General Terms and Conditions for the Use of Comsign's Qualified Trust Services

Comsign Ltd.

Version 1.1

Publication Date: 08.06.2023

Mailing address: P.O.B 58077, Kiryat Atidim, Tel Aviv 6158001, Israel

Office address: Building #4, Kiryat Atidim, Tel Aviv 6158001, Israel

Telephone: 972-3-6485255.

Fax: 972-3-6474206

Email: info@comsign.co.il

Document History		
Version	**Date**	**Description**
1.0	18.05.2021	Original Version
1.1	08.06.2023	OID Updates

Table of Contents

1. Information of the Version and Definitions

1.1. Name of Document and Identification

This document shall be named "General Terms and Conditions for the use of Comsign's Trust Services". This document can be viewed at: http://www.comsign.co.il/repository.

1.2. Definitions and acronyms

Authentication	Verification of a person's alleged identity.
Certification Authority (CA)	The part of Comsign's hierarchy responsible for issuing and verifying electronic certificates and certificates revocation lists using its electronic signature.
Certificate or **Electronic Certificate**	An electronic batch that includes information about the identity of the Public Key owner (in the context of this document, the "Subscriber") and the electronic signature of the CA that has verified the Certificate's contents.
Certificate Policy (CP)	Comsign's Certificate Policy for Qualified Certificates.
Certification Practice Statement (CPS)	The document stating the practices and regulating the activity of Comsign as a Trusted Service Provider (TSP)/CA in providing certification services for Qualified Certificates for Qualified Electronic Certificates and Seals. The document can be viewed at http://www.comsign.co.il/repository
eIDAS Regulation	Regulation (EU) No. 910/2014 [repealing Directive 1999/93/EC] of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.
Electronic Seal / Qualified Electronic Seal	A batch attached by a legal entity to an electronic document or other data which ensures the data's or any other digital asset's origin and integrity. See eIDAS. Electronic Seals can be incorporated in processes executed automatically in a digital environment. A qualified electronic seal is an electronic seal that is compliant to eIDAS thus must be created by a qualified electronic device and based on a qualified certificate for electronic seal.

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 required by the Law, as part of the public key infrastructure.
(The) Law	The Israeli Electronic Signature Law 2001.
Local Registration Authority (LRA)	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.
OCSP	Online Certificate Status Protocol.
OID	A unique identifier of an object
OCSP	Online Certificate Status Protocol.
OID	A unique identifier of an object
(The) Parties	Comsign, its representatives and the Certificates users, namely the Subscriber and the Relying Party.
PIN code	A code used to activate Qualified Certificates for Electronic Signatures and Electronic Seals.
Qualified Electronic Certificate	A Certificate issued by a CA which has been accredited and supervised by authorities designated by a EU state (in Israel the Registrar) and meets the requirements of eIDAS and the Law.
Qualified Electronic Signature	An advanced electronic signature created by a qualified electronic signature creation device and issued a Qualified Certificate.
QSCD	A Secure Signature Creation Device that meets the requirements laid down in chapter II of the eIDAS Regulation. QSCD can be either local in the form of a USB token or a smart card or Remote in the form of a Hardware Security Module
Qualified Trust Service	A trust service, as defined in eIDAS Regulation, that meets the applicable requirements laid down in that regulation.
Qualified Trust Service Provider	A trust service provider (TSP) who provides one or more qualified trust services and is granted the qualified status by the supervisory body.

(The) Registrar	Registrar of Certification Authorities appointed to office according to the Law and its Regulations. The Registrar serves as a supervisory body for Qualified Trust Service Providers.
Revoked Certificate	A Certificate that appears on the Certificates Revocation List (CRL) in the Comsign Repository.
Relying Party	A third party who receives a message signed with a Qualified Electronic Signature and who takes action or refrains from action on the basis of 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. Known a Private Key in the PKI hierarchy.
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. Known a Public Key in the PKI hierarchy.
Subscriber	An entity requiring the services provided by a TSP and which has explicitly or implicitly agreed to its terms and conditions.
Subscriber Agreement	Agreement between Comsign and the Subscriber for use of the trust services provided by Comsign as a TSP.
Valid Certificate	A Certificate that appears on the list of valid Certificates in the Comsign Repository
X.509	X.509 is a format for certified Public Key's, which are suitable for use in various Public Key Infrastructure systems.

