Comsign Europe LTD

Certification Practice Statement (CPS)

In the framework of providing Electronic Certificates issuance services complying with the requirements of the eIDAS regulation

Version 1.3

Date of publication of this version: 15.07.2026

Comsign Europe LTD.

Copyrights Notice

Comsign's Address:

Email: info@Comsigntrust.com

Table of Contents

Version No.	Date of change	Main changes updated
1.0	1/1/2023	
1.1	30/07/2024	• Clearing PKI participants • Clearing PKI hierarchy • Adding the Comsign Europe OID • Adding ECC algorithm • General Review
1.2	**13.08.2024**	• Review of the certificates on the scope of the CPS • Removing remote Identification
1.2	01.05.2025	• General Review
1.2	21.06.2026	• General Review
1.3	15.07.2026	• OID uodates

1. Introduction

Comsign Europe Ltd. is a certification authority operating in accordance with the eIDAS regulation (Regulation [EU] 910/2014). In this capacity, Comsign validates the identity of the Applicant applying for an Electronic Certificate, which is an electronic confirmation of the validity of the Electronic Signature and the correctness of its details and issues the Certificate.

The PKI infrastructure is managed by Comsign Israel on behalf of Comsign Europe. In this document Comsign Europe is referenced as Comsign.

This CPS regulates the provision of Comsign's Electronic Certificate issuing services, which comply with the eIDAS regulation and its usage, including identification and authentication [chapter 3], issuance, revocation, and renewal of Certificates [chapter 4], physical security [chapter 5], logical security [chapter 6], Certificate profile and Certificate Revocation List (CRL) [chapter 7].

The legal engagement between Comsign and the Applicant requires the signing of a Subscriber Agreement and Terms & Conditions.

This document conforms to the RFC 3647 standard. Comsign further confirms that it conforms to ETSI EN 319 411 - 2 standard and the current version of the Baseline Requirements of the CA-Browser Forum.

1.1 Overview

The Electronic Certificates services of Comsign support secured e-commerce and other electronic services and answer technical, business and private needs of users of Electronic Signatures. Comsign is a Certification Authority and acts as a trustworthy third party which issues, manages and revokes Electronic Certificates according to these Procedures.

These Procedures describe and regulate the process of issuing Electronic Certificates from beginning to end, and processes and services relating to issuing and managing of Electronic Certificates. Comsign and its representatives apply these Procedures when issuing and managing Electronic Certificates.

Comsign acts as a third party that verifies the connection between a certain Electronic Signature and the signer by an Electronic Certificate - an electronically signed message issued by Comsign as a Certification Authority, validating that the Signature Verification Device (as defined below) belongs to the holder of the Electronic Certificate.

The Certificate issuance services include application and registration, adequate Applicant identification, issuance, revocation, and documentation of the actions carried out by Comsign. Revocation of Certificates is carried out only in cases mentioned in Clause 4.9.1 of this CPS, in accordance with the eIDAS Regulation (Regulation [EU] 910/2014),

The certificate types addressed in this CPS are the following:

Name	Details	Comments
Comsign Europe N1 Root CA	Root CA	
Comsign Europe S1 Root CA	Root CA	
Comsign Europe CS1 Root CA	Root CA	
Comsign Europe Intermediate N1 CA	SubCA	An Intermediate CA in Comsign PKI Hierarchy that issues certificates according the eIDAS regulation
QSIG Certificate	Qualified level end user certificate for natural persons	A Qualified certificate issued to a natural person (/on behalf an organization) according to the eIDAS regulation
Signature Certificate	End user certificate for natural persons	A certificate issued to a natural person
QSEAL Certificate	Qualified level end user certificate for legal persons	A Qualified certificate issued to a legal person according to the eIDAS regulation

Seal Certificate	End user certificate for legal persons	A certificate issued to a legal person
QWAC Certificate	SSL QWAC certificate according to EIDAS	A Qualified SSL Certificate issued according to the eIDAS regulation and according to the BR as published by the CAB/F

1.2 Document name and identification

This document, referred to as the Procedures or CPS, is available at the following address: http://www.Comsign.co.il/repository.

The OID of the document is 1.3.6.1.4.1.61201.2.1.

Comsign Europe uses OID arcs for the various certificates and documents described in this CPS as follows:

QSIG: 1.3.6.1.4.1.61201.1.1 issued with a QSCD (ETSI policy): 0.4.0.194112.1.2 according to this CPS.

QSEAL: 1.3.6.1.4.1.61201.1.1 issued with a QSCD (ETSI policy): 0.4.0.194112.1.3 according to this CPS.

QWAC: 1.3.6.1.4.1.61201.1.1 issued to a natural or legal person (ETSI policy): 0.4.0.194112.1.4 according to this CPS.

CAB/F Compliant SSL Certificates:

Domain Validation: 1.3.6.1.4.1.61201.1.2.1 CAB\F policy: 2.23.140.1.2.1 according to this CPS.

Organizational Validation: 1.3.6.1.4.1.61201.1.2.2 CAB\F policy: 2.23.140.1.2.2 according to this CPS.

1.3 PKI participants

1.3.1 Certification Authorities:

Comsign is a Certification Authority (CA). The Procedures of Comsign are based on the eIDAS regulation and international standards. Comsign does not cross-sign certificates.

1.3.2 Registration Authority:

Comsign's certification services are organized in a manner that enables the handling of applications for certificates, identification of applicants and their registration by an authorized Registration authority appointed by Comsign. The Registration authority shall abide by these Procedures and the instructions of Comsign. The Registration authority is subordinated to Comsign, and although bound by a specific responsibility as part of its appointment, Comsign remains liable for the Registration authority's activities. This ensures the uniformity of the services provided by Comsign and its agents.

1.3.2.1 Additional requirements from a Registration Authority for electronic certificates issued to internet servers:

Comsign may perform the activities listed in clause 3.2 below dealing with the issuance of electronic certificates to internet servers employing the services of a Registration Authority subject to the fulfillment of all the requirements listed in clause 3.2 below as well as all these Procedures *mutatis mutandis*.

1.3.3 Subscribers:

See definition in article 1.6 below.

1.3.4 Relying Parties:

See definition in article 1.6 below.

1.3.5 Other participants:

1.3.5.1 Comsign registration and verification clerks:

Comsign's representatives receiving the applications of the Certificate Applicants, filling in their personal details, verifying and confirming their identity, issuing the Certificate, and finally, verifying that the Certificate operates properly. Upon completion of the above, collecting the payment and issuing an invoice and a receipt. In case of a Certificate revocation, verifying the identity of the person requesting the revocation and carrying out the request.

1.3.5.2 Applicant's representative:

The Applicant's representative must be a natural person. The identity of the Applicant's Representative is verified in accordance with these Procedures.

1.4 Certificate usage

1.4.1 Appropriate Certificate usages:

An eIDAS Qualified Certificate or CAB/F compliant SSL certificate issued in accordance with this CPS, and/or the eIDAS Regulation and/or the CAB/F requirements may be issued to a natural or legal persons. The use of that certificate is the sole responsibility of the Subscriber and may be used for legal purposes only.

1.4.2 Prohibited Certificate usages:

Subscribers are exclusively responsible to the legality of the information they provide and present, and to the usages of the Certificates issued in accordance with this CPS in any jurisdiction in which the contents of the Certificates are available or reviewed. Thus, Applicants and Subscribers shall be aware of the existence of different laws regarding data transmission, especially encoded data or such that include encryption algorithms, and the fact that such laws may be significantly different from each other in different countries. Additionally, in most cases, it is nearly impossible to limit the distribution of content on the Internet or in certain networks based on the location of the user\observant. Thus, Applicants and Subscribers shall follow the laws in any jurisdiction in which the Certificate is used, or its contents are available.

1.5 Policy administration

1.5.1 Organization administering the document:

The party at Comsign who is responsible for the implementation of the CPS is the Security Forum that includes the CEO and the Security Officer and MAY include other relevant personnel (IT team manager, legal counsel, etc.).

1.5.2 Contact person:

The person in charge of the application of the policy and the Procedures at Comsign is the Security Officer. E-mail address: security@Comsigntrust.com

Information concerning qualified Electronic Certificates and assistance is available by email: support@Comsigntrust.com

The person determining CPS suitability for the policy: The CA manager is the party in charge of adapting the Procedures to the policy of the CA.

1.5.3 CPS Procedures approval:

These Procedures were prepared in accordance with the eIDAS regulation (Regulation [EU] 910/2014)

1.6 Definitions and terms:

In this CPS, the following terms shall have the meaning mentioned next to them:

Applicant	A natural person, a corporation, or a public institution that submits a request for issuing an Electronic Certificate, as described in chapter 4 below.
Application	The process by which the Applicant (as defined above) requests that an Electronic Certificate be issued.
Attestation Letter	A certified public accountant, lawyer, government official, or other reliable third party customarily relied upon for such information's letter attesting that Subject Information is correct.
Authorized Port	One of the following ports: 80 (http), 443 (http), 115 (sftp), 25 (smtp), 22 (ssh).
CAA Record	A Certification Authority Authorization (CAA) record is used to specify which certificate authorities (CAs) are allowed to issue certificates for a domain.
CA/B Forum	Certificate Authority / Browser Forum – an international forum
Device or Hardware Device	Smart card, token, HSM or any other hardware component used to create and secure the Signature Device.
Domain Authorization Document	Documentation provided by, or a CA's documentation of a communication with, a Domain Name Registrar, the Domain Name Registrant, or the person or entity listed in WHOIS as the Domain Name Registrant (including any private, anonymous, or proxy registration service) attesting to the authority of an Applicant to request a Certificate for a specific Domain Namespace.
Domain Contact	The Domain Name Registrant, technical contact, or administrative contract (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record.
Domain Name Registrant	Sometimes referred to as the "owner" of a domain name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a domain name is used, such as the natural person or legal entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.
Domain Name Registrar	A person or entity that registers domain names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national domain name authority/registry, or (iii) a network information center (including their affiliates, contractors, delegates, successors, or assigns).
eIDAS	(Regulation [EU] 910/2014)
Electronic Signature or Qualified Electronic Signature	Qualified Electronic Signature as defined by eIDAS.

FQDN	A fully qualified domain name (FQDN) is the complete domain name for a specific computer, or host, on the Internet. The FQDN consists of two parts: the hostname and the domain name.
Internal Name	A string of characters (not an IP address) in a Common Name or Subject Alternative Name field of a Certificate that cannot be verified as globally unique within the public DNS at the time of certificate issuance because it does not end with a Top-Level Domain registered in IANA's Root Zone Database.
Key (private, public) or Pair of Keys	A private key and its associated public key connected by a single-value correspondence in accordance with accepted methods of encryption as part of the public key infrastructure.
ICANN	Internet Corporation for Assigned Names and Numbers - Oversees the huge and complex interconnected network of unique identifiers that allow computers on the Internet to find one another.
The Parties	Comsign, its representatives and the Certificates users, namely the Subscriber and the relying party.
The Procedures or these Procedures	The Procedures detailed below for regulating the activities of Comsign as a Certification Authority. These Procedures apply only to the Certificates (as defined below).
Representative of Comsign	A party external to Comsign that was appointed by Comsign as a Registration authority for the purpose of registering and identifying Applicants and handling applications for the issuance of Electronic Certificates.
Revoked Certificate	A Certificate that appears on the Certificates Revocation List (CRL) in the Comsign Repository.
Reliable Data Source	An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate.
Relying Party	A third party who receives a message signed with a Qualified Electronic Signature and acts or refrains from action based on the Qualified Electronic Signature and/or on information found in Comsign's Repository.
Signature Device	Unique software, object or information required for creating a secure Electronic Signature. A Signature Device is used to produce a qualified electronic signature. A Signature Device is unique to its owner and kept confidential by its owner.
Signature Verification Device	Unique software, object or information required for verifying that a secure Electronic Signature was created using a specific Signature Device. A Signature Verification Device has a single value correspondence with the signature device. A particular Signature Verification Device is used to identify a secure electronic signature as one produced by a particular Signature Device. It is possible to make the Signature Verification Device available to the public for the purpose of such verification.
Subscriber	An Applicant to whom an Electronic Certificate was issued.

Technically Constrained Subordinate CA	A Subordinate CA's certificate which uses a combination of Extended Key Usage settings and Name Constraint settings to limit the scope within which the Subordinate CA Certificate may issue Subscriber or additional Subordinate CA Certificates.
Valid Certificate	A Certificate that appears on the list of valid Certificates in the Comsign Repository
WebTrust	The current version of CPA Canada's WebTrust Program for Certification Authorities.
X.509	X.509 is a format for certified Public Key's, which are suitable for use in various Public Key Infrastructure systems.

2. Publication and Repository Responsibilities

The purpose of this chapter is to review the ways in which Comsign publishes relevant information to the public, to relying parties, Subscribers and Applicants, as applicable. This chapter relates to the types of information published, the frequency of publication, and ways of accessing the Comsign Repository.

Comsign shall develop, implement, enforce, and update these Procedures in accordance with the requirements of the eIDAS regulation (Regulation [EU] 910/2014), the latest requirements of the CA/Browser forum and any other relevant practices and requirements.

2.1 Repositories

To conduct its business, Comsign maintains repositories for storage and retrieval of Certificates and other related information, known together as the Repository. Comsign's Repository includes, inter alia, the following sub-repositories:

(i) a database of valid Electronic Certificates (including Comsign's Certificate) issued to domain names and details of the verification checks Comsign performed prior to the issue of each electronic certificate to any domain name or IP address,

(ii) (ii) a database of revoked Certificates that includes information on the revocation of Certificates, lists of revoked Certificates and other information as Comsign may determine from time to time.

Only part of the information stored in Comsign's Repository is accessible to the public. Access to the lists of revoked Certificates, their serial number and date of revocation is granted freely and publicly subject to certain limitations and controls.

Comsign's repositories are GDPR compliant (the EU General Data Protection Regulation).

2.2 Publication of certification information

In the framework of Comsign's Repository, Comsign shall publish a list of Revoked Certificates, updates of the Procedures and other information corresponding to these Procedures.

The above information is published on Comsign's website and includes updates of the CPS and the due date of its validation.

Comsign hosts test Web pages with signed SSL certificates that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to Comsign's Root Certificate.

These test Web pages are as follows:

(1) A valid Subscriber certificate: https://fedir.comsigntrust.com/test.html

(2) A revoked Subscriber certificate: https://revoked.comsign.co.uk/test.html

(3) An expired Subscriber certificate: https://expired.comsign.co.uk/test.html

Concerning certificates for authenticating servers accessible through the Internet, Comsign conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates (for QWAC certificates the requirements in the BR shall apply as published at http://www.cabforum.org. In the event of any inconsistency between this document and those Requirements those Requirements take precedence over this document.

2.3 Time or frequency of publication

Comsign shall publish a new list of Revoked Certificates no later than every 12 hours or immediately after a Certificate is revoked. The published list of Revoked Certificates is valid for 24 hours. The published list is available at: https://www.comsign.co.il/repository

For the avoidance of doubt, the updated and valid list of Revoked Certificates is the one appearing in Comsign's Repository. The Relying Party should perform a new online examination of the Revoked Certificates in the Repository every time reliance on a Certificate is needed to ensure that the examination is based on the updated list of the Revoked Certificates.

Changes in the CPS shall be published no less than once a year.

2.4 Access controls on Repositories

Free access to the Repository from Comsign's website is available to sections open to the public. The address of the Revoked Certificates Repository is https://www.comsign.co.il/repository. Access to other sections of the Repository is restricted, except to access authorized individuals according to Comsign's Procedures.

3. Identification and Authentication

The purpose of this chapter is to review the requirement for physical presence (when applicable or mandatory), the process of identifying and verifying the identity of the Applicant, the documents that the Applicant shall present, verification of the application, instances in which the application is rejected, and the process for identifying the Subscriber for purposes of revocation or re-issuance.

While applying for a certificate for a natural person the Identification and Authentication shall be performed according to the sections below concerning Natural persons

While applying for a certificate for a Legal person (Qwac/Q/Seal etc.) the Identification and Authentication shall be performed according to the sections below concerning legal persons and organizations.

While applying for Qwac – the requirements listed in the BR shall be met including role separation.

3.1 Naming

3.1.1 Types of names:

The name of the Subscriber is stated in the Certificate according to standard X509. It is possible to issue several Certificates for different authorized signatories in the same corporation and\or public institution, provided that this issuance is carried out according to this CPS. It is also possible to issue several different Electronic Certificates to the same Applicant for their different positions. When a Subscriber holds multiple electronic certificates, the Subscriber is obligated to inform the Registration authority to that effect at the time the person is issued an electronic certificate and to confirm that the person was cautioned of the risks resulting from possessing multiple electronic certificates and the person's duty to fulfill the requirements of exclusive control over his numerous signature's means.

3.1.2 Need for names to be meaningful:

The name of the Subscriber shall be meaningful. Namely, the name shall refer to a person or a registered corporation/public institution in a manner that prevents mistakes in identifying or referring a Certificate to its owner.

3.1.3 Anonymity or pseudonymity of Subscribers:

Comsign shall not issue an Electronic Certificate bearing a nickname of the Subscriber or one that does not state the name of the Subscriber. Notwithstanding, at the explicit request of the Applicant, Comsign may issue an electronic certificate bearing the Subscriber's nickname in parenthesis adjacent to the Subscriber's registered first name stating that this is a nickname.

This exclusion does not apply to electronic certificates issued to domains and internet servers.

3.1.4 Rules for interpreting various name forms:

To ensure that the data included in an electronic certificate is unique to the Subscriber, including the use of Distinguished Names (DN) and represents unique values that can be verified in accordance with international standards, Comsign employs the X.500 standard, and all its derivatives.

