December 2023 02:10:33
Invalidity Date	Date from which the certificate is considered invalid	Tuesday, 10 December 2023 02:10:33

Revocation Reason Codes

Possible reasons for revocation:

Code	Reason
(0)	unspecified
(1)	keyCompromise
(2)	cACompromise
(3)	affiliationChanged
(4)	superseded
(5)	cessationOfOperation
(6)	certificateHold
(8)	removeFromCRL
(9)	privilegeWithdrawn

Code Reason

(10) aACompromise

CRL Number

Field	Description	Example
CRL Number	Serial number of the CRL list	Example: 1e

7.3 Online Certificate Status Protocol (OCSP) Profile

7.3.1 Version Number

The **OCSP response version is 1**.

7.3.2 OCSP Extensions

Field Name	Description	Example
Responder ID	Identifier used to identify the OCSP responder. The identifier may use either the responder's name or the hash of its public key.	byKey: 5f39bbeb80201bbdb8d7f9bebe5f4011a3dac25b

Produced At

Field	Description	Example
Produced At	Date and time the OCSP response was signed	2023-12-07 12:04:25 (UTC)

Cert ID

Identification details of the certificate whose validity is checked by the OCSP responder.

The details include:

1. Hash algorithm

2. Hash value of the issuer name
3. Hash value of the issuer public key
4. Certificate serial number

Example:

hashAlgorithm (SHA-1)
Algorithm Id: 1.3.14.3.2.26 (SHA-1)

issuerNameHash: 7b7f618dd153e1d2f7ad862f000cc6f0a116bcb0
issuerKeyHash: f5bbadea31234b005d5b4f76de6f8b02e0fddff0
serialNumber: 0x00e8d3baab1b84226459fb12378cd6f459

Certificate Status

Field	Description
Cert Status	Certificate validity status

Possible values:

Value	Meaning
good [0]	Certificate is valid
revoked [1]	Certificate has been revoked
unknown [2]	Certificate status unknown

This Update / Next Update

Field	Description	Example
This Update	Beginning of the validity period of the information used by the OCSP responder	2023-12-07 08:00:17 (UTC)
Next Update	End of the validity period	2023-12-08 08:00:18 (UTC)

Signature Algorithm

Field	Description	Example
Signature Algorithm	Algorithm used to sign the OCSP response	sha256WithRSAEncryption

Signature

Field	Description	Example
Signature	The responder's signature on the OCSP response	1c12e794f305b2ca183f1da117c465deb4fc21667146a2ae...

Certificate

Certificate used to sign the OCSP response.

Example structure:

signedCertificate
version: v3 (2)
serialNumber: 0x0e2bcda4aa4f8f…
signature …
Algorithm Id: 1.2.840.113549.1.1.11
issuer: …
validity: …
subject: …
subjectPublicKeyInfo: …
extensions: …

8. Compliance Audit

8.1 Frequency or Circumstances of Audits

Comda is subject to **internal operating procedures and audit and review processes**.

Audits are conducted **annually**, and if necessary, **more frequently**.

In addition, in order to comply with the **Israeli Standard 27001 and ISO 9000/9001**, audits shall be conducted as required under those standards by **licensed auditing bodies authorized to conduct such audits**.

Comda complies with **all CA/Browser Forum requirements**, including requirements for **periodic audits and reporting**.

8.2 Identity of the Auditor

The auditor is a **qualified professional in the field of information security**.

In accordance with **CA/Browser Forum requirements**, the auditor must be an auditor meeting the certification requirements of **WebTrust and/or ETSI**.

8.3 Auditor Independence

The auditor is an **independent contractor**, who is **not an employee of Comda and is not subordinate to Comda in any manner**.

8.4 Topics Covered by the Audit

The audit topics are specified within each applicable standard, including:

- **ISO 27001**
- **ISO 9001**
- **WebTrust**
- and others.

8.5 Actions Following Findings of Deficiencies or Failures

Comda shall review the audit reports and **promptly correct any deficiencies**, if any are identified.

8.6 Distribution of Audit Results

Audit findings are considered **confidential information** and are **not intended for distribution**, except for:

- the **management of the issuing authority**, and
- the **responsible parties within the organization** in the relevant areas where findings requiring corrective action were identified.

Comda **does publish its WebTrust audit results**, which can be viewed in Comda's repository at:

http://www.comda.co.il/repository

8.7 Internal Self-Audit

Comda conducts a **quarterly internal audit**, during which its operations and compliance are reviewed against:

- this policy document
- internal operating procedures
- CA/Browser Forum requirements.