2. General Terms

2.1 Comsign Ltd. (the "**Company**" or "**Comsign**") is a qualified certification authority acting in accordance with the Law. The Company further applies the eIDAS Regulation as well as European and international standards. The Company provides its subscribers with trust services, as well as Qualified Trust Services, including Qualified Certificates for electronic signatures. The Company's trust services are based on a PKI infrastructure and on reliable data and are intended to provide reliable and trustworthy trust services and certificates for electronic users. The electronic certificate issued by the Company as a TSP identifies the Company as the issuing authority.

2.2 The Company as CA may operate through others acting as LRA'a on its behalf and under its responsibility. The Company operates under the supervision of the Registrar and abides by eIDAS.

2.3 The Company acts as an independent third party that implements policies and practices detailed in its CPS and CP that constitute a legally binding contract between the Company and Subscriber while using such services and for the Relying Party, while relying on issued Certificates. Thus, the Subscriber must be familiar with these Terms and Conditions and accept them.

2.4 The Subscriber and the Company have executed a Subscriber Agreement, which includes the present Terms and Conditions, and where all specific service conditions are detailed. In case of conflict between the Subscriber Agreement and this document, the provisions of the Subscriber Agreement shall prevail.

2.5 This document can be amended by the Company at any time subject to the publishing of the amended document and a 14 days adjustment period prior to its coming into effect.

2.6 The Company may refuse the issuance of the Certificate at its sole discretion.

3. Certificate types, acceptance and usages

3.1 **Certificates**

a) The Company issues the following Certificates:

- Qualified Electronic Signature (on a QSCD) for natural person.

  OID: 1.3.6.1.4.1.19389.2.2.1

- Qualified Electronic Signature (on a QSCD) for a natural person authorized by a legal person. OID: 1.3.6.1.4.1.19389.2.2.1
- Qualified Electronic Seal (on a QSCD) for legal person. OID: 1.3.6.1.4.1.19389.2.2.2
- Qualified Electronic Web Authentication Certificate. OID: 1.3.6.1.4.1.19389.2.2.3

b) Upon submitting an application for a Certificate, the Subscriber confirms that he/she is familiar with and accepts the Terms and Conditions.

c) The following acts constitute Certificate acceptance for Qualified Electronic Signature and Qualified Electronic Seal:

- The issuance of the Certificate to the Subscriber and his/hers verification of the Certificates data constitutes the Subscriber's acceptance of the Certificate. In the event of a valid Certificate renewal – verification is not required. Use of the Certificate by the Subscriber may also constitute acceptance.
- For an Electronic Seal Certificate, failure of the Subscriber to object to the Certificate or its content within 24 hours from downloading it, constitutes Certificate acceptance.

d) All Certificates will be valid beginning the day and hour of their issuance by Comsign. The Certificate will be valid for the term stated in the Subscriber Agreement, unless the Certificate is revoked or renewed earlier. The validity period may range up to 4 years.

4. Prohibited Usage

4.1. Use of the Certificates for electronic signatures and seals is limited as per Comsign's CPS. Additionally, usage limitation may be explicitly requested by the Subscriber. These limitations appear in the Certificate Policy field.

4.2. Subscribers are exclusively responsible to the legality of the uses of the Certificates in any jurisdiction in which the contents of the Certificates are available or reviewed. 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 Subscribers must follow the laws in any jurisdiction in which the Certificate is used or its contents are available.

5. Reliance Limits

5.1. The size of the signing device (private key) of the TSP is at least 2048 bits and it is installed on a reliable hardware component (at least FIPS 140-1 Level 3). The key pair are valid for at least 4 years from date of issue. The key pair may be replaced prior to the date of expiration, inter-alia for reasons of legal changes as well as changes in the guidelines defining the size and/or the type of algorithm of the Company's signing device (private key), or for any other reason requiring such replacement. Whenever a replacement takes place, the Company will publish its new public key in its repository.