3.1.5 Uniqueness of names:

The Certificate enables a unique identification of the Subscriber using a unique identity marker. In a personal Certificate - the ID number of the Subscriber (or its equivalent). In a corporate Certificate - the registration number of the corporation (or its equivalent). In certain cases, other or additional identity markers such as the number of a professional license, a VAT number etc., may be used.

3.1.6 Recognition, identification and role of trademarks:

Applicants and Subscribers warrant to Comsign and/or to its representatives that the details in the application for issuing a Certificate do not impair or violate the rights of any third party, in any jurisdiction, with respect to trademarks, service marks, trade names or any other intellectual property. They further warrant that they will not use any of these details for any illegal purpose including, but not limited to, causing a breach of contract or other illegal intervention in contractual relationships, unfair competition, damage to the reputation of another and misleading any person, corporation or legal entity.

Comsign and its representatives shall not be held accountable for details included in the Certificate that were reported by the Applicant or by the Subscriber to Comsign, its representative, or to its Repository or provided by the Applicant or by the Subscriber in any other manner, nor to any violation of a law or any third party's right resulting from its inclusion in the Certificate.

Email addresses provided by the Applicant to be included in the electronic certificate (other than for SSL certificates) are not verified by Comsign in any manner and for any purpose and relying on these email addresses is at the sole risk of the relying party.

3.2 Initial Identity Validation

3.2.1 Method to prove possession of a private key:

An Electronic Certificate for natural persons shall not be issued to a person not possessing a private key that fulfills the following requirements:

(1) The private key is based on an accepted standard that uses one of these:
   (a) A minimum 2,048-bit RSA or DSA key;
   (b) A minimum 224-bit elliptic curve DSA key;
(2) Unique physical or cryptologic QSCD that meets at the least FIPS 140-2 level 2 or common criteria EAL2 standards are required to operate or access the private key.
(3) If operating the private key requires a password, the password shall comply with EU standards.

Proof of possession is achieved by generating the Key Pair concurrently with the issue by Comsign of the Electronic Certificate within the hardware device storing the electronic certificate. If the hardware device was not supplied by Comsign, the electronic certificate shall be issued subject to the Subscriber's signed written declaration stating that the device meets the above requirements.

3.2.2 Authentication of organization identity:

The identification of an Applicant/authorized person on behalf of a corporation as described in this Clause shall be performed by two Comsign registration clerks, based on face-to-face identification, as required and allowed by the eIDAS regulations, as described below.

A corporation registered in the EU:

on the basis of: the incorporation certificate; an attorney's statement confirming the existence of the corporation, its name and registration number, or in lieu of the statement – by verification in the appropriate registries; a certified copy of a resolution of an authorized body in the corporation stating the authorized signatory on behalf of the corporation or an attorney's statement regarding the identity of the said authorized signatory, using the text published on the Internet site of Comsign from time to time.

A corporation not registered in the EU.

on the basis of: a certified copy of a document confirming that the corporation is incorporated; a statement of an attorney confirming the existence of the corporation, its name and registration number, or in lieu of the statement – by verification in the appropriate registries; a certified copy of a resolution passed by the authorized bodies of the corporation regarding the authorized signatories on behalf of the corporation or an attorney's statement regarding the identity of the said authorized signatories, using the text published on the Internet site of Comsign from time to time.

.

3.2.2.1 Identity verification when issuing an electronic certificate to an organization server:

Comsign shall verify the identity and address of the Applicant using at least one of the following:

(1) A government database in the jurisdiction of the Applicant's legal creation, existence, or recognition;

(2) A third-party database that is periodically updated and considered a reliable data source;

(3) A site visit by a Comsign employee or representative; or

(4) An attestation letter signed by a lawyer, CPA or a government official.

Alternatively, Comsign may verify the address of the Applicant (but not the identity of the Applicant) using a utility bill, bank statement or other form of identification that Comsign determines to be reliable.

If the Applicant requests a certificate that will contain subject identity information comprised only of the countryName field, then Comsign shall verify the country associated with the subject using a verification process described in Clause 3.2.2.3. If the Applicant requests a certificate that will contain the countryName field and other subject identity information, Comsign shall verify the identity of the Applicant, and the authenticity of the Applicant representative's certificate request using a verification process described in Clause 3.2.2.1. Comsign shall inspect any document relied upon under this Clause for alteration or falsification.

3.2.2.2 Verification of use of Business Name/Tradename by a server or for Q/Seal:

In the event of QWAC issuance the verification shall be performed by two clerks to ensure security and separation of duties and the process shall comply with the BR by the CAB\F.

If the subject identity information is to include a business or trade name, Comsign shall verify the Applicant's right to use the business name/tradename using at least one of the following:

(1) Documentation provided by, or communication with, a government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;

(2) A reliable data source;

(3) Communication with a government agency responsible for the management of such business names or tradenames;

(4) An attestation letter by a lawyer, CPA or government official; or

(5) A utility bill, bank statement or other form of identification determined as reliable by Comsign.

3.2.2.3 Verification of Country Name in an electronic certificate for a server or for Q/Seal

If the subject: countryName field is present, Comsign shall verify the country associated with the Subject using one of the following:

(1) the IP address range assignment by country for either:

(a) the web site's IP address, as indicated by the DNS record for the web site or
(b) the Applicant's IP address;

(2) The ccTLD of the requested domain name;

(3) Information provided by the domain name registrar; or

(4) A method identified in Clause 3.2.2.1.

Comsign shall attempt to screen proxy servers to prevent reliance upon IP addresses assigned in countries other than where the Applicant is located.

3.2.2.4 Validation of Domain Authorization or Control in an electronic certificate for a server

For issuing certificates to organizations requesting SSL certificates, Comsign performs domain name owner's verification to detect cases of homographic spoofing of IDNs. Comsign employs a process to find the owner of a particular domain. A search failure result is flagged, and the RA rejects the Certificate Request.

Orders for major corporations, well known trademarks and financial institutions shall be reviewed with special care and queued until full review is completed.
In the event an order is queued for review, the administrative contact shall be a full-time employee of the company for successful issuance. Verification methods include one of the following:

(1) Validating the Applicant as a Domain Contact

Confirming the Applicant's control over the FQDN by validating the Applicant is the Domain Contact directly with the Domain Name Registrar. For this method, Comsign shall also authenticate the Applicant's identity as specified in Clause 3.2.2.1 and the authority of the Applicant representative under Clause 3.2.5.

(2) Email, Fax, SMS, or Postal Mail to Domain Contact

Confirming the Applicant's control over the FQDN by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value. The Random Value shall be sent to an email address, fax/SMS number, or postal mail address identified as a Domain Contact.

The Random Value shall be unique in each email, fax, SMS, or postal mail.

The Random Value shall remain valid for use in a confirming response for no more than 30 days from its creation.

(3) Constructed Email to Domain Contact

Confirming the Applicant's control over the requested FQDN by:

(a) sending an email to one or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at-sign ("@"),

followed by an authorization domain name,

(b) including a Random Value in the email, and

(c) Receiving a confirming response utilizing the Random Value.

The Random Value shall be unique in each email.

The Random Value shall remain valid for use in a confirming response for no more than 30 days from its creation.

(4) Domain Authorization Document

Confirming the applicant's control over the requested FQDN by relying upon the attestation to the authority of the applicant to request a certificate contained in a Domain Authorization Document). The Domain Authorization Document shall substantiate that the communication came from the domain contact. Comsign shall verify that the Domain Authorization Document was either:

(a) Dated on or after the date of the domain validation request or

(b) That the WHOIS data has not materially changed since a previously provided Domain Authorization Document for the Domain Name Space.

(5) Agreed-Upon Change to Website

Confirming the applicant's control over the requested FQDN by confirming one of the following under the "/.well-known/pki-validation" directory, or another path registered with IANA for the purpose of domain validation, on the authorization domain name that is accessible by Comsign CA via HTTP/HTTPS over an Authorized Port:

(a) The presence of Required Website Content of at least 112 bites provided by the CA to the Applicant contained in the content of a file or on a web page in the form of a meta tag, or

(b) The presence of the request value generated in a manner as instructed by the CA and linking it to the key of the application for the electronic certificate. The request value may contain a date-time stamp as well as any other unique data.

(6) DNS Change

Confirming the Applicant's control over the requested FQDN by confirming the presence of a Random Value or Request Token in a DNS TXT or CAA record for an authorization domain name or an authorization domain name that is prefixed with a label that begins with an underscore character.

(7) IP Search

Confirming the Applicant's control over the requested FQDN by confirming that the reply to a DNS search for A or AAAA records complies with Section 3.2.2.5.

(8) TLS Using a Random Number

Confirming the Applicant's control over the requested FQDN by confirming the presence of a Random Value within a certificate on the authorization domain name which is accessible by Comsign via TLS over an authorized port.

3.2.2.5 Authentication for an IP Address

For each IP Address listed in a Certificate, Comsign shall confirm that, as of the date the Certificate was issued, the Applicant has control over the IP Address by:

(1) Having the Applicant demonstrate practical control over the IP Address by making an agreed-upon change to information found on an online Web page identified by a uniform resource identifier containing the IP Address;

(2) Obtaining documentation of IP address assignment from the Internet Assigned Numbers Authority (IANA) or a Regional Internet Registry (RIPE, APNIC, ARIN, AfriNIC, LACNIC);

(3) Performing a reverse-IP address lookup and then verifying control over the resulting Domain Name under Clause 3.2.2.4.

3.2.2.6 Wildcard Domain Validation

Before issuing a certificate with a wildcard character (*) in a CN or subjectAltName of type DNS-ID, Comsign shall follow a procedure that determines if the wildcard character occurs in the first label position to the left of a "registry-controlled" label or "public suffix".

If a wildcard falls within the label immediately to the left of a registry-controlled or public suffix, Comsign shall refuse issuance unless the Applicant proves its rightful control of the entire Domain Namespace. To determine what is "registry-controlled" versus the registerable portion of a country code Top-Level Domain Namespace Comsign shall consult a "public suffix list" such as http://publicsuffix.org.

3.2.2.7 Data Source Accuracy

Prior to using any data source as a Reliable Data Source, ComSign shall evaluate the source for its reliability, accuracy, and resistance to alteration or falsification. ComSign shall consider the following during its evaluation:

(1) The age of the information provided,

(2) The frequency of updates to the information source,

(3) The data provider and purpose of the data collection,

(4) The public accessibility of the data availability, and

(5) The relative difficulty in falsifying or altering the data.

3.2.2.8 CAA Records

As part of the issuance process, Comsign shall check for a CAA record for each dNSName in the subjectAltName extension of the certificate to be issued, according to the procedure in RFC 6844, following the processing instructions set down in RFC 6844 for any records found.

If Comsign issues the Certificate, the issuance shall be done within the TTL of the CAA record, or 8 hours, whichever is greater.

When processing CAA records, Comsign shall process the issue, issuewild, and iodef property tags as specified in RFC 6844.

Comsign shall respect the critical flag and not issue a certificate if this flag has an unrecognized property set.

Comsign shall not issue a certificate unless either:

(1) the certificate request is consistent with the applicable CAA Resource Record set or

(2) an exception specified in the relevant Certificate Policy or Certification Practices Statement applies. These exceptions can be only one of the following:

(a) CAA checking is optional for Certificates for which a Certificate Transparency pre-certificate was created and logged in at least two public logs, and for which CAA was checked.
(b) CAA checking is optional for Certificates issued by a Technically Constrained Subordinate CA Certificate where the lack of CAA checking is an explicit contractual provision in the contract with the Applicant.
(c) CAA checking is optional if Comsign or an affiliate of Comsign is the DNS Operator (as defined in RFC 7719) of the domain's DNS.

Comsign shall treat a record lookup failure as permission to issue only in case of all the following:

(a) The failure is outside Comsign's infrastructure;

(b) The lookup has been retried at least once; and

(c) The domain's zone does not have a DNSSEC validation chain to the ICANN root.

Comsign shall document potential issuances that were prevented by a CAA record in sufficient detail to provide feedback to the CA/Browser Forum on the circumstances.

3.2.3 Authentication of individual identity (for Qsig/Q/Seal):

Identification of an individual Applicant for a personal or corporate Certificate pursuant to this Clause shall be carried out by two registration clerks of Comsign, based on face-to-face identification, as described below:
An individual Applicant who is a resident of the EU – based on an identity card (or its equivalent) with the addition of one of the following documents (two different documents, both with a photograph, are required for the identification process):

(1) A valid EU passport; or

(2) A valid EU driving license which includes a photo; or

(3) Another legally binding identifying document issued by a public authority, provided that this document includes a photograph of the Applicant and their identity number (or equivalent).

In the case the Applicant does not possess one of the documents listed above – an affidavit stating the lack of any one of the documents listed above and, in addition, a statement by an attorney verifying the Applicant's identity and that the attorney knows the Applicant personally, accompanied by a picture of the Applicant signed by the attorney.

Whenever possible, the above identity information shall be verified vis-à-vis information received from public records that contain corroborating data;

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

Identification of an Authorized Signatory on behalf of a natural person - As per the request of an Applicant who is a natural person and who has authorized another natural person as their authorized signatory to act in their name and on their behalf, together with an attorney's confirmation of the said authorized signatory, using the text published on the Internet site of Comsign from time to time. The CA shall validate the identity of the authorized signatory as an EU resident or non-resident in the manner detailed in Clause 3.2.3 above.

3.2.4 Non-Verified Subscriber information:

Comsign shall not issue an Electronic Certificate to an Applicant whose identity or the identity of the Subscriber cannot be verified or was not verified by Comsign.

3.2.5 Validation of authority:

Comsign shall not issue an Electronic Certificate to a corporation representative without ensuring that the Applicant has been authorized by the corporation (or an individual, if applicable) to act on its behalf and that the representative was lawfully authorized by the corporation to act and sign on its behalf. The date upon which the corporation's authorization was issued cannot be dated more than 3 months prior to the issuance of the electronic certificate unless authorized by the CA's manager or another authorized entity.

3.2.6 Criteria for interoperation:

Comsign performs and manages issuance using solely the Comsign Issuance system and does not rely on issuances carried out by any external organization.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and authentication for routine re-key:

Comsign shall offer a remote renewal service of an Electronic Certificate issued by it to the Subscriber prior to its expiration upon a telephone request of the Subscriber or by its initiative. The Subscriber's telephone request shall take place within 1-60 days prior to the termination date of the Certificate's validity. A renewal initiated by Comsign can be executed no later than 24 hours prior to termination of Certificate's validity. The renewal is conditioned upon verifying the Subscriber's identity against its details as recorded in Comsign's repository and correctly answering a challenge question that was defined at the time of the Certificate's issuance. In addition, the Subscriber shall identify himself to the device on which the Certificate is installed and follow the instructions of the issuer. In case the remote renewal process fails or does not work for any given reason up to the expiration date of the Certificate, a new Certificate shall be issued using the routine identification process, including identification of the Applicant in the manner applicable to a first-time issue of an Electronic Certificate.

3.3.2 Identification and authentication for re-key after revocation:

A Revoked Certificate cannot be renewed. A new issuance process is required.

3.4 Identification and authentication of revocation requests

Comsign shall revoke a Certificate upon the Subscriber's request after receiving the request and verifying that the person requesting the revocation is indeed the Subscriber or his\her representative. Two clerks shall handle the

revocation process. Identification of the Subscriber asking to revoke his\her Electronic Certificate shall be performed in one of the following ways:

(1) Using a revocation code set by the Subscriber when the application for issuing the Certificate was submitted. A representative of Comsign shall verify the correctness of the revocation code by entering it into the relevant system and receiving a correct/incorrect signal.

(2) If the Subscriber did not set a revocation code or does not remember it, a representative of Comsign and/or someone on its behalf shall call the telephone number that the Subscriber entered on the Certificate application for purposes of ascertaining that the owner of the Certificate is indeed the one requesting its revocation and confirm the details of the person making the revocation request by using the personal details that were entered in the application of the Certificate, including answers to identification questions that were provided by the Subscriber when it was issued.

(3) Comsign shall revoke a Certificate issued to the authorized signatory of a corporation or public institution or a member of an organization or other institutional body or an authorized signatory on behalf of a natural person, at the request of the corporation, public institution, organization or institutional body or natural person for which he\she was authorized to act. The revocation request shall be given by the one authorized to do so, whether the corporation, public institution, organization or institutional body and/or natural person, in the case of an authorized signatory of a natural person and/or in accordance with the arrangements made in the Subscriber Agreement and on the application forms for issuing the Certificate. It is clarified that Comsign shall revoke an electronic certificate issued to an authorized signatory of a public institution defined in Clause 3.2.2 above only after identifying the revocation requestor (other than the authorized signatory) in a manner used to identify an EU resident and in addition using the following documents:

   (a) An identification document issued by the state, carrying a photo and I.D. number (or its equivalent).

   (b) A declaration by the state employee that the person is an authorized signatory of the public institution.

   (c) A document attesting that the state employee is an authorized signatory of the public institution.

4. Certificate Life Cycle Operational Requirements

This chapter describes the process of Certificate issuance, beginning with submitting the request and the required documents, through the process of logical issuance and up to the Certificate issuance. In addition, this chapter includes an explanation regarding the renewal and revocation of a Certificate, including those who are permitted to file requests for renewal and revocation. This chapter also includes the obligations imposed on the Subscriber.

The process for issuing an Electronic Certificate shall be carried out by at least two clerks of the CA.

4.1 Certificate application

4.1.1 Who can submit a Certificate application:

A natural person or a legal entity, by their self or by an Applicant authorized to act on their behalf for this matter, subject to issuing required documents and approvals and meeting the requirements and the provisions of this CPS.