Additional Legal and Business Matters

8.8 Fees

8.8.1 Fees for Certificate Issuance or Renewal

Comda charges fees for **electronic certificate issuance and renewal services**.

Comda's pricing **may change from time to time** and depends on:

- the scope of services provided
- the type of certificates issued.

For the avoidance of doubt, **changes in Comda service prices shall not apply retroactively**.

8.8.2 Fees for Access to Certificate Lists

Comda **does not charge fees for access to lists of electronic certificates**, to the extent such access is available.

8.8.3 Fees for Certificate Status Checking

Comda **does not charge fees for access to the Certificate Revocation List (CRL)** for the purpose of verifying certificate status.

8.8.4 Fees for Other Services

Comda may charge fees for **additional services upon request**, according to its pricing as determined from time to time.

8.8.5 Refund Policy

Subject to applicable law, an **electronic certificate that has been revoked at the request of the certificate holder**, or for any reason not attributable to Comda, including:

- certificates renewed before their expiration date for the remaining period until the original expiration date,

shall not entitle the certificate holder to a refund, including **partial or proportional refunds**.

8.9 Financial Liability

8.9.1 Insurance Coverage

Comda maintains **professional liability insurance** in appropriate amounts and under appropriate terms.

8.9.2 Other Guarantees

Comda has provided **all guarantees and assurances required for its operation as a Certification Authority**.

8.9.3 Insurance or Guarantee for End Users

Comda shall provide **a bank guarantee, other financial guarantee, or insurance** in order to ensure compensation for any person harmed due to an act or omission resulting from Comda's failure to comply with its obligations under these procedures.

The **amount of the guarantee** shall be determined by Comda from time to time **at its sole discretion**, provided that it meets the requirements of the relevant standards.

8.10 Protection of Confidential Business Information

8.10.1 Confidential Business Information

The certificate holder is hereby informed that **any information appearing in the certificate fields**, even if considered confidential business information by the certificate holder, **shall not be treated as confidential and shall not receive protection**.

Therefore, certificate holders are advised **not to include unnecessary information in certificate fields that may be considered confidential business information**.

At the same time, Comda may require the certificate holder to provide **business-related information regarding its operations**, including for:

- identification purposes
- billing and collection
- determining eligibility for a specific type of certificate.

Such information, **which is not included in the certificate fields**, shall be stored in Comda's archive as **confidential information**, accessible **only to authorized personnel on a need-to-know basis** for the purpose of providing certificate services.

It is clarified that **business information that would normally be considered confidential**, but has been **published publicly by an authorized party**, shall **no longer be considered confidential business information**.

8.10.2 Business Information That Is Not Protected

The contents of **certificate fields and certificate revocation lists**, even if they contain business information, **shall not be considered confidential information entitled to protection**.

8.10.3 Obligation to Protect Confidential Business Information

Except for information published in **certificate fields**, Comda undertakes to **maintain the confidentiality of the certificate holder's confidential business information** and **not disclose it to any third party**, except as required by law.

8.11 Protection of Personal Information

8.11.1 Privacy Policy

Comda's databases are registered with the **Registrar of Databases** in accordance with the **Protection of Privacy Law, 5741-1981**, and Comda shall operate in accordance with and subject to that law and the guidelines and requirements issued from time to time.

Comda implements a **privacy protection policy**, the updated provisions of which may be obtained at any time.

8.11.2 Information Considered Confidential Personal Information

Any information related to the **identity of the electronic certificate holder** and records relating to the **certificate issuance process**, except for information published in:

- the certificate fields,
- the certificate revocation list (CRL), or

- information disclosed publicly by an authorized party,

shall be considered **confidential personal information**.

8.11.3 Personal Information That Is Not Protected

The contents of the **electronic certificate fields and the certificate revocation list**, even if they contain personal information, shall **not be considered confidential information entitled to protection**.

8.11.4 Obligation to Protect Privacy

Comda undertakes to **maintain the confidentiality of the certificate holder's personal confidential information** and **not disclose it to any third party**, except as required and subject to applicable law.

8.11.5 Disclosure and Consent for Use of Personal Information

Comda shall **not use any personal information** of the electronic certificate holder provided during the certificate issuance process, which is considered confidential, **without the explicit approval and consent of the certificate holder**.

8.11.6 Disclosure of Information Pursuant to Judicial or Administrative Order

Comda shall comply with any **binding order issued by a judicial or administrative authority** requiring disclosure of information, whether personal or business-related, provided by the applicant or certificate holder, including information considered confidential.

To the extent possible, and subject to any restriction or prohibition imposed by the competent authority requesting the disclosure, Comda shall notify the information owner of such disclosure.

