Comsign Ltd.

PKI Disclosure Statement

For the issuance of electronic certificates for qualified electronic signatures, Domain Names and Internet Servers

Version 1.1

Dated: 17.16.2021

Table of Contents

1. INTRODUCTION

Comsign Ltd. (Comsign) is a Certification Authority (CA) registered and licensed in Israel under the Israeli Electronic Signature Law 2001 and supervised and regulated by the Israeli CA Registrar appointed by the Israeli Ministry of Justice (Registrar).

In addition to the Registrar, Comsign is recognized as a trusted CA by Microsoft, Adobe and Apple.

Comsign CA activity is based on a Public Key Infrastructure (PKI).

The procedures under which Comsign operates are defined in Comsign's Certification Practice Statement (CPS) and the policy requirements on the management of the CA activity are defined in Comsign's Certificate Policy (CP).

Comsign's CPS is available at: www.comsign.co.il/repository

Comsign's CP is available at: www.comsign.co.il/repository

The main participants in the PKI are the CA, the Certificate Holder and the Relying Party.

The purpose of this PKI Disclosure Statement (PDS) is to summarize the key points of the CP for the PKI participants.

As a rule, terms used in this document are defined in the CP or in the CPS.

2. CONTACT INFORMATION

The person in charge of the application of the policy and the procedures at Comsign is the Security Officer. E-mail address: security@Comsign.co.il. Mailing address: 11th floor, Building 4, P.O.B. 58007, Kiryat Atidim, Tel Aviv 6158001 Israel. Tel. 972-3-644-3620, Fax. 972-3-649-1092.

Information concerning qualified Electronic Certificates and assistance is available by email: support@comsign.co.il additional assistance is available by email from Customers Services: customer_services@comsign.co.il Tel: 972-3-6443620 Fax: 972-3-6491092.

3. CERTIFICATE TYPES

Comsign issues Qualified Certificates for electronic signatures by individuals and authorized signatories on behalf of corporations and legal institutions. These Qualified Certificates for qualified electronic signatures are regulated under the Israeli Electronic Signature Law 2001.

In addition, Comsign issues electronic certificates for secured electronic signatures as well as qualified electronic certificates for legal entities and legal seals as such as well as SSL certificates for domain names and internet servers. However, these certificates, although qualified under the European Telecommunications Standards Institute ("**ETSI**") and the Certification Authority Browser Forum ("**CAB Forum**") standards and baseline requirements, are not issued under the terms of the Israeli Electronic Signature Law 2001 and are not recognized, as such, by this Law. Notwithstanding, the link between the physical person or the Legal Entity and the public key is certified and the Applicant must submit proof of his identity and valid documents proving his

mandated responsibility, the existence of the legal entity and control over the domain name or internet server, as applicable.

4. VERIFICATION PROCEDURES

When issuing a Certificate for a Qualified Electronic Signature to an individual or to a signatory on behalf of a Corporation or public institution under the Israeli Electronic Signature Law 2001, the physical presence of the Applicant is mandatory at the initial registration and issuance. Physical presence is not required during renewal of a valid Certificate (prior to its expiry). The identity of the individual is verified on the basis of official identification documents. The legal status and validity of corporations and public institutions is verified based on official registrations and additional official documents. In case of an authorized signatory on behalf of a corporation or public institution, the appointment and authorization are also verified.

When issuing an SSL or EV SSL Certificate, the physical presence of a natural person is not required and the verification process takes place based on available data bases as well as other unique verification procedures.

The specific procedures dealing with verification are detailed in Comsign's CPS and CP as well as in internal procedures.

5. USE OF CERTIFICATES

The use of the Certificate is the sole responsibility of the Subscriber and is intended for legal uses only.

The limitations of the uses of the Certificate may be determined by Comsign or upon an explicit request of the Subscriber. These limitations appear in the Certificate Policy field.

Subscribers are exclusively responsible to the legality of the uses of the Certificates issued by Comsign in any jurisdiction in which the contents of the Certificates are available or reviewed. Thus, Applicants and Subscribers must 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 must follow the laws in any jurisdiction in which the Certificate is used or its contents are available.