4.1.2 Enrollment process and responsibilities:

Comsign publishes on its website the documents required for the Certificate issuance. The Applicant may, subject to prior coordination, fill in these documents and send them to Comsign's offices prior to the issuance process. However, the Applicant shall personally appear in Comsign's office or at the office of its registration representatives to activate the issuance process. Comsign may, though not obligated, send the Applicant a reminder or invitation for the issuance process by means of its discretion [phone message, SMS, and email].

The Applicant is obliged to provide complete, correct and reliable information required by Comsign to start the issuance process. Corporations, individuals and public institutions are allowed to submit an application using authorized signatories.

When applying for a Certificate for an individual resident of the EU the Applicant shall provide the following information and documents:

(1) EU passport or Identity card;

(2) EU driver's license carrying the Applicant's photo;

(3) An identification document issued by the state to a state employee, to an office holder on behalf of the state or in one of the state's institutions, or to a person holding a position by law, for the purpose of performing their duty, with an I.D. number (or equivalent) and a photo of the Applicant; for this matter, "state employee" inter alia military, police etc.

An Applicant not possessing one of (1) to (3) above and filing an affidavit to this effect, can provide in lieu of the above an attestation by a lawyer to the effect that the lawyer knows the Applicant personally and that the attestation letter is intended to support the application for an electronic certificate, including the Applicant's photo signed by the lawyer.

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

(5) Telephone numbers (residence or office as applicable).

(6) E-mail address (not verified).

(7) A signed Subscriber agreement.

When applying for a Certificate for an authorized signatory on behalf of a corporation, the Applicant shall provide the following information and documents:

(1) Certificate of Incorporation.

(2) An attorney's or banker's written statement confirming the corporation's good standing.

(3) A certified copy by an attorney of the resolution passed by the authorized body in the corporation or public institution appointing the Authorized Signatory or a written statement by legal counsel of the corporation or legal institution confirming the identity of the Authorized Signatory.

(4) All documents and information required for the identification of the Authorized Signatory applicable to the issuance process of an electronic certificate to a natural person.

When applying for a Certificate for an authorized signatory of a public institution (government offices, local authorities as well as other authorities, corporations or institutions established by law), the Applicant shall provide the following information and documents:

(1) An official document containing the identification details of the tax returns file of the public institution.

(2) A document issued by a senior officer of the public institution authorizing the authorized signatory to act on behalf of the public institution.

(3) All documents and information required for the identification of the Authorized Signatory applicable to the issuance process of an electronic certificate to a natural entity.

When applying for a Certificate for an authorized signatory of corporation or a public institution not registered in the EU, the Applicant shall provide the following information and documents:

:

An authorized copy of the corporation's certificate of incorporation.

(1) An attorney's or banker's written statement confirming the corporation good standing (including name and registration number), a certified copy of a statement by an authorized organ in the corporation confirming the authorization of the authorized signatory to act on behalf of the corporation or a confirmation of the corporation's legal counsel of such authorization.

(2) All documents and information required for the identification of the Authorized Signatory applicable to the issuance process of an electronic certificate to a natural entity.

A "certified copy" shall mean for the purpose of this clause a copy of a document certified by one of these:

(1) The authority that issued the document.

(2) A licensed advocate.

(3) Diplomatic or consular representative of the Applicant's country of residence.

4.1.3 Filing an application for an electronic certificate for an internet server

When applying for a Certificate for authenticating servers accessible through the Internet, the Applicant shall provide the following information and documents:

(1) A certificate application, which may be electronic; and

(2) An executed Subscriber Agreement, which may be electronic.

Comsign may demand any additional documentation that Comsign determines necessary to meet these Procedures and the CA/Browser Forum Requirements.

4.2 Certificate application processing

4.2.1 Performing identification and verification functions:

An identification clerk shall identify the Applicant and verify their signature on the application form and the Subscriber Agreement. The verification clerk shall present the Applicant with an information and warning form regarding the risks involved in using an Electronic Signature and the obligations imposed upon him/her. The Applicant shall sign a declaration that they was warned as stated above.

4.2.1.1 When performing identification and verification functions for authenticating servers accessible through the Internet

(1) Comsign shall obtain all the required information from the application request filed by the Applicant, from the Applicant itself or from a reliable, independent, third-party data source, provided such third-party information was confirmed with the Applicant. Comsign implements a documented procedure for verifying all data requested for inclusion in the Certificate by the Applicant. Applicant's information shall include, but not be limited to, at least one Fully Qualified Domain Name or IP address to be included in the certificate's SubjectAltName extension.

(2) Documents and data provided to Comsign according to Clause 3.2 to verify Certificate information may be used to issue Certificates up to 398 days as of the time they were obtained.

(3) Comsign implements a documented procedure that identifies and requires additional verification activity for High-Risk Certificate Requests prior to the Certificate's approval, as reasonably necessary to ensure that such requests are properly verified under the CA/Browser Forum Requirements.

(4) Comsign verifies the existence and contents of CAA records prior to issuing Certificates. Comsign acts in accordance with CAA records if present, as specified in Clause 3.2.2.8. The issuer domain names that Comsign recognizes as its identifying domains are 'Comsigntrust.com', 'Comsign.co.uk' and 'Comsigneurope.com'.

4.2.2 Approval or rejection of certificate applications

Upon completion of the identification process, the examination of the documents in terms of signatures and correctness, and the existence of the technical requirements for the issuance, the request shall be handed over to Comsign's issuing service. In case one of the mentioned requirements is not fulfilled, the process shall be stopped until completion\correction is carried out. In case the installation process is stopped, an explanation will be given to the Applicant. Comsign may refuse to issue a Certificate to any Applicant for reasonable reasons, such as a suspicion of incorrect identity, noncompliance of the signature device with the hardware and software requirements, or nonpayment for the service. Subject to the provisions of any law, Comsign shall not bear any responsibility or liability for losses or expenses induced by the rejection. If Comsign refuses to issue the Certificate, Comsign shall refund, without delay, the application fee, if any, that the Applicant paid for the Certificate.

Comsign maintains an internal database of all previously revoked Certificates and previously rejected certificate requests due to suspected phishing or other fraudulent usage or concerns. Comsign alone uses this internal database to identify subsequent suspicious certificate requests.

4.2.2.1 Approval or rejection of certificate applications for authenticating servers accessible through the Internet

Comsign shall only issue certificates to domains with suffixes that were publicly approved by ICANN and will not issue certificates with internal domain name suffixes.

Comsign shall not issue certificates containing a new gTLD under consideration by ICANN. Comsign shall only issue certificates to Subscribers after verifying the control over or exclusive right to use the Domain Name in accordance with Clause 3.2.2.4.

4.2.3 Time to process Certificate applications:

Comsign shall examine information and documents handed over as part of the inspection and processing of the application shortly upon receipt. An application handed over personally to Comsign by the Applicant, along with the required documents, during Comsign's working hours, will be examined in the presence of the Applicant.

An application that passed the examination shall be transferred for issuance without delay during Comsign's work hours.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate issuance:

To verify the identity of the Applicant and to authenticate the connection between the Applicant and his public key (signature verification device), that individuals and/or authorized signatories of corporation filing a request application for an Electronic Certificate shall either personally appear in person in front of Comsign and/or its representatives.

The issuance shall be carried out in the presence of the Applicant by a verification clerk.

The verification clerk shall offer the Applicant a hardware device approved by Comsign for the generating and storing of the signature device and the electronic certificate. In the event the Applicant wished to employ a different hardware device, Comsign shall check that the Applicant possesses a means for generating a secured signature and that the signature device and the signature verification device comply with the hardware/software requirements. For the examination the Applicant shall present Comsign with the following documents and information:

(1) Manufacturer.
(2) Product/design name.
(3) Copy of an approval issued to the device by the following: NIST and/or Common Criteria.

Comsign may be satisfied with a declaration by the applicant that the applicant has provided Comsign with correct details to the best of its knowledge concerning the signature device, its operation and accessibility. Subject to such declaration Comsign shall not be responsible for any additional checks of the signature device nor for its use, provided the private key is generated in the manner detailed in clause 4.5.1 below.

Details of the Applicant shall be entered into the system, the Applicant will generate the signature device (private key) and the signature verification device (public key) using a password known solely to him/her. In the case of issuance of signatory device on a central signature server, the password shall be entered at the stage

of initializing the partition in the server in which the signature device is stored. In this case, the Applicant shall enter his password to create a signature device (the private key) and a verification signature device (the public key) directly on the hardware device without revealing the password and the signature device to Comsign's employee. In case of issuance of a signature device on signature server stored with a third party, the password shall be entered at the stage of initializing the partition in the server in which the signature device is stored. In this case, the Applicant shall enter his password to create a signature device (the private key) and a verification signature device (the public key) directly on the hardware device without revealing the password and the signature device to Comsign's employee.

The verification clerk shall ensure the correctness of the keys and the Certificate and their storage on the hardware device (together with the Subscriber) and suggest to the Subscriber to inspect its functionality with the relevant systems.

At the time of issuance, the Subscriber shall create an identification code which will be used, inter alia, to revoke the Certificate, if applicable. This code shall be entered by the verification clerk into a system that does not enable password reset, but only a "correct" or "incorrect" signal while typing the identification code, see Clause 3.4 above, as well as a remote Certificate renewal code, see Clause 3.3 above. The verification clerk will detail to the Subscriber the Certificate revocation procedure.

The verification clerk shall hand over to the Subscriber the device and explain the obligation to keep it under their control. The verification clerk shall explain to the Subscriber the importance of keeping the device and the importance of keeping the password and/or the access component to the device in a safe and secured location.

4.3.2 Notification to the Subscriber by the CA of issuance of Certificate:

The Certificate (other than an SSL Certificate) shall be issued in the presence of the Applicant and handed over or be transmitted securely to the Subscriber upon completion of the issuance process.

4.4 Certificate Acceptance

4.4.1 Conduct constituting Certificate acceptance:

The handing over (or electronic transmission) of the Certificate by Comsign to the Subscriber shall be considered as acceptance whether the Subscriber approved the acceptance or not, provided that the handing over (or electronic transmission) was documented in Comsign's records. and that the subscriber has verified the accuracy of the data in the certificate. The use of the Certificate by the Subscriber will also be considered as acceptance.

4.4.2 Publication of the Certificate by the CA:

Upon issuing the Certificate, Comsign shall add the details of the Certificate in the valid Certificates list located in Comsign Repository and in other repositories. The access to the valid Certificates list is limited in accordance with the internal work procedures of Comsign. Subscribers are allowed to publish their Certificates in other repositories.

4.4.3 Notification of Certificate issuance by the CA to other entities:

Comsign may, but is not obligated, to inform certain third parties that an electronic certificate was issued.

4.5 Key Pairs and Certificate usage

4.5.1 Subscriber private key and Certificate usage:

The Key Pair created by the Applicant are RSA keys that are 2048 bits long or ECC keys that are 256 bits long.

The device that creates and secures the signature device may be provided either by Comsign or by the Applicant. Comsign shall not issue an Electronic Certificate to a verification signature device that does not comply with the requirements as described in Clause 4.3.1 above. The Applicant's private key shall not be revealed to Comsign during the inspection by Comsign of the Applicant's signature device.

To prevent the insertion into the device of a Key Pair belonging to a person other than the Applicant, Comsign requires that the keys be generated during the issuance process and shall not permit the use of keys generated by the Applicant prior to the issuance ceremony.

Upon receipt of the Certificate, the Subscriber shall ensure that the details in it are correct and in accordance with Clause 4.1.2 above. In case a mistake is found in one of the details, the Subscriber is hereby obligated, according to the Subscriber Agreement, to inform Comsign thereupon that a mistake was found and ask for a Certificate revocation. In case of a discrepancy in the information given by the Applicant prior to the issuance (whether in the application form and/or the personal details form and/or in the Subscriber Agreement), Comsign shall revoke the Certificate and issue a new Certificate to the Subscriber with no additional charge. In any other case, the Certificate shall be revoked, and the Subscriber shall bear the full cost of issuing a new Certificate.

It is the Subscriber's sole responsibility, during the entire Certificate validity period, to take all reasonable measures to safeguard his signature device to prevent any unauthorized use of it; to inform Comsign upon discovering that his control of the Certificate was compromised; and to use the Certificate in accordance with these Procedures.

The Applicant and/or the Subscriber are hereby warned that failure in safeguarding the signature device may result in the unauthorized use of the electronic signature of the Subscriber for committing the Subscriber, conducting transactions in his name, and creating representations on his behalf or performing any other action that can be executed using an Electronic Signature in a manner that may cause significant damages to the Subscriber and/or the relying parties of the Certificate. Thus, safeguarding and protecting the signature device as described in these Procedures is essential.

4.5.2 Relying Party public key and certificate usage:

Checking the validity of an electronic signature on an electronic message is a process that the relying party shall carry out if the relying party wishes to ensure:

(a) that Comsign confirms, with a valid Certificate, that the electronic signature was created by the signatory whose name appears on the Electronic Certificate;

(b) that the signed electronic message was not changed after the electronic signature was created; and

(c) the limitations, if any, on the permitted usages of the Certificate.

The relying party shall check if a Certificate has been revoked, for a revoked Certificate is not valid and cannot be relied upon. It is possible to check the most up-to-date status of a Certificate (if it was revoked) by submitting an inquiry to the Comsign Repository using the link included in the Certificate.

Comda publishes on its Internet site at www.comdatrust.com/repository a list of its signature verification devices that are used to issue Certificates, as well as a list of revoked Certificates related to these signature devices.

A relying party who does not verify the validity of a Certificate as described above and below, risks relying on a revoked Electronic Certificate and may be held legally responsible for any damage induced because of not checking the validity of the Electronic Certificate. Comsign shall not bear any responsibility for any damage caused by relying on a revoked Certificate if it shows that it took all reasonable measures to fulfill its obligations according to this CPS.

The owner of a Certificate and Comsign can limit the permitted usages of a Certificate. Limitations on use of the Certificate at the request of the Subscriber will be done following an explicit request by the Subscriber only. The form and content of the request must be acceptable to Comsign. These limitations are specified in the Certificate or included in it by reference and provide means for warning the Subscriber and relying parties regarding the permitted usages of the Certificate and limitations, if any, on its valid usages mentioned above. It is recommended that those who rely on Comsign's Electronic Certificates inspect the content of the Certificate and look for these warnings and limitations.

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

4.6 Certificate Renewal

4.6.1 Circumstances for certificate renewal:

Only a valid Certificate can be renewed. An invalid Certificate cannot be renewed, and a new issuance is required. Comsign is allowed, but not obligated, to inform the Subscriber of the expected expiration date of the Electronic Certificate held by the Subscriber and the need to renew it, using telephone message, SMS or email. This notice is meant only for the convenience of the Subscriber in the process of renewing the Certificate and its delivery or non-delivery to the Subscriber does not obligate Comsign and/or imposes any liability and/or responsibility of any type on Comsign, either derived from and/or related to the expiration of the Certificate and/or its non-renewal.

4.6.2 Who may request renewal:

A renewal can and will be carried out upon request of the Subscriber or upon an instruction of an authorized authority or upon Comsign's demand. The responsibility of Certificate renewal rests with the Subscriber only.

4.6.3 Processing certificate renewal requests:

Renewal of a Certificate during its validity period can and will be carried out as described in Clause 3.3.1 above, subject to the availability of the service. In this case, the Key Pair of the Subscriber shall remain identical during the extended period of validity of the renewed Certificate.

In case the above renewal procedure is not available and/or the Electronic Certificate of the Subscriber was revoked or expired, or the Subscriber did not create a password, or they cannot remember it, a re-registration shall be carried out in accordance with the complete and ordinary registration procedure, including identification of the Applicant as carried out in any first issuance of a Certificate.

Comsign reserves the right to amend or update the procedure for renewing Certificates. Updated renewal procedures shall be available (after their publication) on the Internet, as part of an amended version of the CPS, at: http://www.comsign.co.il/repository/

4.6.4 Notification of new certificate issuance to Subscriber:

A notice regarding the renewal shall be delivered to the Subscriber at the time of renewal as part of the renewal procedure. In circumstances where a new issuance takes place in lieu of a renewal, the provisions of Clause 4.3.2 above shall apply.

4.6.5 Conduct constituting acceptance of a renewal Certificate:

The handing over of the renewed Certificate by Comsign to the Subscriber shall be considered as acceptance whether the Subscriber confirmed it or not, provided that the handing over was documented in Comsign's records. The use of the Certificate by the Subscriber will be also considered as acceptance.

4.6.6 Publication of the renewal Certificate by the CA:

The renewal of the Certificate's validity is updated by Comsign at the time of renewal in the valid Certificates list in Comsign's repository and in other repositories. The access to the valid Certificates list is limited in accordance with the internal work procedures of Comsign. Subscribers are allowed to publish their Certificates in other repositories.

4.6.7 Notification of Certificate issuance by the CA to other entities:

Certificates renewed in the framework of projects requiring notification to the project's operators, either by contractual undertakings by which the Electronic Certificate was issued, shall be published by Comsign in repositories managed, held and supervised by the project's operators. When due to circumstances a new issuance rather than renewal takes place, is not carried out but a new issuance subject to the provisions of Clause 4.4.3 above shall apply.

4.7 Certificate re-key

This CPS does not permit changing Key Pair for a valid Electronic Certificate. Whenever a change of Key Pair is required, such as in case of changing a standard, requirement to enhance security or fear from deciphering or loss of control of a private key, whether by an initiative of the CA or a request by the Subscriber, a re-issuance of the Electronic Certificate shall be carried out and a new Key Pair shall be generated during the issuance process.

4.7.1 Circumstances for Certificate re-key:

No Stipulation- see the above.

4.7.2 Who may request certification of a new public key:

No Stipulation - see the above.

4.7.3 Processing Certificate re-keying requests:

No Stipulation - see the above.