If Comda is required to disclose confidential information of the certificate holder within legal proceedings in which Comda is **not a direct party**, or where the certificate holder attempts to prevent disclosure and such action results in **legal or other expenses for Comda**, the certificate holder shall reimburse Comda for the **full amount of such expenses**.

8.11.7 Other Circumstances for Disclosure of Personal Information

Restrictions on the disclosure of confidential information **shall not apply in the case of audits conducted by the Registrar of Databases**.

8.12 Intellectual Property Rights

The intellectual property rights in the **information and data contained in this document and in the structure of the electronic certificate issued by Comda** are the property of Comda.

No use may be made of such materials **without Comda's prior written consent**.

8.13 Representations and Obligations

8.13.1 Representations and Obligations of the Issuing Authority

Comda declares that, during its operation as a certification authority, it shall ensure that:

- the electronic certificate **does not contain any factual misrepresentations known to Comda**;
- the certificate **does not contain transcription errors** resulting from Comda's failure to exercise reasonable care in creating the certificate;
- the certificate **complies with all material requirements of these procedures**;
- any information included in the electronic certificate or incorporated by reference that **has not been verified by Comda** shall remain the **sole responsibility of the certificate holder** with respect to its accuracy and correctness;
- after issuance of a certificate, Comda shall **not have a continuing obligation to investigate or verify the accuracy of the information provided in the certificate application**, unless Comda receives explicit notice that information appearing in the certificate is incorrect and Comda reasonably determines that such notice is reliable.

If it is determined that a certificate **contains factual misrepresentations**, the certificate shall be revoked, and a **new certificate containing updated information may be issued upon request of the certificate holder**.

Comda shall **not be liable for damage caused by reliance on an electronic certificate it issued** if it demonstrates that it took **all reasonable measures to fulfill its obligations under this policy document**. Comda's liability shall be subject to the limitations specified in this chapter.

Without derogating from the foregoing, Comda undertakes to:

- provide the **infrastructure and certificate issuance services**, including establishing, publishing, and operating Comda's repository in a reliable and available manner;

- provide the **controls and foundation of Comda's Public Key Infrastructure (PKI)**, including protection of Comda's keys and the implementation of **secret-sharing procedures** as described in these procedures;
- perform **verification procedures for certificate applications** as specified in these procedures;
- issue certificates in accordance with these procedures and honor the representations made to **certificate holders and relying parties**;
- publish the **certificate revocation repository (CRL)** in a manner that is available, online, and immediate for relying parties;
- fulfill the obligations of a certification authority and **protect the rights of certificate holders and relying parties** in accordance with these procedures;
- revoke certificates when required under these procedures;
- process certificate renewals as specified in these procedures.

8.13.2 Representations and Obligations of Comda Registration Authorities

The provisions set forth in **Section 8.13.1 above** shall apply to Comda's **registration authorities**, insofar as they are relevant to the activities performed by them.

See also **Section 8.24 below**.

8.13.3 Representations and Obligations of the Certificate Holder

The certificate holder is obligated to:

- provide Comda with **complete, accurate, and up-to-date information** necessary for identification and issuance of the electronic certificate for the signature device;
- take **all reasonable measures during the entire validity period of the certificate** to maintain full control over the signature device and prevent unauthorized access or use;
- **immediately notify Comda** upon becoming aware of any compromise of control over the signature device, unauthorized use, or changes in information based on which the certificate was issued, including information contained in the certificate;
- comply with all **obligations, instructions, and warnings** set forth in the subscription agreement.

8.13.4 Representations and Obligations of a Relying Party

A relying party declares and undertakes that, prior to relying on an electronic certificate or the information contained therein, it shall:

- verify that the **electronic certificate is valid**;
- verify the **limitations on the use of the certificate** and confirm that such limitations do not apply to the signed electronic message;
- verify that the **authorized signatory of a corporation or public institution** is indeed authorized to sign on behalf of the organization and bind it by their electronic signature.

A relying party that fails to comply with these obligations shall **bear sole responsibility for any damage or expense** incurred by itself, its representatives, or any third party as a result of reliance on the electronic certificate.

Comda shall **not bear any liability and shall not indemnify or compensate any party** for such damages or expenses.

8.13.5 Representations and Obligations of Other Participating Parties

Not applicable.

8.14 Disclaimer of Warranties and Representations

Comda and/or its representatives do not warrant that certificate holders will not repudiate the certificate or any message; they do not warrant any software other than the technology and software used by Comda for certificate issuance and the device on which the signature key is stored, if such device was supplied by Comda.