6. OBLIGATIONS OF APPLICANTS AND SUBSCRIBERS

The Applicant is always a natural person applying on behalf of him/her self as individual, or as an authorized signatory on behalf of a corporation or on behalf of a legal entity. Once the application for Certificate has been approved and the Certificate was issued, the Certificate holder becomes a Subscriber of Comsign's CA services. As such, all of the following apply and obligate the Applicant and Subscriber (as applicable):

a. The Certification Practice Statement (CPS) currently in effect, as drafted by the CA and setting out the procedures used for providing electronic Certificates.

b. The CP.

c. Israeli law in all matters related to the contractual agreement with the Comsign..

d. Provide accurate, complete and precise data and meet the requirements for the type of Certificate issued and in particular the relevant registration procedures.

e. When using the Key Pair, comply with any limits and constraints indicated in the Certificate or in a contractual agreement.

f. The key-pair generation must be undertaken in accordance with the CP, using an algorithm and key length that meet the criteria set out in the CP and the relevant contractual agreements.

g. The Certificate holder is the sole holder of the private key linked to the public key to be certified.

h. When applicable, the key-pair must be generated using an SSCD and the Certificate must be used to create signatures solely by means of this device.

i. Protect the Private Key at all times against loss, disclosure, alteration or unauthorized use. Once the Private and Public key pair have been created, the Subscriber is personally responsible for ensuring the confidentiality and integrity of the Key Pair. The Subscriber is deemed the sole user of the Private Key. The PIN (Personal Identity Number) or password used to prevent unauthorized use of the Private Key must never be compromised or stored under non-secure conditions. The Subscriber holds sole liability for the use of the Private Key. Comsign is not liable for the use made of the Key Pair belonging to the Subscriber.

j. The Subscriber must demand Comsign to suspend or revoke the Certificate as required pursuant to the relevant CPS and the Subscriber's Agreement and application forms.

k. Revocation of a Certificate takes place with immediate effect. The suspension and revocation procedures are set out in the CPS and the CP.

l. The Subscriber agrees to the publication of the issued Certificate in the relevant CA register (when applicable). The list of revoked (and suspended) certificates (CRL) is open to the public. The list of valid certificates is not open to public review.

m. The Subscriber must verify the accuracy of the content of the Certificate published immediately following its receipt and prior to first use. The Subscriber must immediately notify Comsign of any inconsistency noted between the information in the Subscriber Agreement and application forms and the content of the Certificate. Use of the Certificate by the Subscriber constitutes approval by the Subscriber of the Certificate, its operation and its contents.

n. The Subscriber agrees to the retention, for a period of 25 years from the date of expiry of the Certificate, by Comsign of all information used for the purposes of registration, for the provision of a SSCD or for the suspension or revocation of the Certificate, and, in the event that Comsign ceases its activities, the Subscriber permits this information to be transmitted to third parties acting as substitute CAs under the same terms and conditions as those laid down in the CPS, CP and contractual agreements.

When the Certificate is issued to a signatory on behalf of a legal entity (or natural person when applicable), the authorizing entity will be considered as Subscriber and the

following shall apply:

o. The legal entity, represented by its authorized officer, must give its consent to the issue of a Certificate to its authorized Certificate Holder representative and for the Certificate attesting to the professional status of the Certificate Holder representative with respect to the legal entity.

p. When applicable, the legal entity accepts and assumes all liabilities and responsibilities of the Certificate Holder representative and its use of the Certificate on behalf of the legal entity.

q. The legal entity must agree to:

- The CPS and CP.
- The application forms and Subscriber's Agreement.
- Choice of law – Israeli law.
- Being responsible for the accuracy of the data it transmits to Comsign for the purposes of registration of the Certificate Holder representative. The legal entity must immediately inform Comsign of any change to this data, and the latter will then take appropriate action.

r. Comsign may revoke or suspend a Certificate based on a request by the legal entity.

7. OBLIGATIONS OF RELYING PARTIES

Third parties who rely on Certificates issued in accordance with the CPS and CP must:

a. Verify the validity of the Certificate and the Certificate of Comsign as well as the complete certification chain by checking against the appropriate Certificate Revocation Lists (CRLs).

b. Fully consider all the limitations on the use of the Certificate specified in the Certificate, in the CPS and CP.

c. Take all other precautions with regard to use of the Certificate set out in the CPS and CP or elsewhere.