4.7.4 Notification of new Certificate issuance to Subscriber:

No Stipulation - see the above.

4.7.5 Conduct constituting acceptance of a re-keyed Certificate by the CA:

No Stipulation - see the above.

4.7.6 Publication of the re-keyed Certificate by the CA:

No Stipulation - see the above.

4.7.7 Notification of Certificate issuance by the CA to other entities:

No Stipulation - see the above.

4.8 Certificate modification

This CPS does not permit changing or amending a valid Electronic Certificate. Whenever an amendment or a change of the Certificate or its text is required for any given reason, a re-issuance of the Electronic Certificate shall be carried out and a new Key Pair shall be generated during the issuance procedure.

4.8.1 Circumstances for Certificate modification:

No Stipulation - see the above.

4.8.2 Who may request Certificate modification:

No Stipulation - see the above.

4.8.3 Processing Certificate modification requests:

No Stipulation - see the above.

4.8.4 Modification of a new Certificate issuance to subscriber:

No Stipulation - see the above.

4.8.5 Conduct constituting acceptance of modified Certificate:

No Stipulation - see the above.

4.8.6 Publication of the modified Certificate by the CA:

No Stipulation - see the above.

4.8.7 Notification of Certificate issuance by the CA to other entities:

No Stipulation - see the above.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for revocation of an electronic certificate:

A Certificate, including an intermediate certificate, shall be revoked:

(1) At the request of the Subscriber or the authorized signatory.

(2) If Comsign has been notified by the Subscriber or finds out in another way that a theft, loss, change, unauthorized use, failure to meet legal or standards' requirements concerting the signature device and the signature verification device, defect or another harm to the signature device or to the Subscriber's control of the signature device has occurred.

(3) Immediately when known to Comsign that one of the details of the Certificate is incorrect or the reliability of the Certificate was harmed in another way.

(4) Immediately when known to Comsign of a defect in its secured electronic signature, or its signature device, or in its hardware and software systems, or in these systems' data security that might harm the reliability of its signature or that of the Electronic Certificates it issues.

(5) Immediately when known to Comsign that an electronic certificate was issued to a signatory without authorization, the Subscriber died (if a natural entity) or an order of dissolution was issued (if a corporation), provided Comsign is assured that the notification is reliable.

(6) Comsign's activity as CA was terminated and not transferred to another CA or if Comsign is required to comply with the requirements of this CPS.

(7) If a material defect was found in the Certificate issuance process, either a defect originating with Comsign, the Applicant or any other party involved in the issuance process.

4.9.1.1 Circumstances for revocation of a Certificate issued to an internet server.

Comsign shall revoke an electronic certificate issued to an internet server as per each of the circumstances listed in clause 4.9.1 above as well as when Comsign receives evidence to the effect that the verification of the ownership in the domain name or the control in the FQDN or the IP address stated in the Certificate cannot be relied upon or that their continued use was forbidden by judicial or legal decree.

4.9.2 Who can request revocation:

A request to revoke a Certificate shall be submitted by the Subscriber or their agent or another third party whose appointment is explicitly noted in the Subscriber Agreement. In the case of a Certificate for a corporation and/or authorized signatory of a corporation or public institution, Comsign shall revoke the Certificate upon request of the corporation, public institution or organization. The request of revocation shall be delivered by the one appointed to carry it out by the corporation, public institution or organization and/or in accordance with the provisions made in the Subscriber Agreement and the application forms for the Certificate issuance.

A request from Comsign's Registration authority to revoke a Certificate issued by the same Registration authority is permitted, provided that this option and the grounds for revocation by the Registration authority were brought before the Subscriber prior to the issuance of the Certificate and were included in the Subscriber Agreement.

Comsign shall initiate a revocation of an Electronic Certificate when it finds out that one of the circumstances described in Clause 4.9.1 above occurred and require the revocation of the Electronic Certificate.

4.9.3 Procedure for revocation request:

A request to revoke a Certificate by whomever was authorized to do so shall be submitted by phone, email or in writing. The revocation request shall be handled by Comsign's identification clerk. The identification clerk or the revocation Applicant shall complete the revocation form. Comsign's identification clerk will authenticate the identity of the revocation Applicant in accordance with the provisions of Clause 3.4 above. In case of successful authentication, the Certificate shall be revoked by Comsign's registration clerk. In any other case - the Certificate shall be suspended pending final clarification of the matter, subject to Comsign's internal procedures. The revocation procedure shall not be carried out by one person.

4.9.4 Revocation request grace period:

An Electronic Certificate shall be immediately revoked without any extension if there are grounds requiring its revocation without any grace period.

4.9.5 Time within which CA must process the revocation request:

A Certificate that shall be revoked will be revoked immediately.

4.9.6 Revocation checking requirements for relying parties:

It is the obligation of the relying party to inspect the correctness and validity of an Electronic Certificate prior to relying on it. Comsign makes available the Comsign Repository to Subscribers, addressees and third

parties. The Repository contains, inter alia, lists of certificates containing Comsign's signature verification device and lists of revoked Certificates and can be accessed on the website at: https://www.Comsign.co.il/repository.
A link to the list of revoked Certificates can also be found within the Electronic Certificate, see Clause 7.1.8 below as well as at Comsign's web site.

The inspection shall be carried out using the most up-to-date revocation list (CRL) published.

4.9.7 CRL issuance frequency:

Excluding special arrangements originated in contractual undertakings, Comsign shall publish the Certificates Revocation List (CRL) at least once every 12 hours with a 24-hour validity. Comsign usually publishes CRLs every 2 hours. In case a Certificate was revoked by Comsign, the list shall be updated immediately after the revocation.

Comsign shall not publish "last CRL" unless all certificates relevant to that CA have been expired or revoked.

In any case where the issued CRL is the "last CRL" (Termination, deprecation of a SubCA etc.) the "NextUpdate" field in the CRL shall be set to: "99991231235959Z" in accordance with ETSI 319411 and defined in IETF RFC 5280

4.9.8 Maximum latency for CRLs:

The Certificates Revocation List (CRL) is available at any time. Comsign makes sure that the retrieval times will be as minimal as possible without reducing the above maximum availability.

4.9.9 On-line certificate qualified status (OCSP) checking availability:

Comsign enables its Subscribers to verify the qualified status of the issued electronic certificate using an Online Certificate Status Protocol service (OCSP).

The results of the check comply with the RFC6960/RFC5019 requirements and are electronically signed by Comsign.

If the CA's certificate is about to expire Comsign shall compute a last OCSP answer for each issued certificate with "NextUpdate" field set to: "99991231235959Z"

4.9.10 On-line revocation checking requirements:

For Certificates for natural entities, a dedicated data communication line or using the internet may be required. The specified requirements and their specifications shall be given in the framework of separate undertaking between Comsign and the Subscriber.

4.9.10.1 On-line revocation/status checking availability of Certificates for authenticating servers accessible through the Internet.

(1) Comsign supports OCSP capability using the GET method for Certificates issued.

(2) For the status of Subscriber Certificates: Comsign updates information provided via an Online Certificate Status Protocol at least every four days. OCSP responses from this service always have an expiration time of less than ten days.

(3) For the status of Subordinate CA Certificates: Comsign updates information provided via an Online Certificate Status Protocol at least.

(i) Every twelve months and

(ii) Within 24 hours after revoking a Subordinate CA Certificate.

(4) When the OCSP responder receives a request for status of a certificate that has not been issued, then the responder responds with a status of "unknown".

4.9.11 Other forms of revocation advertisements available:

Comsign enables online checking of the list of the revoked Certificates by a relying party. Any other form of advertisement, such as "pushing" the CRL to a subscriber of the service shall be made available according to a rule of law. Comsign is allowed to charge payments for this service. The notice of change of status does not replace the obligation to check the repository of revoked Certificates, unless otherwise stated in an agreement or a rule of law.

4.9.12 Special requirements related to key compromise:

The Subscriber's loss of control of the signature device requires an immediate report to Comsign and a request for an Electronic Certificate revocation. Comsign shall revoke the Certificate immediately upon receiving the notice, as described above in the regular revocation procedure applicable to the revocation circumstances.

Parties may use the following methods to demonstrate key compromise:

- Submission of a signed CSR or other challenge response signed by the private key and verifiable by the public key
- Submission of the private key itself
- Providing references to vulnerability and/or security incident reliable sources from which the Compromise is verifiable
- Any other demonstration methods that will be submitted will be analyzed separately and specifically for each case.

4.9.13 Circumstances for suspension:

4.9.13.1 Circumstances for suspension of Certificates for natural entities

Any circumstance requiring a Certificate revocation (see Clause 4.9.1 above) shall be considered a circumstance for the suspension of the validity of the Electronic Certificate. The CA's discretion whether to revoke or to suspend a Certificate shall be conditioned on additional circumstances and the Subscriber's request or one appointed by him/her in the Subscriber Agreement to ask for the suspension or revocation. Thus, for instance, in case the Subscriber cannot find the signature device but the Subscriber postulates that it can be found after reasonable search, it can and shall be a reasonable ground for Certificate suspension.

4.9.13.2 Circumstances for suspension of Certificates for authenticating servers accessible through the Internet

Comsign does not suspend certificates for servers (QWAC/SSL).

4.9.14 Who can request Certificate suspension:

The permitted entity to request the suspension of the Certificate is the Subscriber or the one appointed by him/her in the Subscriber Agreement to request the revocation or suspension of the Certificate.

4.9.15 Procedure for suspension request:

The manner of handling a request for Certificate, as well as certificate issued to an internet server, suspension is as described in Clause 4.9.3 above regarding the manner of handling Certificate revocation request.

4.9.16 Limit on suspension period:

Suspension of the Certificate shall always be for a defined limited time not exceeding 48 hours after which the suspension shall be lifted, or the Certificate will be revoked. The length of the suspension period shall be set in accordance with the circumstances taking into consideration the request of the suspension Applicant. During the suspension period, the Certificate will be registered in Comsign's CRL.

4.10 Certificate status services

4.10.1 Operational characteristics:

Checking the Certificate status shall be carried out by the relying party using the Certificates Revocation List (CRL) on Comsign's website.

4.10.2 Service availability:

The service of checking the status of the Electronic Certificate shall be available for 24 hours, 7 days a week. In case the availability of the services was unavailable for any given reason, the CA will act to restore the service as soon as possible. See also Clause 5.7 regarding disaster recovery.

4.10.3 Optional features – release from lockup:

Hardware devices include a security measure by which the access to the signature device is protected by a password. The device shall be locked after a specified number of unsuccessful attempts to enter the password. Comsign shall offer Subscribers a service for releasing a locked card without Comsign having access to the signature device, by using a specific mechanism.

4.11 End of subscription

All Certificates shall be valid beginning the day and hour of their issuance by Comsign. The Certificate shall be valid for the term stated in the Subscriber Agreement, unless the Certificate is revoked or renewed earlier.

4.12 Key escrow recovery

This CPS does not allow an escrow of the private key and its retrieval.

4.12.1 Key escrow and recovery policy and practices:

No Stipulation - see above.

4.12.2 Session key encapsulation and recovery policy and practices:

No Stipulation - see above.

5. Facility, Management and Operational Controls

The purpose of this chapter is to review for the Applicant, Subscriber and the relying party the means of physical control, the security of its personnel, and the protection of its records used in its operation. In addition, this chapter includes a description of the records Comsign keeps, and the types of information stored in them.

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

Comsign's internal work procedures include, inter alia, security policy, protection of assets, personnel security, physical security, operations management, management of the access to Comsign's signature infrastructure, reliability of the installation and maintenances, and survivability in event of a disaster.

5.1 Physical Controls

5.1.1 Site location and construction:

The facilities associated with issuing Certificates and managing revocations operate in an environment that physically protects these services against damage caused by unauthorized access to systems or data. Comsign stores elements of the system critical for its operation in a protected location, which prevents unauthorized infiltration or entrance, in accordance with the nature of Comsign's activity. The physical protection is achieved by creating clearly defined perimeter security barriers (meaning, physical obstacles) surrounding the Certificate issuance services, preparing the devices and managing revocations. Any section of the facility that is shared with another organization not operating CA services shall be outside this secured area. The physical security provides a response against nature disasters, fires and water damage, damage to supportive infrastructure such as electricity and communication, facility collapse, theft, burglary and unauthorized infiltration.

5.1.2 Physical access:

No person who enters the secured site is left alone without supervision by an authorized person. Comsign maintains embedded protective controls against unauthorized removal of equipment, information, media and software related to Comsign's CA services. Comsign maintains an inventory of information assets and classifies them to assign the necessary protection required for each asset, in accordance with its risk management analysis. The Security Manager keeps the inventory list of critical assets and the way they are protected. These assets could be either physical assets and/or logical data assets.

5.1.3 Power and air conditioning:

The electricity and air conditioning system includes means and controls to monitor deviations and malfunctions, and alternative supply in case of malfunction and electricity supply shut down to the secured facility.

5.1.4 Water exposure:

The secured facility is disconnected from water supply lines and protective measures against floods and water damage to the facility and the equipment were taken.

5.1.5 Fire prevention and protection:

The facility includes systems for fire detection and extinguishing.

5.1.6 Media storage:

All measures for data storage are in the secured facility and are subject to physical security and access control. The backup systems are stored separately and protected by main storage protection measures.

5.1.7 Waste disposal:

Comsign implements designated procedures regulating shredding or physical destruction of paperwork or physical media that contain confidential or limited access information.

5.1.8 Off-site backup:

Comsign implements a full backup policy and maintains disaster recovery systems located separately from the company's secured operation facility. See Clause 5.7 below.

5.2 Procedural Controls

5.2.1 Trusted roles:

All employees, contractors and consultants of Comsign and/or its representatives who have access to or control of registration, issuance, usage and revocation of Certificates issued by Comsign, including access to limited-access Comsign's Repository operations, shall be considered, for the purpose of these Procedures, as fulfilling a position requiring special trust ("**position of trust**"). The personnel include, but are not limited to, customer service personnel, system management personnel, designated engineering personnel and management personnel whose job is to supervise the infrastructure of Comsign's trust systems. The positions of trust and the authorizations of each person in a position of trust are listed in Comsign's internal procedures. Persons in positions of trust are appointed to their position by the CEO of Comsign and approved by the Security Manager. Persons in positions of trust in Comsign are obligated to maintain confidentiality and avoid conflicts of interest in the context of their work at Comsign.

Persons in positions of trust are employed on a personal contract that includes details of the position and its components, as well as the undertaking by each such employee that they understand the components of the positions and undertakes to act in accordance with these Procedures and their employment contract.

Comsign ascertains that there are no conflicts of interest involving employees in positions of trust and that there is no overlapping of identity among employees in positions of trust. Comsign considers the following positions to be positions of trust: CEO, Security Manager in charge of implementing the security procedures, identification clerk, verification clerk, key managers and holders, security safe key holder, registration manager and logs examiner.

Each position has physical and logical access limits that are derived from internal procedures. These limitations are confidential. A person in a position of trust may not serve in more than one of the following positions: CA manager, security manager, registration clerk, administrator, systems operator or auditor. See clause 5.2.4.

5.2.2 Number of persons required per task:

Every task defined as critical by Comsign is performed by at least two different persons. Comsign keeps personnel reserves to comply with the requirements of these Procedures. A position is not limited to one person, and every person has a substitute in his rank.

5.2.3 Identification and authentication for each role:

Comsign employs an access control and user management policy which uses biometric systems and advanced physical identification devices enabling control over both the identity of the person entering a certain secured

area or their access to secured parts of the system and management of records with respect to times of entry and access as well as areas and parts of the system which were accessed.

5.2.4 Roles requiring separation of duties:

Comsign's security policy prohibits granting different trust authorities to the same official. Thus, for instance, the Security manager cannot simultaneously serve as verification or identification clerk. In addition, execution of certain duties, such as generation of Comsign's Key Pair requires the involvement of several officials with each official performing their part in the duty, a part without which the duty cannot be completed. Comsign acts in accordance with Appendix No. 4a, the Division of Duties, which is part of the Procedures that were submitted to the SII and approved as part of confirmation of compliance with IS 27001 and IS 9001. This appendix includes the Comsign employees' authorization areas and the physical access authorizations to the various areas within Comsign. The appendix presents the process for separating functions and the ability to supervise and ensure that at least two people participate in each critical action. Each functionary has limited exclusive access to each area within the Comsign building. Senior officials have limited access to areas defined as "very sensitive" from a security perspective. There is no one official who has exclusive access to all areas.

5.3 Personnel Controls

5.3.1 Qualifications, experience and clearance requirements:

Comsign employs knowledgeable, experienced, specialized, and competent personnel with the proper skills required for the position and the services provided by them to Comsign. Comsign performs several control measures before employing an employee, including personal interviews, reliability test, checking references, and obtaining documents that testify to the candidate's ability to do the job (certifications, diplomas, employment experience, etc.) Comsign's CEO gives the final approval for all appointments of employees to positions of trust in Comsign.

5.3.2 Background check procedures:

Comsign and its representatives conduct an initial investigation of all personnel working for Comsign. Comsign conducts more comprehensive and detailed evaluations according to its human resources procedures regarding personnel intended for positions of trust. Comsign performs periodical investigations of all persons in positions of trust to verify their reliability and professional capability, in accordance with Comsign's human resources procedures. Employees and representatives are not given access to sensitive areas or allowed to fulfill the functions of a position of trust until the required hiring investigations and checks are completed. Anyone who does not pass the initial investigation, or a periodic investigation will not be employed by Comsign.