5.2. Comsign's signature device fulfills all of the following:

a) It is based on a RSA or DSA key of at least 2048 bits.

b) It is protected with a device satisfying, at least, FIPS 140-2 level 3 requirements.

c) It is backed up using protected and secured means, to the satisfaction of the Registrar; the backup is separately kept.

d) It fulfills whatever additional requirements of the Registrar designed to maintain a reasonable level of security against breach, disruption or mal use.

5.3. Audit logs are retained for no less than 25 years. Records related to the Certificates are stored for at least 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. Documents and information received from Subscribers and Applicants are stored for a period of at least 25 years.

5.4. The information in the Certificates is correct. There are no errors or material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate.

5.5. Certificates become valid as of the date specified in them. The validity of the Certificate expires on the date of expiry indicated in the Certificate or if the Certificate is revoked.

6. Obligations and Liability of Subscribers

6.1. The Subscriber is obligated to use the Certificate in compliance with the Terms and Conditions, the CPS, the Subscriber's Agreement and the Law. The Subscriber shall be solely liable for any damage caused due to failure to abide with the above requirement.

6.2. The Subscriber must submit the Company with accurate, true and complete information and identification documents with respect to the issuance of the Certificate as well as immediately update the Company in the event of any change or event that may require the revocation of the Certificate.

6.3. The Subscriber is solely and fully responsible for any consequence of using the Certificate during and after the validity period.

6.4. The subscriber must protect and control his/her Private Key and the component embedded with the Certificate from risks of damage, loss, disclosure, change or unauthorized use. The Subscriber must immediately inform Comsign of a possibility of unauthorized use of his/her Private Key or if his/her Private Key has been lost, stolen, potentially compromised or if control over his/her Private Key has been lost due to a compromise of authentication credentials (e.g. PIN, PUK, username, password, OTP) or other reasons and immediately revoke his/her Certificate. The Subscriber must immediately discontinue the use of a compromised Private Key.

6.5. The QSCD may be supplied by the Company or by the Subscriber. In the event the QSCD is supplied by the Subscriber, the Company reserves the right to refuse issuing a Certificate on a QSCD that, in the Company's professional discretion, does not comply with legal and other standards that apply to Qualified Certificates.

6.6. The subscriber undertakes not to copy, duplicate or reverse engineer the technology used by the Company in providing the Qualified Certificates.

6.7. A subscriber wishing to limit the usage of its issued Certificate, must advise the Company in writing and refrain from any use of the Certificate prior to verifying that the Company embedded the limitation in the Certificate in a manner accessible to any relying party.

7. Obligations and Liability of a Relying Party and Status Checking

7.1. The Relying Party is obligated to study the risks, liabilities, limitations and uses related to the acceptance of the Certificate, which are set out in the CPS and the present Terms and Conditions. A Relying Part acknowledges that he/she has access to sufficient information to ensure that he/she can make an informed decision as to the extent to which he/she will chose to rely on the information in a Qualified Certificate. A RELYING PARTY IS RESPONSIBLE FOR DECIDING WHETHER OR NOT TO RELY ON THE INFORMATION IN A QUALIFIED CERTIFICATE.

7.2. The Relying Party is obligated to verify the validity status of the Certificate of the Electronic Signature or Electronic Seal by reference to the CRL or OCSP service located in the certificate.

7.3. A Relying Party should take into account all limitations stated within any Certificate issued by Comsign and make sure that the transaction to be accepted corresponds to the relevant CP and CPS.

7.4. Qualified Certificates shall be used only to the extent that use is consistent with applicable law. Qualified certificates are not designed, intended, or authorized for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage.

8. Obligations and Liability of Comsign

8.1. Without prejudice to the terms of this Section 8, Comsign undertakes to provide its Trust Services in accordance with the Law, its CPS and CP and these Terms and Conditions.

8.2. The Company may limit its liability, including the types of usage or the transactions amounts employing the Trust Services. The Company shall not be liable for any damages resulting from usages exceeding the limits stated on the Certificate. Furthermore, the Company may limit its liability toward Subscribers in the Subscriber Agreement.

8.3. However, the Company's limit of liability may not contradict the Law, the terms of the CPS and the rules regulating the Company's activity as a Qualified CA.