They shall not be liable for any damages resulting from reliance on an electronic certificate, provided they demonstrate that they have taken all reasonable measures to fulfill their obligations under this policy document.

Comda and/or its representatives shall not be liable for any **indirect damages** arising from or related to the use of electronic certificates and/or electronic signatures for any purpose whatsoever. Their liability shall apply **only to direct damages** arising naturally and in the ordinary course of events from Comda's failure to fulfill its obligations under this policy document.

Electronic certificates are **not intended for use in hazardous control equipment or in circumstances requiring fail-safe performance**, such as:

- operation of nuclear facilities
- aircraft navigation or communication systems
- air traffic control systems

- weapons control systems
- or any environment where failure could directly lead to death, bodily injury, or environmental damage.

8.15 Limitation of Liability of Comda and Its Representatives

Comda may limit its liability, including limitations relating to:

- the types of uses permitted for a certificate, or
- transaction amounts for which an electronic certificate may be used.

Where such limitations are specified in the electronic certificate, Comda shall **not be liable for damages resulting from use exceeding those limitations**.

Comda may also limit its liability toward a certificate holder in the **subscription agreement**, provided that such agreement does not contradict the provisions of this policy document.

Restrictions on the use of an electronic certificate at the request of the certificate holder shall be implemented **only upon the certificate holder's explicit request**.

Comda may limit its total liability for the use of **secure electronic signatures**, and such limitation shall appear prominently in the electronic certificate and be provided to the certificate applicant prior to issuance. Comda shall publish its liability limitation policy prominently on its website with respect to different types of certificates.

In any event, the **total liability of Comda and/or its representatives toward all parties** (including, but not limited to, an applicant, certificate holder, or relying party) shall not exceed:

- **50,000 NIS** for all secure electronic signatures performed and all transactions related to a particular electronic certificate; and
- **10,000 NIS** for a single secure electronic signature and the transactions related to that individual signature.

The above limitation of damages applies to **all types of loss or damage**, including:

- direct damages
- compensation
- indirect damages
- special damages
- consequential damages

- exemplary damages
- incidental damages

caused to any person, including an applicant, certificate holder, relying party, or any third party, arising from reliance on or use of an electronic certificate issued, managed, suspended, or revoked by Comda, or from reliance on or use of an **expired certificate**.

This limitation applies to **contractual liability, tort liability, and any other liability claims**.

Subject to the above, the liability cap for each electronic certificate shall remain the same **regardless of the number of electronic signatures, transactions, or claims** associated with that certificate.

If claims exceed the liability cap, the cap shall first be allocated to **earlier claims** in order to reach final resolution, unless otherwise ordered by a competent court.

Under no circumstances shall Comda be required to pay an amount **exceeding the total liability cap per certificate**, regardless of how the cap is allocated among claimants.

8.16 Indemnification

Any indemnification obligation shall **not exceed the limitation specified in Section 8.15 above**.

8.17 Validity and Termination of the Policy Document

8.17.1 Validity of the Policy Document

This policy document, and any amendments thereto, shall enter into force and **replace its previous version immediately upon approval and publication** at the issuing authority's address:

http://www.comda.co.il/repository

8.17.2 Expiration of Policies

Comda's policies, as updated from time to time, shall remain valid until replaced by a **new version approved by the management of the issuing authority**.

8.17.3 Consequences of Expiration and Preservation of Validity

Electronic certificates shall be issued **only in accordance with the policy document in force at the time of issuance**.

Certificates shall not be issued under an expired policy document. However, the provisions of an expired policy document shall continue to apply to certificates issued during its validity period.

8.18 Notices

Whenever a party to these procedures wishes or is required to provide notice, demand, or request relating to these procedures, such communication shall be delivered:

- by **electronically signed messages**, consistent with the requirements of these procedures, or
- **in writing**.

Electronic messages shall be considered valid once the sender receives a **valid receipt confirmation** from the recipient. Such confirmation must be received within **five (5) days**, otherwise written notice must be sent.

Written messages to Comda must be delivered via:

- **courier service with written confirmation of delivery**, or
- **registered mail**, to Comda's address.

Notices from Comda or a Registration Authority to another person shall be sent to the **most recently registered address**.

Any Registration Authority of Comda must **immediately notify Comda** of any legal notice received that may affect Comda.

The above shall not apply to:

1. Notice for revocation of an electronic certificate (Section 4.9).
2. Notice for scheduling certificate issuance (Section 4.1.2).
3. Notice regarding certificate expiration and the possibility of telephone renewal (Section 4.6).