Comsign employs operational checks including organizational checks, checks of personnel, checks of external parties and additional management checks. These checks include requirements related to training and instruction of Comsign's employees and/or its representatives, setting policy regulating the allocation of positions within Comsign, documentation requirements and procedures and scheduled audits. The Security Manager conducts these operational checks to ascertain that work is being done in accordance with the Procedures. If the Security Manager finds that an employee is not doing what the employee is supposed to be doing, in accordance with their job description and the Procedures, disciplinary action shall be taken and the option of discontinuing their employment with Comsign will be considered.

5.3.3 Training requirements:

Comsign conducts employees training in which the knowledge of the Procedures, job descriptions are refreshed, as well as drawing conclusions from security incidents and other events. The annual training program is produced during the last month of each calendar year.

5.3.4 Retraining frequency and requirements:

The frequency of training is set in the framework of the annual program and includes quarterly training sessions. A higher frequency is possible in case of a change in the Procedures or adaption of new technologies.

5.3.5 Job rotation frequency and sequence:

Comsign does not operate a policy obligating a rotation of positions among its employees.

5.3.6 Sanctions for unauthorized actions:

Comsign exercises a strict and extensive reporting and debriefing procedures in any case of malfunction or a complaint. Findings indicating a violation of work procedures by an employee, or an independent contractor are handled with disciplinary actions and may result in dismissal or termination of the contractual agreement.

5.3.7 Independent contractor requirements:

When Comsign enters a contract with any subcontractor for work during which the subcontractor is given access to or control over registration, issuance, usage or revocations processes by Comsign Certificates, including work on limited-access parts of the Comsign Repository, the subcontractor undertakes, in its contract with Comsign, to uphold the strict security requirements to which Comsign is obligated in accordance with this CPS in respect of the work done by the subcontractor. In addition, the subcontractor undertakes to compensate Comsign if any damage is caused because of breaching data security.

5.3.8 Documentation supplied to personnel:

The CA's team receives full access, according to the matter and the job description, to the internal work procedures of the CA, this CPS and the security and operational instruction given from time to time.

5.4 Audit logging procedures

Logs production is a recording action of incidents taking place in the framework of issuing Electronic Certificates using Comsign's computerized system. The logging is performed by keeping a log of the events in a manner preventing its erasure by unauthorized agents.

5.4.1 Types of events recorded:

Comsign and/or its representatives keep reliable records, including records of all actions and events concerning operation, close by to the time of the event, including inter alia: activation time of the computerized system used for the operation of the CA and each of its applications and their shut down, changing of passwords, unauthorized attempts to infiltrate the system, creating or changing keys, issuance and revocation of Certificates, and access permits to the computer system.

5.4.2 Frequency of processing log:

The logs are checked on an hourly, daily, weekly or monthly basis. Actions defined as critical are checked by the Security Manager. In addition, Comsign checks the logs in the event of any warning of a suspicious or unusual event.

5.4.3 Retention period for audit logs:

The archival period is up to 25 years.

5.4.4 Protection of audit log:

The logs are kept in a secured electronic format in Comsign's computerized systems as part of the secured facility with logical and physical protection. The protection includes access control and management of users authorized to access the archived logs.

5.4.5 Audit log backup procedures:

Comsign uses adequate backup means of the logs, with high accessibility, reliability, and protection from loss of information.

5.4.6 Audit collection system (internal or external):

Comsign employs an internal system for collecting audit logs from the different systems operating within the framework of issuing Electronic Certificates by Comsign. The system enables both the collection of the material and its retrieval at any given moment, and it is subject to the audit of the auditor.

5.4.7 Notification of security events:

The logs control system includes features of immediate alerts in real time about material events and should be reported to the manager of the CA and the Security Manager. In addition, according to the internal work procedures of Comsign and eIDAS, there are types of security events that require immediate attention and should be reported to the appropriate supervisory body and in certain cases to all Comsign Subscribers.

5.4.8 Vulnerability assessment:

The documented logs are kept and examined to, inter alia, monitor and check the vulnerability of Comsign's software and hardware systems. The assessment of Comsign's software and hardware systems vulnerability level is carried out and examined in the framework of the annual security and risks audit based on the logs data. In addition, risk assessments may take place on a daily, monthly and annual basis in accordance with the requirements of Comsign's audit and security procedures based on the most up-to-date logs data.

5.5 Records archival

Comsign archives records as documents in writing or in the form of computerized messages, provided that their keying, storage, safeguarding and retrieving are accurate and complete.

5.5.1 Types of records archived:

The records archived by Comsign relate to actions and information critical to any Certificate application and to the issuance, usage, revocation, expiration or renewal of Certificates, entering and exiting secured areas within Comsign, recording of data security systems etc. The recording includes the date of the recording, the identity of the individual performing the documented action in the record and the type of the record. The purpose of the recording is to enable supervision and examination of the actions performed by Comsign's employees during the Certificate issuance process and its revocation, as well as: the identity of the Subscriber whose name is in every Certificate and the documents by which the Subscriber was identified; the identity of the persons asking for revocation of the Certificates; other details specified in the Certificate; material details concerning the issuance process including the Applicant's statement; recording details concerning the management of Comsign's private key (signature device, including, creating a key, its backup, safeguarding, destruction and the manner of managing the private key's hardware and software encryption; recording of data security events including known attempts to harm Comsign's software, the actions taken by Comsign regarding information security, changes in Comsign's information security systems, malfunctions of software and hardware etc.

5.5.2 Retention period for archive:

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

Comsign shall store documents and information received from Subscribers and Applicants for a period of at least 25 years.

5.5.3 Protection of archive:

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

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

5.5.4 Archive backup procedures:

Adequate backup procedures shall be in place so that in the event of the loss or destruction of the primary archives, a complete set of backup copies will be available within a feasible

5.5.5 period of time Requirements for time stamping of records:

The electronic records include a day and hour stamp indicating the time the record was created. See Clause 6.8 below. Written records include hand written date of their creation.

5.5.6 Archive collection system (internal or external):

Comsign applies an internal archival system for collecting and keeping records. The system enables both the collection of the material and its retrieval at any given moment, and it is subject to audit by the auditor.

5.5.7 Procedures to obtain and verify archive information:

Physical records are kept in the original format and match the requirements in Comsign's internal work procedures. Electronic records, including physical documents converted by scanning to electronic format, are created, kept and retrieved according to the applicable law that grants them the status of an original document.

5.6 CA Keys changeover

In case grounds occurred requiring the replacement of Key Pair (private and public) by which the CA signs the Electronic Certificate of the issuance server, or the Electronic Certificate issued to the Subscriber, a procedure of keys generation takes place, as described in Clause 6.1 below. Once the Key Pair has been changed, the Certificates issued shall be signed from now on only using the new (replaced) Key Pair. Not every key replacement requires revocation on the date of the replacement of valid Electronic Certificates that were signed using the previous Key Pair.

The "valid to" date of a CA certificate shall always be longer than that of an end entity certificate signed by this CA. The CA shall be renewed when it is still valid for longer than five years.

For an event requiring Certificate revocation due to harm caused to the signature device and the need to change the Key Pair - see Clause 4.9.1 above.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures:

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

The Plans are intended for the specified incidents below which prevent the continued operation of the CA in the site:

(1) General loss of electric power and failure of the entire Uninterruptible Power Supply (UPS) system in the building where Comsign's computer system is located.

(2) Physical destruction of Comsign's computers and/or the information contained thereon, caused by force majeure and/or fire and/or flood and/or magnetic disruptions and/or any other cause beyond the control of Comsign.

(3) Logical or physical breach of data security.

5.7.2 Computing resources, software and/or data are corrupted:

In any event resulting in damages to the availability of the CA's computerized systems, procedures for dealing with malfunctions shall be activated to overcome the prevention and restore complete operation of the CA's computerized systems within the accessibility constraints under which these systems operate. If the CA realizes that it is impossible to overcome the damages within the accessibility constraints, it shall activate the disaster recovery procedure described in Clause 5.7.4 below.

5.7.3 Entity private key compromise procedures:

Loss of control or damage to the private key of a member in the CA hierarchy in circumstances requiring the generation of a new Key Pair and issuance of a new Electronic Certificate in lieu of the Certificate signed by the damaged private key will be carried out in accordance with Comsign's internal work procedures. This includes replacement of Electronic Certificates whose reliability was damaged in coordination with the Subscribers, and when applicable, with the relying parties.

5.7.4 Business continuity capabilities after a disaster:

Comsign has a substitute recovery facility for Disaster events (DRP) which enables Comsign to continue publication of the Certificate Revocation List (CRL) in case of a disaster damaging its main facility preventing its functionality.

5.8 CA or RA termination

Comsign shall terminate or interrupt its operations in the following circumstances:

(1) Issuance of a preemptory liquidation order for the liquidation of Comsign.

(2) The Board of Directors of Comsign adopts a resolution terminating Comsign's activity as a CA.

If Comsign's operations are terminated, Comsign shall take the following steps:

(1) Refrain from issuing new Electronic Certificates.

(2) Revoke, as soon as possible, all the valid Electronic Certificates that it has issued.

(3) Notify all Subscribers and relying parties.

(4) Add the revoked Certificates to the CRL.

(5) Revoke the appointment of any Registration authority appointed to act on its behalf.

(6) Continue the maintenance of the records required for providing evidence in legal proceedings. If Comsign's operations are terminated, Comsign may transfer its management to a substitute CA. In this case, Subscribers have the right to demand the substitute CA to revoke their Certificates.

Comsign shall immediately notify the Subscribers of all valid Certificates on the date it terminates operations and take action to minimize the potential disruptions that Subscribers and relying parties are likely to suffer from the termination of its operation. The notice shall be sent by e-mail.

5.9 Physical security - signatures server

A corporation intending to store its signature device on the intra-organizational signatures' server is responsible to take intra-organizational security measures which prevent unauthorized access to the device, removal of the signature device and/or its copying.

If the signatures server in which the signature device is stored is held by a third party, the server must be located in a physically secured area protected by physical security measures, including an access control system and management of authorized persons entry to the secured area in which the server is located, monitoring and alert systems, to the satisfaction of the CA.

If the signature server is stored at Comsign, Comsign shall ensure that it will be kept under all security requirements that apply to Comsign as a CA.

6. Technical Security Controls

6.1 Key Pair generation and installation

6.1.1 Key pair generation:

Generating the Key Pair of the Subscriber is performed by the Subscriber using reliable hardware that complies with the requirements in a manner that prevents the access and the intervention in the generation process.

The Key Pair shall be always under the Subscriber's control or an individual on their behalf.

6.1.2 Private Key delivery to the Subscriber:

The private key delivery to the Subscriber shall take place during the issuance in a secured manner that protects the exclusive control of the Subscriber, or an individual on their behalf, of the private key. The key shall be generated inside a hardware device that prevents unauthorized access to the signature device. The CA is not permitted to hold a copy of the Subscriber's private key in his possession.

6.1.3 Public key delivery to the Certificate issuer:

Delivery of the Subscriber's public key to the CA requires the use of a mechanism ensuring that the public key shall be handed over in full without any change and that the Subscriber holds the private key corresponding to the delivered public key.

6.1.4 CA public key delivery to relying parties:

Comsign's key pair generation takes place under physical and logical security conditions employing holders of positions of trust specially selected for this. Six persons are required for the generation of Comsign's signature device and its encryption. Key reconstruction requires at least four persons. As added security, the key parts are generated using a secure HSM and are divided between trust position holders in a way that only the combination of all trust holders, holding together all parts of the key will enable the decryption and reconstruction of the key.

The CA's public key is available to the public relying on the Electronic Certificates issued by the CA on the CA's website at the address: https://www.comsign.co.il/repository

6.1.5 Key sizes:

6.1.5.1 CA Certificates Key Sizes

The size of Comsign's signature device (private key) is 4096 bytes. The size of the Subscriber's signature device shall not be smaller than 2048 bytes. Comsign's Key Pair is valid until July 16, 2036. The Key Pair may be replaced prior to that date. The new public key shall be published in Comsign's Repository. Furthermore, the Key Pair shall be replaced in case of a change in the regulations or the instructions defining the length and/or the algorithm of the signature device (the private key) of Comsign.

6.1.6 Public key parameters generation and quality checking:

Comsign's CA public key is generated in the framework of a Key Ceremony carried out by at least 4 people in trusted roles that must include the Security officer, a ceremony manager and key holders in accordance with internal work procedures that received the approval of a WebTrust auditor and are intended to create a secured environment both physically (with dual control and other security measures) and in terms of the reliability of the participants and the hardware used. A reliable hardware device (FIPS 140-2 Level 3) is used to create, protect, and destroy Comsign's signature device (the private key).

The Subscriber's public key is generated upon Certificate issuance as provided in clause 3.2.1 above and 6.2.1 below and as per terms provided therein.

6.1.7 Key usage purposes (as per X.509v3 key usage fields:

In each Electronic Certificate signed using a Key Pair of the CA the following fields are activated: Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing, and the keys are used only to create Electronic Certificates and CRLs within the scope of the protected hardware. To comply with the requirements of X.509v3 standard, the field of usage of the Electronic Certificates signed by the CA's signature device contains a limitation of use in accordance with the Subscriber Agreement and the Certificate application.

6.2 Private Key protection and cryptographic module engineering controls

6.2.1 Cryptographic modules standards and controls:

Comsign's CA signature device for signing Electronic Certificates was created solely by Comsign and is under its exclusive control. Comsign's and/or its representatives' signature device is protected by reliable secure hardware devices and comply with all the following:

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

(2) Protected by means that comply, at least, with the FIPS 140-2, Level 3 standard or CC EAL4;

(3) Backed-up using protected, secure mean; the backup is stored separately;

(4) Additional requirements to provide a reasonable level of security against infiltration, disruption or malicious use.

At a reasonable time prior to the revocation or expiration of the CA's signature device, the CA shall create a new signature Key Pair to avoid compromising its continuous operation. Generating a new Key Pair is also carried out in accordance with the above standard or a higher one, as the standard requires at that time.

Generating and storing the Subscriber's signature device shall be also carried out using a reliable hardware device (Smart Card, Token, HSM etc.). Whenever the access to the private key of the Subscriber requires a password, the password shall comply with high security requirements according to international standard.

6.2.2 Private Key (M out of N) multi-person control:

To mitigate risk of fraud, the following measures are taken to protect Comsign's signature device (private key): Comsign's signature device (private key) is completely encrypted on a hardware-based encryption card and stored in Comsign's safe box. The encryption key that encrypted the signature device (private key) is split into several parts. Each part is deposited with a Comsign employee who does not directly deal with Certificate management and issuing services. All such employees undergo strict, periodic reliability checks. Only by assembling all parts, using a controlled and supervised process, enables the reconstruction of the encryption key.

6.2.3 Private Key escrow:

Comsign's private key is not deposited in escrow. The protection is achieved as described in Clause 6.2.2.

6.2.4 Private Key backup:

Comsign backups all its systems, including the private key, in the framework of preparing for disasters. The backup of the private key is carried out using individuals in Positions of Trust and keeping the backups separately, subject to the security procedures used in protecting Comsign's signature device.

6.2.5 Private Key archival:

After revocation, expiration or termination of use of Comsign's private key, Comsign's signature device is kept in secured conditions corresponding the provisions of these Procedures regarding protection of Comsign's private key, for a minimum period of 12 months.

Archiving the Subscriber's expired or revoked private key is subject to the sole discretion of the Subscriber. The Subscriber is not obligated by agreement to archive his signature device after its revocation or expiration.

6.2.6 Private Key transfer into or from a cryptographic module:

Hardware devices used by Comsign to create the signature device, of both the CA and the Subscriber, are characterized by the fact that generating the private key is carried out within the hardware device and insertion or ejection of the private key from the device is impossible.

6.2.7 Private Key storage on cryptographic module:

The CA's and the Subscriber's private key are stored in the secured hardware device as described in Clause 6.2.1 above.

6.2.8 Method of activating private key:

The access to the signature device and its activation is allowed only to the Subscriber or to an individual on their behalf. Activating the signature device is enabled only by using the password or other single-value identification mean (e.g., biometric) of the Subscriber or their representative.

6.2.9 Method of deactivating private key:

The activity of the private key stops at the end of each activation and it stops being active.

6.2.10 Method of destroying private key:

The outcome of destroying the private key is the destruction of the logical information of the signature device. This can be accomplished by a complete erasure of the logical information stored in the hardware component in which the private key is stored or the complete destruction of the hardware device in a manner that prevents the continuous usage of the information stored in it or its recreation.

6.2.11 Cryptographic module rating:

The CA's and the Subscriber's signature devices are protected using encryption software or hardware tokens and both comply with the requirements of the provisions of these Procedures.

Where the Applicant received from Comsign the hardware device that creates and contains the signature device, Comsign bears the responsibility of compliance of the signature device and the signature verification device that identifies the signature device. In case the Applicant did not receive from Comsign the hardware device on which the signature device will be installed, Comsign shall issue an Electronic Certificate to the Applicant only after it verified that the Applicant holds a signature device for issuing a secured electronic signature and that the signature device and the signature verification device that identifies it comply with the provisions of the Procedures. Comsign is permitted to receive the Applicant's declaration regarding the signature device they use, the manner of its operation and access thereto.

6.3 Other aspects of Key Pair management

6.3.1 Public key archival:

Comsign archives in its archives the public keys of its signature servers and applies the provisions of Clause 5.5 above, subject to necessary changes.

The Subscriber is not obligated to archive the public key after the destruction, expiration or revocation of their corresponding private key.

6.3.2 Certificate operational periods and the key pair usage periods:

The Electronic Certificate's validity period is set at the time of the Certificate issuance. The validity period shall not exceed 5 years or a shorter period if so set by any change because of technological requirement or any other reason obligating replacement of the Key Pair and issuance of a new Electronic Certificate. Under no circumstances shall the validity period of an electronic certificate issued to an internet server exceed 398 days.

Renewal of an Electronic Certificate prior to its expiration shall not obligate the replacement of the Key Pair.