8. LIMITATIONS OF WARRANTY AND LIABILITY

By issuing a Certificate, Comsign makes the certificate warranties listed herein to the following Certificate Beneficiaries:

a. The Subscriber that is a party to the Subscriber Agreement for the Certificate;
b. All Application Software Suppliers with whom the Root CA has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier; and
c. All Relying Parties who reasonably rely on a valid certificate.

Comsign represents and warrants to the Certificate Beneficiaries that, during the period when the Certificate is valid, ComSign has complied with its Certificate Policy and Certification Practice Statement in issuing and managing the Certificate.

Comsign will not be held responsible for damage caused by relying on an Electronic Certificate that it issued, if it can prove that it took all reasonable precautions to fulfill its obligations according to the Israeli Electronic Signature Law 2001, the CPS and CP and the Subscriber Agreement. The responsibility of Comsign is subject to the limitations listed in the CPS and CP and the Subscriber Agreement

9. CONTRACTUAL RELATIONS – SUBSCRIBER AGREEMENT, CPS AND CP

The Relationship between the Subscriber and Comsign is defined in the Subscriber Agreement, and further regulated, when applicable by the Israeli Electronic Signature Law 2001. By reference of the Subscriber Agreement and the reliance on the Certificate and the data included therein, Comsign, the Applicant, the Subscriber and the Relying Party accept the contractual binding effect of the terms and conditions contained in the CPS and CP,

10. PERSONAL DATA PROTECTION

Personal data communicated to Comsign by the Applicant are entered into a file held by Comsign. The data are used solely for the provision of Comsign CA services. The Subscriber has the right to inspect and, where necessary, rectify this data.

11. REFUND POLICY

The sole remedy available to the Subscriber for a revoked certificate due to fault of Comsign is the issuance of a substitute certificate. No remedy is available for revocation or suspension of a Certificate for any other reason.

12. DISPUTE RESOLUTIONS AND CHOICE OF LAW

In the event of technical problems relating to the Certificate or complaints about the CA services provided, the Subscriber may contact Comsign's helpdesk:

Comsign Ltd.

Telephone number: +972 3 644 3620

e-mail address: support@comsign.co.il

In the event of disputes relating to the validity, interpretation or performance of the Agreement concluded between them, Comsign and the Subscriber must make every endeavor to find an amicable solution. If no amicable solution can be found, any dispute concerning the validity, interpretation or performance of the Agreement binding the parties must be brought before the courts of Tel Aviv, Israel with the law of the State of Israel to apply. As provided in the CPS, the Israeli substantive law and procedures and the legal venue of Tel Aviv, Israel are exclusive and exclude all other jurisdictions, laws and regulations and are binding on Comsign on one hand and all other parties, including third and relying parties,

on the other hand.

13. QUALIFICATIONS, AUDITS, INSPECTIONS

Comsign is a Certification Authority licensed as such by the Israeli CAs Registrar and authorized to issue qualified electronic certificates to qualified signatures as such terms are defined under the Israeli Electronic Signature Law 2001. Comsign is further recognized by Adobe, Apple and Microsoft as a trusted service provider for electronic certificates and listed on the list of trusted root certificates authorities of these corporations.

During the period in which Comsign issues Certificates, Comsign will monitor adherence to its Certificate Policy, Certification Practice Statement and the CA/Browser Forum Requirements 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.

Comsign is subject to the audit and inspection procedures in accordance with the Israeli Electronic Signature Law 2001 and its Regulations. This audit is carried out annually, and if necessary, upon the Registrar's request at a more frequent rate.

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

In the event a Qualified Electronic Certificates is issued on a signature device stored in a signature server held by a third party, an inspection of the software installed on the signature server will be carried out by an applicative data security expert prior to the issuance, as well as an inspection of the overall formation by a data security assessor and by the auditor. If the same software and the same formation are used repetitively by different clients, there is no need for a follow-up audit.

Comsign complies with all CAB Forum requirements, including conducting periodical audits and reports and is annually audited under the WebTrust scheme for CA and BR-SSL certificates.