8.19 Changes and Amendments

8.19.1 Procedures for Making Changes

Amendments to this policy document may be made through **partial updates**.

Where partial updates are made, the **approval date of each amendment** shall be published alongside the change to allow tracking of its effective period.

Amendments shall take effect **upon publication**, but shall not impose additional obligations on holders of certificates issued under a previously valid policy document, as long as their certificate remains valid.

Certificate holders shall have **60 days from the publication date** of an updated version to submit:

- objections
- corrections
- comments

for Comda's consideration. Comda shall provide **written responses** to all submissions received within this period.

Comments received **after 60 days** from publication shall not be considered.

8.19.2 Publication of Changes

The updated version of the policy document shall be published at:

http://www.comda.co.il/repository

8.19.3 Circumstances for Changing the Object Identifier (OID)

Changes to this policy document **do not require a change to the Object Identifier (OID)**.

8.20 Dispute Resolution

Before initiating any dispute resolution mechanism (including litigation or arbitration) concerning any aspect of these procedures or an electronic certificate issued by Comda, affected parties shall notify:

- Comda
- the Registration Authority
- and any other party involved in the dispute

in order to attempt resolution among themselves.

8.21 Governing Law

These procedures are drafted in accordance with the **laws of the State of Israel**, without regard to conflict-of-law rules or the requirement to demonstrate a commercial connection to Israel.

These procedures shall be governed by the **laws of the State of Israel**.

The choice of governing law is intended to ensure **uniform procedures and interpretation for all users**, regardless of their place of residence or use of their certificates.

Comda declares that these procedures were prepared in accordance with **ETSI TS 456** and **CA/Browser Forum requirements**.

8.22 Compliance with Laws

These procedures are subject to the **laws of the State of Israel**.

8.23 Miscellaneous

8.23.1 Entire Agreement

These procedures replace any prior version, and **no other version, written or oral, explicit or implied, shall have any validity**, except as provided in these procedures, as amended from time to time.

8.23.2 Assignment of Rights and Obligations

Comda may **assign its rights and/or obligations under these procedures to another party**.

8.23.3 Conflicting Provisions

In case of conflict between:

- the **subscription agreement** and this policy document – the provisions of **this document shall prevail**.
- an **updated policy document** and a previous version – the **updated policy shall prevail**.

8.23.4 Enforcement

These procedures are binding on:

- the issuing authority and its representatives
- certificate holders
- authorized representatives
- relying parties
- and all parties acting on their behalf.

No waiver, delay, extension, or failure to act by Comda or the certificate holder shall be interpreted as a waiver of rights under these procedures.

Section headings follow the **RFC 3647 standard** and are provided for convenience only. They shall not be used for interpretation or enforcement of these procedures.

Unless otherwise specified, these procedures shall be interpreted **in a commercially reasonable manner**, taking into account their international scope and the benefits of consistent interpretation and good faith.

8.23.5 Force Majeure

Comda and its representatives shall not be liable for any breach, delay, or failure to perform under these procedures due to events beyond their control, including:

- force majeure
- wars
- states of emergency
- pandemics
- power outages
- fires
- earthquakes
- other disasters

provided that Comda could not reasonably have prepared for such events.

8.24 Additional Arrangements – Registration Authorities

8.24.1 Introduction

Some certificate issuance services provided by Comda may be performed through **authorized representatives**.

Such representatives shall be **approved by Comda prior to their appointment as Registration Authorities (RA)**.

They operate under Comda's discretion and participate in:

- processing certificate applications
- identifying applicants

- registering applicants.

Representatives must comply with all requirements specified in these procedures.

8.24.2 Application to Act as a Comda Registration Authority

Any **individual, corporation, or public institution** wishing to act as a Registration Authority for Comda must submit a **signed application verified by an attorney**.

Applications that are not verified or incomplete shall not be processed.

The application must include, among other details:

- Name, address, fax and telephone numbers, email addresses of the applicant, administrative contacts, and authorized representatives.
- Information demonstrating the applicant's **reliability**, including financial status (e.g., insolvency past or present).
- Certified copies of the **certificate of incorporation**, corporate documents, and resolutions authorizing appointment as a Comda Registration Authority.
- Attorney confirmation regarding the corporation's activities and authorized representatives.
- A declaration confirming the applicant's ability to **comply with these procedures**.
- Any additional information required by Comda.

The applicant's representative shall perform all required actions and sign all documents necessary for approval.

8.24.3 Address for Submitting Applications

Applications to act as a Comda Registration Authority, including all required information and attorney verification, shall be submitted to **Comda's offices**, which shall review the application and determine whether to grant final approval.