Only one electronic certificate can be issued to the same key pair. Therefore, termination of the previous Certificate is a prerequisite of the renewal of an electronic certificate.

6.4 Activation data

6.4.1 Activation data generation and installation:

Generation of the required information for activating and installing the signature device on the hardware device storing it (Smart Card, Storage microchip, web server, HSM etc.) shall comply with the security requirements of these Procedures.

6.4.2 Activation data protection:

The data required for the activation of the signature device is protected by cryptographic means and shall be under the absolute control of the Subscriber or the Subscriber's representative responsible for its protection.

6.4.3 Other aspects of activation data:

No Stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements:

In the framework of providing the services, Comsign and its representatives shall solely use reliable systems that comply with the requirements referred to in these Procedures.

The system components used for identifying the Applicant, issuing the Electronic Certificate and revoking it, shall comply with the security level of standard EAL4 common criteria.

Comsign uses reliable information security systems. These systems are confidential to the public but controlled by external agents. As part of the control, an annual audit is performed by an external independent auditor to ensure the reliability of the systems and compliance with the Procedures.

Furthermore, an annual systems risk survey is performed by an external independent data security expert. It should be noted that Comsign complies with the standards of ISO 27001 regarding data security and audited by independent agents to comply with these standards.

Comsign enforces multi-factor authentication for all accounts capable of directly causing certificate issuance.

6.5.2 Computer security rating:

Comsign implements and complies with the standards of data security required by these Procedures.

6.6 Life cycle technical controls:

6.6.1 System development controls:

Prior to the activation of any development or upgrade of a system component used in the operation of the CA, it shall comply with quality and adaptation controls. In addition, every such development is examined in the annual risk assessment survey by an external independent expert.

6.6.2 Security management controls:

Comsign operates a control and monitoring system, managed by the CA's Security Manager, which maintains a continuous follow up intended to identify security malfunctions and protect the integrity of Comsign's systems and data against viruses and malicious and unauthorized software; minimize damage caused by security incidents by reporting the incidents and employing the response procedures; treat securely the media Comsign uses in order to protect it from damage, theft and unauthorized access; implement media management procedures that provide protection against outdating and physical deterioration of the medias during the period the records shall be kept; maintain procedures for every managerial and trust position that influences the accessibility and quality of the Certificate services; monitor the capacity requirements and create a forecast of future capacity requirements in order to guarantee availability of the processing power and the storage devices; act, within reasonable time and with cooperation, in order to quickly respond to incidents and limit the effect of security breaches. Every incident is reported thereupon and is monitored continuously until it is rectified.

6.6.3 Life cycle security controls:

Comsign operates an ongoing control system designed to guarantee that the functionality and integrity of the hardware systems that deal with data encryption and signing, data dealing with Electronic Certificates and the status of their validity, Certificates revocation and active lists and additional information concerning their activation or revocation is maintained. See Clause 6.2.2 above.

6.7 Network Security Controls

Comsign implements a network security policy, access control and users' management while maintaining a complete separation of systems dealing with Certificates issuance and management and online systems connected to the internet. Online system components are protected with security measures designed to prevent system breaches, viruses or malicious programs and identification of unauthorized infiltration attempts.

6.8 Time-stamping

The Day and Time Stamp is intended to improve the reliability of Comsign's Certificate issuance services. The stamp attests the correct day and time of the action and the identity of the person or the device that created the stamp. The stamp represents the Greenwich Mean Time (GMT) and adopts the conventions of UTC. Comsign's stamp relies on the time source of a reliable third party that provides the global official time at any given moment.

Comsign shall use the stamp, whether directly on the data or on a parallel reliable control line, on the following data:

(1) Certificates.

(2) Certificates Revocation Lists, and other records of the revoked Certificates' databases.

(3) Other information, in accordance with the provisions of these Procedures.

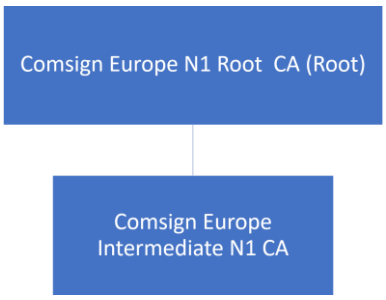
6.9 Logical security- the Signature server

When the signature device is stored in a signature server, it is required that the signature device is created and kept in a cryptographic module which complies with the Common Criteria EAL4 standard, or FIPS 140-2 standard level 3 or 4 at least, and does not allow duplicating the signature device after its creation or its copying (excluding backups) to an external source outside the storage device. The access and activation of the signature device requires a single-value identification of the Subscriber and shall be limited to the partition of the signature server in which the signature device is stored. The method of activation and accessing the signature device using a physical cryptographic component or a unique password which comply with the standard and the other requirements will enable the Subscriber exclusive control in their electronic signature.

If the signature device is stored in the signature server held by a third party, a higher security level is required to ensure the exclusive control of the signature device owner in the private key. This higher security level is intended to achieve the same exclusive control as it was if the signature device would have been stored in an independent component which was held by an authorized individual. This requirement is achieved by combining a separate device for the activation of the signature device (e.g., a Smart Card, a device that produces changing passwords to a cell phone with changing passwords) and a password known solely to the authorized individual (or with a biometric device). Only after that, the access to the signee's personal storage device is possible by using a different unique password. Upon approval of the access to the storage device itself, the required access to the activation of the signature device within the designated partition on the signature server is granted to the authorized individual.

7. Certificate, CRL, and OCSP Profiles

The current PKI Hierarchy:



7.1 Certificate profile

Comsign generates.

7.1.1 Version number(s):

Comsign issues Electronic Certificates that comply with X. 509 version 3 standard.

7.1.2 Certificate extensions:

Comsign utilizes the following extension fields:

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 Comsign Europe N1 Root CA Certificate extension fields

(1) basicConstraints:

(a) This extension appears as a critical extension.

(b) The cA field is set to true.

(c) The pathLenConstraint field is not present.

(2) keyUsage:

(a) This extension is present and marked as critical.

(b) Bit positions for digitalSignature, keyCertSign and cRLSign are set.

(3) certificatePolicies

(a) This extension is not present.

(4) extendedKeyUsage

(a) This extension is not present.

(5) Subject Information

(a) The Certificate Subject contains the following:

countryName (OID 2.5.4.6). This field contains the two-letter ISO 3166-1 country code for the country in which the CA's place of business is located = EE

organizationName (OID 2.5.4.10): This field is present and the contents contains the Subject CA's name

Common Name (OID 2.5.4.3): Comsign Europe N1 Root CA

(6) certificate details:

Data:
Version: 3 (0x2)
Serial Number:
7a5d2ea9d5bcd4a84cfb4c969ddf8e37
Signature Algorithm: sha384ECDSA
Issuer:
countryName = EE
organizationName = ComSign Europe.
commonName = ComSign Europe N1 Root CA
Validity:
Not Before: 17.04.2024 12:32:14
Not After : 17.04.2049 12:48:52
Subject:
countryName = EE
organizationName = ComSign Europe.
commonName = ComSign Europe N1 Root CA
Subject Public Key Info:
Public Key Algorithm: ECC (384 Bits)
Public-Key: ECC (384 bit) X509v3 extensions:
X509v3 Basic Constraints: critical
CA: TRUE
X509v3 Key Usage: critical
Digital Signature, Certificate Sign, CRL Sign
X509v3 Subject Key Identifier:
51d604bce052d694ed8af4e3b37d31a21d1e8cb5
Signature Algorithm: sha384ECDSA

7.1.2.2 Subordinate CA Certificate

(1) certificatePolicies

(a) This extension is present and is not marked critical.

(b) certificatePolicies: policyQualifiers: qualifier: cPSuri HTTP URL for the Root CA's Certificate Policies and Certification Practice Statement.

(2) cRLDistributionPoints

(a) This extension is present and is not critical. It contains the HTTP URL of the CA's CRL service.

(3) authorityInformationAccess

(a) This extension is present. It is 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).

(4) basicConstraints

(a) This extension is present and is marked critical.

(b) The cA field is set to true.

(5) keyUsage

(a) This extension is present and is marked critical.

(b) Bit positions for keyCertSign and cRLSign are set.

(6) Subject Information - Certificate Subject contains the following:

(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 = EE.

(b) organizationName (OID 2.5.4.10): the Subject CA's name

(c) Locality Name

(d) Common Name (OID 2.5.4.3): Comsign represents that it followed the procedure set forth in its Certificate Policy and Certification Practice Statement to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate.

(7) Example: ComSign Europe Intermediate N1 CA certificate details:

Data:
Version: 3 (0x2)
Serial Number:
1b0000000887a7899b47ebda88000000000008
Signature Algorithm: sha384ECDSA
Issuer:
countryName = EE
organizationName = Comsign Europe Ltd.
commonName = Comsign Europe Intermediate N1 Root CA
Validity
Not Before: 17.06.2024 14:12:15
Not After : 17.06.2024 14:22:15
Subject:
commonName = Comsign Europe Intermediate N1 CA
organizationName = Comsign Europe Ltd.
countryName = EE
Subject Public Key Info:
Public Key Algorithm: ECC (384 Bits)
Public-Key: ECC (384 bit) X509v3 extensions:
Authority Information Access:
OCSP - URL=http://ocsp1.comsigneurope.com/ocsp

CA Issuers - URL=http://fedir.comsigneurope.com/cacert/ComsignEuropeIntermediateN1CA.crt
X509v3 Basic Constraints: critical
CA: TRUE, pathlen: 0
X509v3 Certificate Policies:
Policy: X509v3 Any Policy
CPS: http://www.comsign.co.il/repository

X509v3 CRL Distribution Points:

Full Name:
URL=http://fedir.comsigneurope.com/crl/ComsignEuropeN1RootCA.crl
Full Name:
URL=http://crl1.comsigneurope.com/crl/ComsignEuropeN1RootCA.crl
X509v3 Subject Key Identifier:
78dd043b5005f8ed2a45073c3a55917b0c6a708c
X509v3 Authority Key Identifier:
keyid: 51d604bce052d694ed8af4e3b37d31a21d1e8cb5
Signature Algorithm: sha384ECDSA

7.1.2.3 Subscriber Certificate

(1) An eIDAS Qualified Personal Certificate structure (Certificates for natural persons)

Field Name	Description	Example
Version	Certificate version	V3
Serial number	Certificate serial number. This number is single-value	Bc be ac 46 8b 09 ad e5 2d 31 ed f0 8e 02 00 ed ab
Signature algorithm	The signature algorithm used by the certificate owner. Hash algorithm will be SHA2 type	"sha2RSA"
Issuer	Fields describing the CA	
	Full name- CN	Comsign EIDAS CA
	CA name - O	"ComSign Europe Ltd."
	Country C	"EE"
Valid from	Date the certificate becomes valid (issue date)	Wednesday, January 4, 2023 10:08:37
Valid to	Expiration date	Monday, January 3, 2025 17:05:29
Subject Details of the certificate owner	Details of the individuals whose certificate was issued (the certificate owner)	
	CN (Full name of the certificate owner in English and their identity number)	"John Doe P_012345678"
	Family name (English) SN	Doe
	First name (English) G	John
	ID number SERIALNUMBER	01-012345678
	Organization name- O (identification code and ID)	07-012345678
	Subunit –OU (full name of the certificate owner in English)	Doe
	Position-T	Personal Certificate
	Country-C	"EE"
Public key	The length of the certificate owner's key	RSA (2048 Bits)
CRL Distribution Points	Link to the CRL	[1]CRL Distribution Point Distribution Point Name: Full Name URL=http://fedir.comsigneurope.com/crl/comsigneuropen intermediaten1ca.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl1. comsigneurope.com/crl/comsigneuropen intermediaten1ca.crl
qcStatements	1.3.6.1.5.5.7.1.3	This certificate is limited to 50,000 NIS
Authority Key Identifier	Key Identifier of the intermediate certificate	KeyID=727746 e93dcfebfcd37f02e5a22e38255cff0fb3
Certificate Policies	CPS for regulating the CA's (ComSign Europe) operation	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.61201.2.1.1 [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.ComSign.co.il/repository [1,2] Policy Qualifier Info: Policy Qualifier Id=User Notice

		Qualifier: Notice Reference: Organization=ComSign Europe Notice Number=11 Notice text= The certificate owner was identified in person on the basis of documents and/or other identifying information. The procedures of ComSign will apply to use of this certificate. The responsibility and liability of ComSign is limited as described in the procedures. Limitations on use of the certificate – optional
Enhanced Key Usage	The purposes for which the certificate is designated. These purposes change according to the type of certificate, signature and identification, respectively.	Secure Email (1.3.6.1.5.5.7.3.4) And/or Client Authentication (1.3.6.1.5.5.7.3.2) Smart card logon (1.3.6.1.4.1.311.20.2.2)
Subject Alternative Name Details of the authorized signatory Subject's alternative name	Details of the authorized signatory	
	E-mail address of the certificate owner RFC822 Name	".co.ee"
	Country C	"EE"
	Organization name- O (identification code and ID)	07-012345678
	Subunit- OU (full name of the certificate owner	
	Position T	Personal certificate
	Family name SN	Doe
	First name G	John
	CN (name and ID of the certificate owner	John Doe ID_012345678
[1] Authority Info Access		[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2(Alternative Name: URL=http://fedir.comsigneurope.com/cacert/ComSigneuropeintermediaten1CA.crt
Subject Key Identifier		07 19 61 9a d1 4e 07 71 06 25 a3 78 71 19 bc b3 0a 83 7c 5c
Key usage	Description of the purposes for which it is permissible to use the certificate.	Digital Signature, Non-Repudiation, Key Encipherment (e0)
Thumbprint Algorithm	The signature algorithm used to sign the certificate.	"sha2"
Thumbprint	Details of the certificate signed by the CA	e2 a1 5a 40 07 e4 a3 c3 88 66 91 14 5b 9c 00 ff e4 1d 24 8e
*at this stage- positions O and OU of _____ certificates are reversed (name of corporation=O)		

(2) Qualified Signature Certificate structure

(Certificates for natural persons\on behalf of legal persons in accordance with the eIDAS)**Field Name**	**Description**	**Example**
Version	Certificate version	V3
Serial number	Certificate serial number. This number is single-value	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 owner. Hash algorithm will be SHA2 type	"sha2RSA"
Issuer	Fields describing the CA	
	Full name- CN	Comsign EIDAS
	CA name - O	"ComSign Europe Ltd."
	Country C	"EE"
Valid from	Date the certificate becomes valid (issue date)	Thursday, June 29, 2023 15:37:06
Valid to	Expiration date	Tuesday, June 28, 2025 15:37:06
Subject Details of the authorized signatory of the corporation or public institution Subject	Details of the Authorized Signatory of a Corporation or Public Institution:	
	Full name (English)- CN	"John Doe P_012345678"
	Family name (English)- SN	John
	First name (English) G	Doe
	ID number- serial number	"01-012345678"
	O (identification code and thereafter corporation number)	05-519999999
	OU- name of the corporation/ public institution- English	Comda LTD.

	Position T	Manager
	Country C	"EE"
Public key	The length of the certificate owner's key	RSA (2048 Bits)
CRL Distribution Points	Link to the CRL	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://fedir.comsigneurope.com/crl/comsigneuropen1intermediateca.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl1. comsigneurope.com/crl/comsigneuropen1intermediateca.crl
QC Statement	1.3.6.1.5.5.7.1.3	30 48 30 3c 06 08 2b 06 0H0<..+. 01 05 05 07 0b 01 30 30 ......00 30 2e 81 29 54 68 69 73 0..)This 20 63 65 72 74 69 66 69 certifi 63 61 74 65 20 69 73 20 cate is 6c 69 6d 69 74 65 64 20 limited 74 6f 20 35 30 2c 30 30 to 50,00 30 20 4e 49 53 81 01 20 0 NIS.. 30 08 06 06 04 00 8e 46 0.....F 0b 01.
Authority Key Identifier	Key Identifier of the intermediate certificate	KeyID=18377087bc9eff25561a8fc938ac94204bf7109a
Certificate Policies	CPS for regulating the CA's (ComSign) operation	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.61201.2.1.1 [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.ComSign.co.il/repository [1,2] Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Reference: Organization=ComSign Europe Notice Number=11 Notice text= The certificate owner was identified in person on the basis of documents and/or other identifying information. The procedures of ComSign will apply to use of this certificate. The responsibility and liability of ComSign is limited as described in the procedures. Limitations on use of the certificate – optional In a certificate on behalf of a public institution: "An electronic certificate for _____ (name of the public institution) and to an authorized signatory on its behalf in the position _____ (description). This certificate is installed on an automatic signature system- in case the certificate was installed on the mentioned system.
Enhanced Key Usage	The purposes for which the certificate is designated. These purposes change according to the type of certificate, signature and identification, respectively.	Secure Email (1.3.6.1.5.5.7.3.4) And/or Client Authentication (1.3.6.1.5.5.7.3.2) Smart card logon (1.3.6.1.4.1.311.20.2.2)
Subject Alternative Name Details of the authorized signatory Subject's alternative name	Details of the authorized signatory	
	E-mail address r RFC822 Name	John@test.co.ee
	Country C	"EE"
	O identification number and corporation number	05-519999999
	OU- name of the corporation/ public institution	Comsign Europe Ltd
	Position T	manager
	Family name - SN	JOHN
	First name - G	Doe
	CN – full name and ID of the certificate owner	John Doe P_012345678
Authority Information Access		[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2(Alternative Name: URL=http://fedir.comsigneurope.com/cacert/ComSigneuropen1intermediateCA.crt
Subject Key Identifier		e4b822fc6327949194ac8792791524369be68049