8.4. Limitations on the usage demanded by a Subscriber require the Subscriber's explicit request.

8.5. The Company and/or its representatives –

8.5.1. Do not warrant that a subscriber will not an electronic message signed by a Qualified Certificate.

8.5.2. Do not warrant the proper state and/or compatibility to standards and/or to any rule of law of any software other than the technology and software serving the Company's issued Certificates if supplied by the Company.

8.5.3. Are not responsible for any damages caused as a result of relying on a non-valid Certificate, provided the Company proved it employed all reasonable measures needed to fulfill its duties according to the Law and the CPS.

8.5.4. Are released from any liability for indirect and/or consequential damage of any type, and are only responsible for direct damage, not exceeding the Certificate usage limitations, resulting from reliance on a Certificate seemingly in proper state that was proven to be faulty.

8.6. Certificates are not intended for use with control equipment and/or with usages requiring fail proof performances such as nuclear facilities, air navigation, communication systems, air control systems, weapon control systems and/or any failure that may directly result with death, bodily injury or environmental damage.

8.7. The Company and its representatives shall not be liable for any breach of duty, delay or refraining from performing Trust Services, resulting from events outside their control, such as force majeure, wars, economy emergency periods, plagues, electricity stoppages not within the control of the Company and its representatives, earthquakes and other disasters, provided the Company and its representatives were not able to reasonably prepare to these events.

8.8. Whenever the Certificate issued by the Company is part of an electronic message signed by a Qualified Electronic Signature certified with a Qualified Electronic Certificate issued by the Company in its capacity as a Qualified CA, the Company's liability for the Certificate shall not exceed its total combined liability as a Qualified CA. In any other event, the total liability of the Company and its representatives toward the Parties shall not exceed NIS 50,000 (fifty thousands) for all transactions executed or related to the same Certificate and not more than NIS 10,000 (ten thousands) for a single transaction executed or related to a certain Certificate. Such limit also applies to any contractual, in tort or any liability claim. In the event the amount of claims exceeds the limit of liability, the liability limit shall first be applied to earlier claims in order to finally settle them, unless a competent court orders otherwise. In no event shall the Company be liable to pay any amount exceeding the total limit of liability for any specific Certificate, without allocating the payment between the numerous claimants.

8.9. The Company shall inform the Subscriber before it terminates the service of Qualified Certificates and shall maintain the documentation related to the terminated services and information needed in accordance to the process established in the CPS and these Terms and Conditions.

9. Privacy policy and confidentiality

9.1. The Company adheres to and enforces a data protection policy when handling personal information and logging information.

9.2. All information that has become known while providing services and that is not intended for publication (e.g. information that had been known to the Company because of operating and providing the Qualified Certificates) is confidential.

9.3. The Company protects confidential information and information intended for internal use from compromise and refrains from disclosing it to third parties by implementing different security controls.

9.4. Disclosure or forwarding of confidential information to a third party is permitted only with the written consent of the legal possessor of the information based on a court order or in other cases provided by the applicable legislation.

10. Refund Policy

Subject to any applicable law, a Certificate that was revoked due to a request of the Subscriber or for any other reason no related to Comsign - does not entitle the Subscriber any refund in whole or in part.

11. Law, Jurisdiction and dispute resolution

11.1. The Certificate, in all aspects, is governed by the laws of the State of Israel without reference to other laws and/or rules regarding the choice of law, and without any requirement to establish a commercial connection to Israel. The choice of law was made to ensure uniform procedures and interpretation for all users, without reference to their place of residence or where their Certificates are used.

11.2. Comsign declares that these terms and conditions were formulated according to the relevant ETSI and Base Line Requirements of the CA-Browser Forum.

11.3. 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 must notify Comsign, the LRA and any Party to the dispute, so they can attempt to settle the dispute among themselves.

12. Contact information

Comsign Ltd.
Mailing address: P.O.B 58077, Kiryat Atidim, Tel Aviv, 6158001 Israel.
Office address: Kiryat Atidim, building 4, 6158001, Tel Aviv, Israel.
Tel: 972-3-6485255.
Fax: 972-3-6474206.
Email: Support@Comsign.co.il; info@comsign.co.il.