Key Usage	Description of the permitted usages for the certificate	Digital Signature, Non-Repudiation, Key Encipherment (e0)
Thumbprint Algorithm	The signature algorithm used to sign the certificate.	"sha2"
Thumbprint	Details of the certificate signed by the CA	"f1 36 18 f7 fe 2a 1a 34 24 47 e6 7f 85 24 93 40 4d d5 18 73"
*At this stage- positions O and OU of _____ certificates are reversed (name of corporation=O)		

(3) Qualified Signature Certificate structure

(Certificates for natural persons\on behalf of legal persons in accordance with the eIDAS)

Field Name	Description	Example
Version	Certificate version	V3
Serial number	Certificate serial number. This number is single-value	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 owner. Hash algorithm will be SHA2 type	"sha2RSA"
Issuer	Fields describing the CA	
	Full name- CN	Comsign eIDAS CA
	CA name - O	"ComSign Europe Ltd."
	Country C	"EE"
Valid from	Date the certificate becomes valid (issue date)	Thursday, June 29, 2023 15: 37: 06
Valid to	Expiration date	Tuesday, June 28, 2025 15: 37: 06
Subject Details of the authorized signatory of the corporation or public institution Subject	Details of the Authorized Signatory of a Corporation or Public Institution:	
	Full name (English)- CN	"Joe Doe"
	Family name (English)- SN	John
	First name (English) G	Doe
	ID number- serial number	"01-012345678"
	O name of the corporation/ public institution- English	Comda LTD
	OIdentifier – organization's number	51444478
	Position T	Manager
	Country C	"EE"
Public key	The length of the certificate owner's key	RSA (2048 Bits)
CRL Distribution Points	Link to the CRL	
QC Statement	1.3.6.1.5.5.7.1.3	esi4-qcStatement-1 esi4-qcStatement-4 esi4-qcStatement-5 esi4-qcStatement-6.1
Authority Key Identifier	Key Identifier of the intermediate certificate	
Certificate Policies	CPS for regulating the CA's (ComSign) operation	
Enhanced Key Usage	The purposes for which the certificate is designated. These purposes change according to the type of certificate, signature and identification, respectively.	
Subject Alternative Name Details of the authorized signatory Subject's alternative name	Details of the authorized signatory	
	E-mail address r RFC822 Name	john@test.co.ee
	Country C	"EE"
	O identification number and corporation number	05-519999999
	OU- name of the corporation/ public institution	Comda
	Position T	Manager
	Family name - SN	John
	First name - G	Doe
	CN – full name and ID of the certificate owner	John Doe P_012345678
Authority Information Access		
Subject Key Identifier		e4b822fc6327949194ac8792791524369be68049
Key Usage	Description of the permitted usages for the certificate	Non-Repudiation
Thumbprint Algorithm	The signature algorithm used to sign the certificate.	"sha2"
Thumbprint	Details of the certificate signed by the CA	"f1 36 18 f7 fe 2a 1a 34 24 47 e6 7f 85 24 93 40 4d d5 18 73"

(5) Advanced Seal Certificate structure

Field Name	Description	Example
Version	Certificate version	V3
Serial number	Certificate serial number. This number is single-value	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 owner. Hash algorithm will be SHA2 type	"sha2RSA"
Issuer	Fields describing the CA	
	Full name- CN	Comsign eIDAS CA
	CA name - O	"ComSign Europe Ltd."
	Country C	"EE"
Valid from	Date the certificate becomes valid (issue date)	Thursday, May 22, 2023 15:37:06
Valid to	Expiration date	Tuesday, May 21, 2028 15:37:06
Subject Details of the authorized signatory of the corporation or public institution Subject	Details of the Authorized Signatory of a Corporation or Public Institution:	
	CommonName - CN	Comsign LTD
	Full Organization Name (English)- OrganizationName	"Comsign LTD"
	OrganizationIdetnifier	511111118
	Country C	"DE"
Public key	The length of the certificate owner's key	RSA (2048 Bits)
CRL Distribution Points	Link to the CRL	
QC Statement	1.3.6.1.5.5.7.1.3	esi4-qcStatement-4 esi4-qcStatement-5
Authority Key Identifier	Key Identifier of the intermediate certificate	
Certificate Policies	CPS for regulating the CA's (ComSign) operation	
Authority Information Access		
Subject Key Identifier		e4b822fc6327949194ac8792791524369be68049
Key Usage	Description of the permitted uses for the certificate	Digital Signature Non-Repuditaion
Thumbprint Algorithm	The signature algorithm used to sign the certificate.	"sha2"
Thumbprint	Details of the certificate signed by the CA	"f1 36 18 f7 fe 2a 1a 34 24 47 e6 7f 85 24 93 40 4d d5 18 73"

(6) Qualified Seal Certificate structure

(Certificates for legal persons in accordance with the eIDAS)

Field Name	Description	Example
Version	Certificate version	V3
Serial number	Certificate serial number. This number is single-value	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 owner. Hash algorithm will be SHA2 type	"sha2RSA"
Issuer	Fields describing the CA	
	Full name- CN	Comsign eIDAS CA
	CA name - O	"ComSign Europe Ltd."
	Country C	"EE"
Valid from	Date the certificate becomes valid (issue date)	Thursday, June 29, 2023 15:37:06
Valid to	Expiration date	Tuesday, June 28, 2025 15:37:06
Subject Details of the authorized signatory of the corporation or public institution Subject	Details of the Authorized Signatory of a Corporation or Public Institution:	
	CommonName - CN	Comsign LTD
	Full Organization Name (English)- OrganizationName	"Comsign LTD"
	OrganizationIdetnifier	511111118
	Country C	"EE"
Public key	The length of the certificate owner's key	RSA (2048 Bits)
CRL Distribution Points	Link to the CRL	
QC Statement	1.3.6.1.5.5.7.1.3	esi4-qcStatement-1 esi4-qcStatement-4 esi4-qcStatement-5 esi4-qcStatement-6.2
Authority Key Identifier	Key Identifier of the intermediate certificate	
Certificate Policies	CPS for regulating the CA's (ComSign) operation	

Authority Information Access		
Subject Key Identifier		e4b822fc6327949194ac8792791524369be68049
Key Usage	Description of the permitted usages for the certificate	Digital Signature Non-Repudiation
Thumbprint Algorithm	The signature algorithm used to sign the certificate.	"sha2"
Thumbprint	Details of the certificate signed by the CA	"f1 36 18 f7 fe 2a 1a 34 24 47 e6 7f 85 24 93 40 4d d5 18 73"

(7) Qualified Web Authentication Certificate structure

(SSL Certificates in accordance with the eIDAS)

Field Name	Description	Example
Version	Certificate version	V3
Serial number	Certificate serial number. This number is single-value	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 owner. Hash algorithm will be SHA2 type	"sha2RSA"
Issuer	Fields describing the CA	
	Full name- CN	Comsign eIDAS CA
	CA name - O	"ComSign Europe Ltd."
	Country C	"EE"
Valid from	Date the certificate becomes valid (issue date)	Thursday, June 29, 2023 15:37:06
Valid to	Expiration date	Tuesday, June 28, 2025 15:37:06
Subject Details of the authorized signatory of the corporation or public institution Subject	OrganizationName – Subject's name or DBA (OID – 2.5.4.10)	"Comsign LTD"
	StreetAdress (OID – 2.5.4.9)	"Dvora Hanevia 126"
	GivenName – (OID – 2.5.4.42)	Shlomo
	Surname – (OID 2.5.4.4)	Cohen
	LocalityName – (OID 2.5.4.7)	
	StateOrProvineName – (OID 2.5.4.8)	
	PostalCode - (OID 2.5.4.17)	
	CountryName (OID 2.5.4.6)	
	OrganizationUnitName – (OID 2.5.4.11)	
Public key	The length of the certificate owner's key	RSA (2048 Bits)
CRL Distribution Points	Link to the CRL	
QC Statement	1.3.6.1.5.5.7.1.3	esi4-qcStatement-1 esi4-qcStatement-5 esi4-qcStatement-6.3
Certificate Policies	CPS for regulating the CA's (ComSign) operation	2.23.140.1.2.2 0.4.0.194112.5
Enhanced Key Usage	The purposes for which the certificate is designated. These purposes change according to the type of certificate, signature and identification, respectively.	id-kp-serverAuth id-kp-clientAuth
Subject Alternative Name	DNS Name	Comsigntrust.com
Authority Information Access	Link to the OCSP responder + CA Certificate	
Subject Key Identifier		e4b822fc6327949194ac8792791524369be68049
Key Usage	Description of the permitted usages for the certificate	Non-Repudiation
Thumbprint Algorithm	The signature algorithm used to sign the certificate.	"sha2"
Thumbprint	Details of the certificate signed by the CA	"f1 36 18 f7 fe 2a 1a 34 24 47 e6 7f 85 24 93 40 4d d5 18 73"

7.1.3 Algorithm object identifiers (OIDs)

Comsign uses the following Hash algorithm:

SHA256 with RSA Encryption – OID 1.2.840.113549.1.1.11

ECDSA with SHA256 – OID 1.2.840.10045.4.3

7.1.4 Name forms:

Different names may appear in the Certificates issued by Comsign in accordance with Clause 3.1.

The names may be one of the following:

(1) Name of a person or an organization as it appears in the document used for identification, as described in Clause 3.2.
(2) Email address, according to standard RFC822.
(3) Distinguish name according to standard RFC1770, including fields such as O, CN, T, SN, G, C, OU.

7.1.4.1 Issuer Information

The content of the certificate issuer Distinguished Name field always matches the Subject DN of the Issuing CA.

7.1.4.2 Subject Information - Subscriber Certificates

By issuing a Certificate, Comsign represents that it followed the procedure set forth in its Certificate Policy and Certification Practice Statement to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate.

Comsign shall only include a Domain Name or IP Address in a Subject attribute according to the specifications in Clauses 3.2.2.4 and 3.2.2.5.

7.1.4.3 Subject Alternative Name Extension

See Clause 7.1.2.

Comsign shall not issue certificates for Reserved IP Addresses or Internal Names

7.1.4.4 Subject Distinguished Name Fields

For the possible fields of the subject DN see Clause 7.1.2.

All of the information present in the subject DN shall be verified according to Clauses 3.2.2 and 3.2.3.

The Subject DN fields shall only contain meaningful information that relates to the certificate owner and not metadata such as '.', '-', and ' ' (i.e., space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.

7.1.5 Name constraints:

Comsign does not limit names, provided that the names match the conditions described in Clause 3.1.

7.1.6 Certificate policy object identifier:

Electronic Certificates issued by Comsign conform to Comsign's policy that holds the following object identifiers:

(1) The policy for Certificate of natural entities:
OID 1.3.6.1.4.1.61201.1.1
(2) The policy for Certificate of servers according to the CAB/F– Domain Validation (DV)
OID 1.3.6.1.4.1.61201.1.2.1
(3) The policy for Certificate of servers according to the CAB/F – Organization Validation (OV)
OID 1.3.6.1.4.1.61201.1.2.2

Comsign may also use other policy identifiers such as OID 2.23.140.1.2.1, OID 2.23.140.1.2.2. These policies are specified in Clauses 7.1.2.3-**Error! Reference source not found.Error! Reference source not found.** and 7.1.2.3-**Error! Reference source not found.Error! Reference source not found.**

For details regarding policy identifiers in the root CA certificate, subordinate CA certificates or subscriber certificates see Clause 7.1.2.

7.1.7 Usage of policy constraints extensions:

No use is made of the policy constraints extension.

7.1.8 Policy qualifiers syntax and semantics:

Comsign indicates in the Certificate policy field a reference to this document and to the Certificates policy stated in it.

Comsign indicates in the Qualified Certificates statement (QC Statement) compatibility to Qualified Electronic Certificate standards, according to a specification of a number of international organizations, as described in Comsign's internal procedures.

When the electronic certificate is issued to a signature device stored on a network server, this shall be clearly stated in the certificate policies field of the Certificate. Whenever the network server is stored at a third-party facility, this shall be stated specifically in the certificate policies field of the Certificate. This is meant to provide a potential relying party full information concerning the storage of the signature device.

7.2 CRL profile

7.2.1 Version number(s):

The CRL files are in version 2.

7.2.2 CRL and CRL entry extensions:

CRL profile

Field name	Description	Example
Version		V2
Issuer	Fields describing the issuing CA	
	Name of CA- CN	e.g. "Corporations"
	Organization name O	"Comsign Europe Ltd.
	Country	"EE"
Validity	Fields describing the validity of the CRL	
	Effective Date - Date of publication of the CRL	Tuesday, July 28, 2020 09:59:40
	Next Update - Date of publication of the next CRL	Wednesday, July 29, 2020 10:34:40
Signature Algorithm	The signature algorithm used to sign the CRL.	sha256
Signature Hash Algorithm	The Hash algorithm used for the signature	Sha 256RSA
2.5.29.60 (Expired Certs On CRL)	The Expired certs that appear in the CRL	180F32303139303130313030303030305A
Authority Key Identifier	AKI of the issuing CA	KeyID=1fc697bcb197e9964fc8fb01af6fb56afda34f0f
CA Version		V0.0
CRL Numer	Monotonically increasing serial numberfor each CRL	CRL Number=0304
Revoked Certificates	Field describing the revoked Certificates	
Serial Number	The serial number of the Certificate. Single-value	"00 bc be ac 46 8b 09 ad e5 2d 31 ed f0 8e 02 ed ab""
Revocation Date	The date on which the Certificate was revoked	Tuesday, December 10th 2023 02:10:33
CRL Reason Code	The reason of the revocation	unspecified (0) key Compromise (1) cA Compromise (2) affiliation Changed (3) superseded (4) cessation Of Operation (5) Certificate Hold (6) remove From CRL (8) privilege Withdrawn (9) A Compromise (10)

7.3 OCSP profile

7.3.1 Version number(s):

The version of replies for OCSP requests is 1.

7.3.2 OCSP extensions:

Field name	Description	Example
OCSP Basic by Key Responder ID	The certificate that signed the response's SKI	029aa73a4c3f9e2d19b15eb3c77eaf34a3649552
Produced At	Date and hour of the response	6/16/2023 1:18 PM
Algorithm Object ID	The ID of the response's hash	1.3.14.3.2.26
Issuer Name Hash		
Issuer Key Hash		
Serial Number	the validated certiciate's Serial Number	3800000011d077e3ec54ea127e000000000011
Status	The requested certificate status	OCSP_BASIC_GOOD_CERT_STATUS
OSCP Response Info	The validity status of the Certificate	The following values can be accepted: [0] good [1] revoked [2] unknown
This update Next update	The start and end of the validity of the information source the OCSP responder uses	thisUpdate: 2016-12-07 08:00:17 (UTC) nextUpdate: 2016-12-08 08:00:18 (UTC)
Archive CutOff (1.3.6.1.5.5.7.48.1.6)	An extension that shows the certificate was valid in the point of time it was used	
Certificate 0	The certificate used for signing the OCSP response	signedCertificate version: v3 (2) serialNumber: 0x0e2bcda4aa4f8f…… signature (sha256WithRSAEncryption) Algorithm Id: 1.2.840.113549.1.1.11 issuer: ….. validity: ….. subject: …. subjectPublicKeyInfo: ….. extensions: …..

8. Compliance Audit and other assessments

8.1 Frequency or circumstances of assessment

Comsign maintains compliance with the eIDAS regulation and is also subject to internal procedures as well as to the audit and inspection procedures.

Audits are carried out annually.

Furthermore, to comply with standards ISO 27001 and ISO 9000/9001, as well as WebTrust standards audits shall be conducted by organizations that are licensed to conduct audits in accordance with the requirements of those standards.

eIDAS audits are carried out once every two years in accordance with the eIDAS requirements.

Comsign complies with all CAB\Forum requirements, including conducting periodical audits and reports.

8.2 Identity/qualifications of assessor

The assessor for compliance with CAB\Forum requirements is an auditor accredited by WebTrust and/or ETSI.

The assessor for eIDAS compliance is a qualified conformity assessment body accredited by a European Union member state national accreditation body against the requirements defined in the eIDAS regulation.

8.3 Assessor's relationship to assessed entity

The assessor is an independent contractor who does not work for Comsign nor is subjected to Comsign in any manner.

8.4 Topics covered by assessment

The topics for the WebTrust assessment are listed in WebTrust principles and criteria for certification authorities for Cas and for SSL

The topics of the eIDAS assessment are determined by the qualified conformity assessment body.

8.4.1 Topics covered by assessment of Certificate issuance to internet servers

When auditing the issuance of electronic certificates to internet servers the assessment shall also include at least one of the following audit formats:

(1) WebTrust for Certification Authorities v2.2 And up
(2) WebTrust for SSL Certificates V2.4.1 and up
(3) An assessment format complying with ETSI TS 102 042/ ETSI EN 319 411

The assessment shall be performed by an accredited auditor in line with clauses 8.2 and 8.3.

Prior to the Certificate issuance Comsign shall verify that the domain name and its control were verified in accordance with clause 3.2.2.4 or that the verification of the IP address as provided in clause 3.2.2.5 performed by a third party acting as Comsign's representative or Registration authority was:

(1) Performed by at least one person (not machine), or
(2) At least part of the verification of the domain name control was performed directly by Comsign.

If Comsign's representative is not Comsign's accredited Registration authority, the assessment shall include a review of the third party's activity and confirm that such activity fulfills these Procedures. In case the

assessment's results are negative, Comsign shall immediately cease all cooperation with the third-party concerning issuance of Certificates to internet servers.

The validity of the assessment shall not exceed 12 months.

8.5 Actions taken as a result of deficiency

Comsign shall review the assessment and shall correct whatever is required, if any, as soon as possible.

8.6 Communication of Results

The detailed assessment results are confidential and are not designated for publication, excluding the management of the CA and other functionaries in charge of those areas in which malfunctions/defect were located.

The WebTrust audit reports are published and available at Comsign's Repository at: www.comsign.co.il/repository

8.7 Self-Audits

During the period during which Comsign issues Certificates, Comsign monitors adherence to its Certificate Policy, Certification Practice Statement and strictly control its service quality by performing self-audits on at least a quarterly basis against a randomly selected sample of the greater of one certificate or at least three percent of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate issuance or renewal fees:

Comsign charges payment for issuance and renewal services of Electronic Certificates. The rates are subject to change from time to time and are affected by the service provided and the type of the Certificates. For the avoidance of doubt, it is noted hereby that changes in the rates of Comsign's services are not applied retrospectivly.

9.1.2 Certificate access fees:

Comsign does not charge payment for accessing Electronic Certificates of any type, if available.

9.1.3 Revocation or status information access fees:

Comsign does not charge payment for accessing the CRL.

9.1.4 Fees for other services:

Comsign is allowed to charge payment for different services required of it. The payment shall be charged according to the current rates at the time these services are provided.

9.1.5 Refund policy:

Subject to any law, a Certificate that was revoked due to a request of the Subscriber or for any other reason not related to Comsign, including a Certificate revoked as a result of its renewal for the period between the renewal and the original date of termination, does not entitle the Subscriber any refund in whole or in part.

9.2 Financial responsibility

9.2.1 Insurance coverage:

Comsign insures its professional responsibility.

9.2.2 Other assets:

Comsign provides the required guarantees and securities for its operations.

9.3 Confidentiality of Business Information

9.3.1 Scope of confidential information:

It is hereby clarified to the Subscriber that all the information appearing in the Certificate fields, even if considered as confidential business information by the Subscriber, shall not be considered as such and will not be protected. Therefore, the Subscriber is hereby advised to avoid including it in the Certificate fields non-required information that may be considered as confidential business information.

However, the Subscriber may be asked to provide Comsign with information concerning their business and its operation, whether for identification, payments, or their entitlement for a certain type of Certificate. Such information, which is not included in the Certificate fields, shall be kept in Comsign's archive as confidential information, and the access to it shall be limited to authorized individuals, and only in case a direct access is needed for performing their duties in the framework of issuing Comsign's Electronic Certificates.

It is hereby clarified that business information not included in the Certificates fields or in the CRL, and is usually considered as confidential, but was made public by the one authorized to do so, shall not be considered as confidential business information.

9.3.2 Information not within the scope of confidential information:

The content of the Electronic Certificate fields and the CRL, even if it is business information, shall not be considered as confidential information entitled to protection.

9.3.3 Responsibility to protect confidential information:

Comsign undertakes to maintain the confidentiality of the Subscriber's confidential business information and not to disclose it to any third party, unless required to do so by law.

9.4 Privacy of personal Information

9.4.1 Privacy plan:

Comsign complies with the GDPR regulations and has adopted a compliant privacy protection policy , and its updated provisions can be received at any time.

9.4.2 Information treated as private:

All the information regarding the Subscriber's identity and the records concerning the Electronic Certificate issuance, excluding information published in the Certificate fields, or in the CRL or was disclosed by an individual authorized to do so, shall be considered as confidential private information.

9.4.3 Information deemed private but not protected:

The content of the Electronic Certificates fields and the CRL, even though it is confidential private information, are not entitled to protection.

9.4.4 Responsibility to protect private information:

Comsign undertakes to maintain the confidentiality of the Subscriber's confidential private information and not to disclose it to any third party, other than as required by any law.

9.4.5 Notice and consent to use private information:

Comsign shall not use the private information that is considered confidential of the Subscriber which was provided to it in the process of issuing the Electronic Certificate, without an explicit consent of the Subscriber.

9.4.6 Disclosure pursuant to judicial or administrative process:

It is hereby clarified that Comsign shall comply with any binding instruction of judicial or administrative authority ordering it to disclose information, private or business, which was provided to it by the Applicant or the Subscriber, including information considered confidential. If applicable, and subject to any limitation or prohibition imposed on Comsign by an authorized authority requiring the information's disclosure, Comsign shall inform the Subscriber on the disclosure as per the mentioned instruction.

If Comsign is required to disclose confidential information of the Subscriber in the framework of procedures in which it is not a direct party or in case the Subscriber had asked to prevent the disclosure of the information and as a result Comsign sustained legal expenses, the Subscriber shall reimburse Comsign in the full these expenses.

9.4.7 Other information disclosure circumstances:

The limitations of confidential information disclosure shall not apply in case of audits.

9.5 Intellectual Property Rights

The property rights in the information and the data of this CPS and the structure of the Electronic Certificate issued by Comsign are considered Comsign's property and using them is only possible with the explicit written consent of Comsign.

9.6 Representation and Warranties

9.6.1 CA Representations and warranties:

Comsign declares that during its operation as a CA it shall ensure that the Certificate does not contain any factual misrepresentations of which Comsign is aware; there are no copying errors in the data, as received by Comsign from the Applicant, resulting from Comsign not taking reasonable precautions when creating the Certificate; the Certificate complies with all material requirements of these Procedures; all data stated in the Certificate or included in it by reference, other than the Subscriber's e-mail address, was verified by Comsign. After the Certificate is issued, Comsign shall not have an ongoing obligation to investigate and check the accuracy and correctness of the information included in the application for issuing a Certificate, unless Comsign receives explicit notification that one of the details appearing on the Certificate is incorrect. In this case, the Certificate shall be revoked, and it will be possible, at the request of the Subscriber, to issue a new Certificate that contains the updated information provided that while issuing this Certificate Comsign has complied with these Procedures.

Comsign shall not be held responsible for damage caused by relying on an Electronic Certificate that it issued, if it can prove that it took all reasonable precautions to fulfill its obligations according to this CPS. The responsibility of Comsign is, as noted, subject to the limitations listed below in this chapter. Without derogating from the above, Comsign is committed to provide the infrastructure and the Certificate issuing services, including the establishment, publication and operation of Comsign's Repository, in a trustworthy and accessible manner as detailed in these Procedures; provide the controls and foundation for Comsign's public key infrastructure (PKI), including protection of Comsign's keys, and maintaining the procedures for Confidentiality Partners, as stated in this CPS; implement the Certificate applications verifications procedures, as stated in this CPS; issue Certificates according to these Procedures and respect various representations made to Subscribers and relying parties in these Procedures; publish an accessible on-line list of revoked Certificates in Comsign's Repository for whomever wishes to rely on a particular Electronic Certificate, as described in these Procedures; fulfill the commitments of a CA and protect the rights of Subscribers and relying parties, according to these Procedures; revoke Certificates as required in these Procedures; handle Certificates renewal as described in these Procedures.

9.6.2 RA Representations and warranties:

Everything stated in Clause 9.6.1 above, shall also apply to the Comsign's Registration Authorities, as far as it is relevant to their activities. See clause 9.16 below.

9.6.3 Subscriber representations and warranties:

The Subscriber is obligated to provide Comsign with complete and updated information required for their identification or the identification of an authorized individuals on their behalf to issue an Electronic Certificate for their signature device; take every reasonable measures to keep the signature device under their full control and to prevent access to it and the use of it by other during the validity period of the electronic certificate; report to Comsign thereupon when their control in the signature device was harmed or was used by unauthorized individual or there was a change in the information or the details according to which the

Electronic Certificate was issued, and to comply with all the provisions, instructions and warnings stated in the Subscriber Agreement.

9.6.4 Relying party representations and warranties:

A relying party declares and undertakes that prior to relying on an Electronic Certificate or its information, they shall check and verify that the Electronic Certificate approving the signature on the electronic document is indeed valid, the limitation of use of the Electronic Certificates and that these limitations do not apply to the signed electronic message and that an authorized individual on behalf of a corporation or public institution was indeed authorized to sign on behalf of and commit the corporation or public institution.

A relying party that does not comply with these obligations shall solely bear any damage or expense caused to themself or to any one on their behalf or to a third party because of reliance of the relying party on an Electronic Certificate and Comsign shall not bear responsibility nor reimburse or compensate for any damage or expense.

9.6.5 Representations and warranties of other participants:

No Stipulation.

9.7 Disclaimers of warranties

Comsign and/or its representatives do not warrant that the Subscribers shall not deny the Certificate or any other message; do not warrant any software other than the technology and the software used by Comsign for the issuance of Electronic Certificates and to the device on which the signature device is installed if it was provided by Comsign; are not responsible to any damages caused by reliance on a revoked Certificate whose details were lawfully published in the CRL prior to the mentioned reliance and provided that they prove that they had taken any reasonable measures to fulfill their legal obligations and those stated in this CPS; are not liable to any indirect damage that stem from /or are connected to any use for any purpose in the Electronic Certificate and/or in the Electronic Signatures and the liability of Comsign and/or its representatives shall apply to direct damages only which stem naturally and during the regular course of affairs from noncompliance by Comsign with its obligations.

The Electronic Certificates are not intended for usage in control equipment under hazardous circumstances and/or for usages that require fail safe performance, such as the operation of nuclear units, aircraft navigation or communication systems, aviation control systems and/or weapon control systems and/or where failure may directly cause death or physical damage to both a person and the environment.

9.8 Limitation on liability

Comsign's liability is limited, including the types of Certificate usage or transaction amounts for which the Certificate may be used.

If the limitations are listed on the Electronic Certificate, Comsign and its representatives shall not be responsible for damage caused because of a use exceeding these limitations. Furthermore, Comsign may limit its liability toward a Subscriber in the Subscriber Agreement subject to any applicable law and this CPS. In all other instances, Comsign's liability shall not exceed the amounts and terms stated hereinbelow.

Limitations on the usage of the Certificate following the request of the Subscriber shall be imposed only upon an explicit request of the Subscriber solely.

Comsign may limit its overall liability for use of an Electronic Signature, and this limitation shall appear in a conspicuous manner on the Certificate and the Applicant shall be informed of this limit before the Certificate is

issued. Comsign shall publish its policy regarding limitations on its liability for different types of Certificates in a conspicuous place on its Internet site.

In any event, the total liability of Comsign and/or its representatives toward any party (including, inter alia, an Applicant, Subscriber or relying party) shall not exceed EUR 10,000 (ten thousand Euros) for all of the Electronic Signatures issued and all of the transactions related to a particular Certificate, and not exceed EUR 2,500 (two thousand five hundred Euros) for a single Electronic Signature issued and a single transaction related to that single signature.

The above limitation on damages and payment for damages applies to any type of loss and damage including direct damages, compensation, indirect damages, special and consequential damages, exemplary compensations or secondary damages caused to any person including the Applicant, Subscriber, a relying party or any third party and which are caused due to relying on or using a Certificate that Comsign issues, manages, uses, suspends or revokes, or for relying upon or using an expired Certificate. This limitation of damages or payment for damages also applies to contractual liability, tort liability and any liability claim. Subject to the aforementioned conditions, the liability limit for each Certificate shall be identical without regard to the number of Electronic Signatures, transactions or claims resulting from a specific Certificate. If the amount of claims exceeds the limit of liability, the limit of liability shall be allocated first to the earlier claims to reach a final settlement of the conflict, unless an authorized court instructs otherwise. In no event shall Comsign be obliged to pay an amount exceeding the total maximum liability sum for each Certificate, regardless of the method used to distribute maximum liability among several claimants.

9.9 Indemnities

The compensation liability, if set, shall not exceed the limitation mentioned in Clause 9.8 above.

9.10 Term and Termination

9.10.1 Term:

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

9.10.2 Termination:

Comsign's Procedures, as published from time to time, shall remain in force until replaced by a new version of the Procedures.

9.10.3 Effect of termination and survival:

Electronic Certificates shall be issued only in accordance with a valid CPS. No Electronic Certificates shall be issued subject to a non-valid CPS. The terms of a terminated CPS shall continue to apply on Electronic Certificates that were issued during the period of its validity.

9.11 Individual notices and communications with participants

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

From Comsign or a Registration authority to another person: To the most recent registered address. Each Registration authority of Comsign shall immediately notify Comsign of any legal notification received that might affect Comsign. The above mentioned does not apply to:

(1) Certificate revocation notices, as described in Clause 4.9 above.

(2) Notification inviting the Applicant to the enrollment process as described in Clause 4.1.2 above.

(3) Notification on the Certificate's upcoming termination date and the option of on-line renewal as described in Clause 4.6 above.

9.12 Amendments

9.12.1 Procedure for amendment:

This CPS may be amended by issuing a partial update. Each amendment to these Procedures shall be published in a manner that enables monitoring the date on which a document became valid and when the previous document or chapter became invalid. Amendments shall be applicable from the date of publication; however, this shall not impose additional obligations on a Subscriber to whom a Certificate was issued previously, based on a previous CPS and for as long as the Certificate remains valid. After an updated CPS is published, Subscribers are given a 60-day extension for filing objections, amendments or reservations – so that Comsign may consider them. Comsign shall send a written response to all comments received. There shall be no response to comments received more than 60 days after the updated CPS is published.

9.12.2 Notification mechanism and period:

An updated version of the CPS shall be published in the CA's website at the address: http://www.comsign.co.il/repository. Wherever major changes are applied to this CPS and/or the CP and/or the T&C Comsign shall put a notice in Comsign's website at the homepage – www.comsign.co.il

9.12.3 Circumstances under which OID must be changed:

Changes in this CPS shall not obligate a change of its OID- Object Identifier.

However, in cases where major changes apply that may require a distinction between versions Comsign shall change the OID at its sole discretion while the new OID shall be published in the next version and in the certificates issued since then.

9.13 Disputes resolutions provisions

Prior to using any kind of mechanism for conflict resolution (including legal proceedings or arbitration) in a dispute related to any aspect of these Procedures or to a Certificate issued by Comsign, the injured party shall notify Comsign, the Registration authority and any party to the dispute, so they can attempt to settle the dispute among themselves.

9.14 Governing Law

Comsign declares that these Procedures were formulated according to the ETSI EN 319 411 - 2 standard and the relevant Base Line Requirements of the CA-Browser Forum. To ensure uniform procedures and interpretation for all users, without reference to their place of residence or where their Certificates are used, the laws of the State of Israel shall exclusively apply without reference to other laws and/or rules regarding the choice of law, and without any requirement to establish a commercial connection to Israel. These Procedures are subject to the laws of the State of Israel.

9.15 Miscellaneous provisions

9.15.1 Entire agreement:

These Procedures replace all other previous texts, whether written or oral, and there shall be no validity, either explicit or implied, to any other text unless otherwise stated in these Procedures as amended from time to time.

9.15.2 Assignment:

Comsign may assign its rights and/or obligations as described in these Procedures to any other party.

9.15.3 Severability:

In the event of any contradiction between the provisions of the Subscriber Agreement and provisions of this CPS, the provisions of this CPS shall prevail. In the event of any contradiction between the provisions of the updated CPS, and a previous version of the CPS, the updated version shall prevail.

9.15.4 Enforcement (attorney's fees and waiver of rights):

These Procedures are binding and enforceable on the CA and every representative operating on its behalf, as well as the Subscriber, an authorized individual on their behalf, a relying party and every individual operating on its behalf.

No waiver, discount, rejection, extension or avoidance of action on an agreed date by Comsign and/or the Subscriber shall be interpreted as a waiver of their rights as they are stated in these Procedures, nor will it be used as an argument or debarment from any legal action on their behalf.

The headings of clauses and sub clauses in these Procedures comply with standard RFC 3647 and are presented only for the sake of convenience and reference, and may not be used for interpretation, or for enforcing the instructions of these Procedures. The appendixes, including the definitions of these Procedures, are an integral and binding part of these Procedures for all purposes.

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

9.15.5 Force Majeure:

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

9.16 Additional Arrangements – Registration authority

9.16.1 Introduction:

Some of the Certificate issuing services provided by Comsign may also be provided by representatives on its behalf. The representative acts at Comsign's discretion. Comsign's representatives shall participate in the services provided by Comsign for all matters relating to receiving and handling applications for Electronic Certificates, identifying Applicants, and registering them. Representatives of Comsign are obligated to comply with all the various requirements listed in this CPS.

The activities listed in Clause 3.2.2.4 are excluded from the authority of the Registration authority.

9.16.2 An application to act as a Comsign Registration authority:

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

(1) Name, address, fax and telephone numbers and e-mail addresses(s) of the Applicant, its administrative contact persons and its authorized representatives.

(2) Details of any information that might affect the reliability of the Applicant (for example, current or former insolvency) and which might materially influence the ability of the Applicant to act as a Registration authority for Comsign.

(3) If a corporation: Certified copies of the incorporation certificate, the corporation's founding documents, minutes of resolutions adopted by the appropriate bodies in the corporation regarding its appointment as a Registration authority for Comsign, and minutes authorizing the person appointed by the corporation to act as a representative and undertake on its behalf in any matter regarding the appointment of the corporation as a Registration authority for Comsign.

(4) If a corporation: An attorney's statement on the corporation's field of activity, the identity of the corporation's representative who is authorized to make commitments on its behalf and confirmation that the decisions of the relevant corporate bodies regarding its appointment and functioning as a Registration authority for Comsign are valid, bind the corporation and were adopted in accordance with the corporation's incorporation documents and resolutions.

(5) A declaration by the Applicant that it will fulfill the requirements of the Procedures, and an undertaking by the Applicant to comply literally with the instructions of this CPS.

(6) Any other information required by Comsign. The representative who submits the application shall take all required steps and shall sign all documents required to receive Comsign's approval for the appointment as a Registration authority for Comsign.

9.16.3 The address for applying to act as a Registration authority for Comsign:

Applications to act as a Registration authority for Comsign, containing all documents and information required by Comsign, approved and verified by an attorney (including additional information as required) shall be submitted to the offices of Comsign Ltd.